FBI FLASH

FBI LIAISON ALERT SYSTEM
#M-000045-TT

The following information was obtained through FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in **42 USC § 10607**.

In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and systems administrators to guard against the persistent malicious actions of cyber criminals.

This product is released at TLP: GREEN. The information in this product is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

SUMMARY

The FBI is providing the following information with **HIGH confidence**:

A group of cyber actors utilizing infrastructure located in Iran have been conducting computer network exploitation activity against public and private U.S. organizations, including Cleared Defense Contractors (CDCs), academic institutions, and energy sector companies. The actors typically utilize common computer intrusion techniques such as the use of TOR, open source reconnaissance, exploitation via SQL injection and web shells, and open source tools for further network penetration and persistence. Internet-facing infrastructures, such as web servers, are typical targets for this group. Once the actors penetrate a victim network, the actors exfiltrate network design information and legitimate user credentials for the victim network. Often times, the actors are able to harvest administrative user credentials and use the credentials to move laterally through a network.

According to public network registration information, IP addresses previously utilized by this group were assigned to "Tarh Andishan." The group primarily utilized two Iran-based IP addresses to conduct its activity, 78.109.194.114 and 217.11.17.99. There has been no recent activity from these IP addresses since early 2014; however, the group now primarily utilizes a series of proxy or midpoint infrastructure in support of their computer network operations. The most recent midpoint infrastructure used by this group was located in the United Kingdom and the Netherlands.

TECHNICAL DETAILS

Tools: The following tools have been known to be utilized by the cyber actors.

1021114.aspx
4g.exe
akisapi.php
ASPACK
Atkill.txt
Bitvise
c99shell.php
Cafae
Cain and Abel
CCProxy
CCproxy.zip
cmd.aspx
Cprivesc
debug.aspx
DefaultWS.asmx
Dirbuster
FileZilla
Find_tokens.exe
Find_tokens.txt
Gsecdump
Havij
hscan.zip
hscan1.2
img.asp
img.aspx
In2.txt
isapi.aspx
J.exe
Jasus.exe *size: 118,272 MD5: 53841511791E4CAC6F0768A9EB5DEF8A Type: ARP POISON TOOL*
Jasus.pdb
Kappfree
kappfree.dll
Kelloworld
kelloworld.dll
Klock
klock.dll
Lc.exe
lc15.exe
Libeay32.doc
Libeay32.txt

Loader.exe
LoggerModule.e
mim2.2.exe
Mimikatz
mimikatz.exe
mimikatz.swf
Mx.exe
NBrute Force
NC.exe
ncat.exe
Ncrack
Nc-themida.exe
Netcat
Netscp.exe
netscp_total.exe
Netview
Nmap
NTFS
OS_Detector.exe
ospcsvc.exe
osppsvc.exe
OSQL
ossisvc.exe
ossysvc.exe
Plink
plink.exe
priorities_readfile.aspx
Privesc.exe size: 51,200 MD5: DABF638EB53070CDC7B10BFA5E4E8142
ProcDump
proxy.php
PsExec
PsExec.exe
PsKill
PsList
Putty Link
putty.exe
pw.exe
PwDump
PwDump7.exe
PwDump7_p.exe
rdcmd.aspx
RunAs.exe
Samdump

sekurlsa.dll
Sl.exe
snmpwalk.exe
SQL Manager
STR.EXE
Themida
u.exe
U.exe size: 60,928 MD5: DDA3E5629A0E8FB63A3E19027AE45458
upload.aspx
Wcet
winBypass.php
WinDump
WinDump.exe
winpcap-nmap-4.12.exe
winusr.dll
wminotify.dll
wndTest.exe
wt.exe
xcmd-aspack.exe
xCmdSvc.exe
Xcmdt.exe
xcmd-themida.exe
xp_cmdshell
ZXPortMap.exe

IP Addresses: The following IP addresses have been observed to be utilized by the cyber actors.

64.120.208.154
78.109.194.114
159.253.144.209
217.11.17.99
95.211.191.225
95.211.241.249
95.211.241.251
108.175.153.158
88.150.214.162
88.150.214.166
88.150.214.168
88.150.214.170
184.82.158.18

Snort Signatures:

Havij Rules:

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET SCAN Havij SQL Injection Tool User-Agent Outbound"; flow:established,to_server; content:"|29| Havij|0d 0a|Connection|3a| "; http_header; reference:url,itsecteam.com/en/projects/project1.htm; classtype:web-application-attack; sid:2011924; rev:2;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN Havij SQL Injection Tool User-Agent Inbound"; flow:established,to_server; content:"|29| Havij|0d 0a|Connection|3a| "; http_header; reference:url,itsecteam.com/en/projects/project1.htm; classtype:web-application-attack; sid:2012606; rev:2;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"MALWARE-TOOLS Havij advanced SQL injection tool user-agent string"; flow:to_server, established; content:"Havij"; http_header; pcre:"/User-Agent\:[^\x0a\x0d]+?Havij/H"; metadata:policy balanced-ips drop, policy security-ips drop, service http; reference:url,itsecteam.com/en/projects/project1.htm; classtype:attempted-user; sid:21459; rev:3;)

Acunetix Rules:

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Acunetix Version 6 Crawl/Scan Detected"; flow:to_server,established; content:"/acunetix-wvs-test-for-some-inexistent-file"; http_uri; threshold: type threshold, track by_dst, count 2, seconds 5; reference:url,www.acunetix.com/; reference:url,doc.emergingthreats.net/2008571; classtype:attempted-recon; sid:2008571; rev:5;)

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Acunetix Version 6 (Free Edition) Scan Detected"; flow:to_server,established; content:"(Acunetix Web Vulnerability Scanner"; fast_pattern:only; threshold: type limit, count 1, seconds 60, track

by_src; reference:url,www.acunetix.com/; reference:url,doc.emergingthreats.net/2009646; classtype:attempted-recon; sid:2009646; rev:6;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"APP-DETECT Acunetix web vulnerability scan attempt"; flow:to_server,established; content:"Acunetix-"; fast_pattern:only; http_header; metadata:service http; reference:url,www.acunetix.com; classtype:web-application-attack; sid:25358; rev:2;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"APP-DETECT Acunetix web vulnerability scanner probe attempt"; flow:to_server,established; content:"/acunetix-wvs-test-for-some-inexistent-file"; fast_pattern:only; http_uri; metadata:service http; reference:url,www.acunetix.com; classtype:web-application-attack; sid:25359; rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"APP-DETECT Acunetix web vulnerability scanner authentication attempt"; flow:to_server,established; content:"password=g00dPa$$w0rD"; fast_pattern:only; http_uri; metadata:service http; reference:url,www.acunetix.com; classtype:web-application-attack; sid:25360; rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"APP-DETECT Acunetix web vulnerability scanner RFI attempt"; flow:to_server,established; content:"src=/testasp.vulnweb.com/"; fast_pattern:only; http_uri; metadata:service http; reference:url,www.acunetix.com; classtype:web-application-attack; sid:25361; rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"APP-DETECT Acunetix web vulnerability scanner base64 XSS attempt"; flow:to_server,established; content:"PHNjcmlwdD"; fast_pattern:only; http_uri; metadata:service http; reference:url,www.acunetix.com; classtype:web-application-attack; sid:25362; rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"APP-DETECT Acunetix web vulnerability scanner URI injection attempt"; flow:to_server,established; content:"http:/www.acunetix.com"; fast_pattern:only; http_uri; content:"Acunetix-"; nocase; http_header; metadata:service http; reference:url,www.acunetix.com; classtype:web-application-attack; sid:25363; rev:2;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"APP-DETECT Acunetix web vulnerability scanner prompt XSS attempt"; flow:to_server,established; content:"<ScRiPt>prompt("; fast_pattern:only; http_uri; metadata:service http; reference:url,www.acunetix.com; classtype:web-application-attack; sid:25364; rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"APP-DETECT Acunetix web vulnerability scanner XSS attempt"; flow:to_server,established; content:">=|5C|xa2";

fast_pattern:only; http_uri; metadata:service http; reference:url,www.acunetix.com; classtype:web-application-attack; sid:25365; rev:1;)

DirBuster Rules:

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN DirBuster Web App Scan in Progress"; flow:to_server,established; content:"User-Agent|3a| DirBuster"; fast_pattern:only; http_header; reference:url,owasp.org; reference:url,doc.emergingthreats.net/2008186; classtype:web-application-attack; sid:2008186; rev:5;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ET SCAN DirBuster Scan in Progress"; flow:established,to_server; content:"/thereIsNoWayThat-You-CanBeThere"; nocase; http_uri; threshold: type limit, track by_src,count 1, seconds 60; reference:url,www.owasp.org/index.php/Category%3aOWASP_DirBuster_Project; classtype:attempted-recon; sid:2011914; rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"INDICATOR-SCAN DirBuster brute forcing tool detected"; flow:to_server,established; content:"User-Agent|3A| DirBuster"; fast_pattern:only; http_header; metadata:service http; reference:url,sourceforge.net/projects/dirbuster/; classtype:web-application-attack; sid:19933; rev:7;)

The FBI requests network personnel use the following guidance to determine whether the cyber actors have compromised your computer network:

1. Analyze web servers

Identify SQL injection activity

Analyze web logs for SQL injection activity against external facing web servers, domains, and IP addresses.

SQL injection activity may contain strings such as: 1', 1=0, ‘,'1'='2, or '1'='1'.

SQL injection activity may contain strings such as “admin’ or 1=1”.

Search for evidence of DirBuster or Acunetix scanning. Sample user agent strings contain: "DirBuster-0.12 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)" or “Acunetix”.

Identify the use of xp_cmdshell, a SQL Server tool that executes a given command string as an operating-system command shell and returns any output as rows of text.

Identify creation of users and databases named “haha”.

Analyze new malicious files on web server

Search for new PHP or ASPX web shells placed on the network. The shell typically relies on cmd.exe to process commands like net user, net administrator, whoami, etc. The request for cmd.exe to process these commands was observed in the clear and an IDS can flag these cmd.exe requests as an intrusion indicator.

Analyze logs on web server

Search for web page queries containing "wp-content" or "wp-includes" in the URL.

2. Analyze internal computer systems (including web server)

Analyze event logs for unauthorized Remote Desktop Protocol (RDP) connections.

Analyze event logs for unauthorized user login activity typically from valid credentials. In many cases, administrative accounts are typically used. Actors will attempt to locate and compromise a domain controller, if present.

The actors may use the file atkill.txt to execute "at" commands to manipulate scheduled tasks. A file named "in.txt" may be used setup scheduled tasks to process the "whoami" command and direct the output to the file "res.txt" in the folder C:\windows\temp\.

Identify usage of .bat batch files for installation of malware and manipulation of service processes. Examples of such files are: autc.bat, autcc.txt.

The actors may disable and re-enable anti-virus scanner software, such as McAfee Antivirus Scanner. This may be achieved via scheduled tasks located in a file named "in2.txt".

Tools

Look for usage of software tools such as Incognito, RunAs, xCmd, OpenSSL toolkit, and Windows Credentials Editor. These tools may enable the actors to impersonate user tokens, conduct encrypted communications, and execute remote commands. File names associated with the use of these tools are as follows: find_tokens.exe, find_tokens.txt, kappfree, kelloworld, klock, libeay32.doc, and libeay32.txt.

Renaming “exe” and “dll” files to have common extensions (i.e., doc, sys, log) . Examples of such files are: sekurlsa.doc, kappfree.doc, kelloworld.doc, clock.doc, mimikatz.sys, and mikikatz.log.

Identify usage of the malware file churrasco.exe, potentially in the directory "c:\windows\temp\UUNKXUAE". The file may be saved to the temp folder which is a common place to place malware. A review of this folder would be a good practice to identify malicious files. The Churrasco.exe malware could allow a user to impersonate the rights of the SYSTEM user and consequently execute code with elevated privileges.

Usage of the PsExec software tool. This tool may be named "pse.exe" and located in the directory C:\windows\temp\ma. In general, .exe files located in temporary directories should be scrutinized.

Exfiltration of data

Identify recovery of “passwd” file on Unix-based hosts or “win.ini” file on Windows hosts.

Identify usage of 7zip compressed files, namely, "ma.7z" and "ma1.7z".

Actors may redirect their network activity logs to log files with the following names: 111.txt, 1111.txt, 1110.txt, pases.txt, 11011.txt, 11111.txt, and 11001.txt.

Actors may rename keylogger data from victim machines as attachments to spam messages/spam advertisements for Viagra, but they also contained .c7z attachments.

3. Perform network traffic analysis (host-based and network-based)

Analyze network traffic for attempts to create user profiles with a temporary sharklasers.com e-mail account.

Identify usage of 7zip compressed files, namely, "ma.7z" and "ma1.7z".

Identify unauthorized remote administration tool usage such as RDP or SSH. Also, identify any unauthorized RDP activity over port 3389.

POINT OF CONTACT

The FBI encourages recipients who identify the use of tool(s) or techniques discussed in this document to report information to their local FBI field office or the FBI's 24/7 Cyber Watch. Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855-292-3937 or by e-mail at cywatch@ic.fbi.gov.

Press inquiries should be directed to the FBI National Press Office at npo@ic.fbi.gov or 202-324-3691.