Alert (TA14-353A)

Targeted Destructive Malware

Original release date: December 19, 2014

Systems Affected

Microsoft Windows

Overview

US-CERT was recently notified by a trusted third party of cyber threat actors using a Server Message Block (SMB) Worm Tool to conduct cyber exploitation activities recently targeting a major entertainment company. This SMB Worm Tool is equipped with a Listening Implant, Lightweight Backdoor, Proxy Tool, Destructive Hard Drive Tool, and Destructive Target Cleaning Tool.

SMB Worm Tool: This worm uses a brute force authentication attack to propagate via Windows SMB shares. It connects home every five minutes to send log data back to command and control (C2) infrastructure if it has successfully spread to other Windows hosts via SMB port 445. The tool also accepts new scan tasking when it connects to C2. There are two main threads: the first thread calls home and sends back logs (a list of successful SMB exploitations), and the second thread attempts to guess passwords for SMB connections. If the password is correctly guessed, a file share is established and file is copied and run on the newly-infected host.

Listening Implant: During installation of this tool, a portion of the binaries is decrypted using AES, with a key derived from the phrase "National Football League." Additionally, this implant listens for connections on TCP port 195 (for "sensvc.exe" and "msensvc.exe") and TCP port 444 (for "netcfg.dll"). Each message sent to and from this implant is preceded with its length, then XOR encoded with the byte 0x1F. Upon initial connection, the victim sends the string, "HTTP/1.1 GET /dns?\x00." The controller then responds with the string "200 www.yahoo.com!\x00" (for "sensvc.exe" and "msensvc.exe") or with the string "RESPONSE 200 OK!!" (for "netcfg.dll"). The controller sends the byte "!" (0x21) to end the network connection. This special message is not preceded with a length or XOR encoded.

Lightweight Backdoor: This is a backdoor listener that is designed as a service DLL. It includes functionality such as file transfer, system survey, process manipulation, file time matching and proxy capability. The listener can also perform arbitrary code execution and execute commands on the command line. This tool includes functionality to open ports in a victim host's firewall and take advantage of universal Plug and Play (UPNP) mechanisms to discover routers and gateway devices, and add port mappings, allowing inbound connections to victim hosts on Network Address Translated (NAT) private networks. There are no callback domains associated with this malware since connections are inbound only on a specified port number.

Proxy Tool: Implants in this malware family are typically loaded via a dropper installed as a service, then configured to listen on TCP port 443. The implant may have an associated configuration file which can contain a configurable port. This proxy tool has basic backdoor functionality, including the ability to fingerprint the victim machine, run remote commands, perform directory listings, perform process listings, and transfer files.

Destructive Hard Drive Tool: This tool is a tailored hard-drive wiping tool that is intended to destroy data past the point of recovery and to complicate the victim machine's recovery. If the CNE operator has administrator-level privileges on the host, the program will over-write portions of up-to the first four physical drives attached, and over-write the master boot record (MBR) with a program designed to cause further damage if the hard drive is re-booted. This further results in the victim machine being non-operational with irrecoverable data (There is a caveat for machines installed with the windows 7 operating system: windows 7 machines will continue to operate in a degraded state with the targeted files destroyed until after reboot, in which the infected MBR then wipes the drive.) If the actor has user-level access, the result includes specific files being deleted and practically irrecoverable, but the victim machine would remain usable.

Destructive Target Cleaning Tool: This tool renders victim machines inoperable by overwriting the Master Boot Record. The tool is dropped and installed by another executable and consists of three parts: an executable and a dll which contain the destructive components, and an encoded command file that contains the actual destruction commands to be executed.

Network Propagation Wiper: The malware has the ability to propagate throughout the target network via built-in Windows shares. Based on the username/password provided in the configuration file and the hostname/IP address of target systems, the malware will access remote network shares in order to upload a copy of the wiper and begin the wiping process on these remote systems. The malware uses several methods to access shares on the remote systems to begin wiping files. Checking for existing shares via "\\hostname\admin$\system32" and "\\hostname\shared$\system32" or create a new share "cmd.exe /q /c net share shared$=%SystemRoot% /GRANT:everyone, FULL". Once successful, the malware uploads a copy of the wiper file "taskhostXX.exe", changes the file-time to match that of the built-in file "calc.exe", and starts the remote process. The remote process is started via the command "cmd.exe /c wmic.exe /node:hostname /user:username /password:pass PROCESS CALL CREATE". Hostname, username, and password are then obtained from the configuration file. Afterwards, the remote network share is removed via "cmd.exe /q /c net share shared$ /delete". Once the wiper has been uploaded, the malware reports its status back to one of the four C2 IP addresses.

Technical and strategic mitigation recommendations are included in the Solution section below.

US-CERT recommends reviewing the Security Tip Handling Destructive Malware #ST13-003.

Description

Cyber threat actors are using an SMB worm to conduct cyber exploitation activities. This tool contains five components – a listening implant, lightweight backdoor, proxy tool, destructive hard drive tool, and destructive target cleaning tool.

The SMB worm propagates throughout an infected network via brute-force authentication attacks, and connects to a C2 infrastructure.

Impact

Due to the highly destructive functionality of this malware, an organization infected could experience operational impacts including loss of intellectual property and disruption of critical systems.

Solution

Users and administrators are recommended to take the following preventive measures to protect their computer networks:

- Use and maintain anti-virus software – Anti-virus software recognizes and protects your computer against most known viruses. It is important to keep your anti-virus software up-to-date (see Understanding Anti-Virus Software for more information).
- Keep your operating system and application software up-to-date – Install software patches so that attackers can't take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it (see Understanding Patches for more information).
- Review Security Tip Handling Destructive Malware #ST13-003 and evaluate their capabilities encompassing planning, preparation, detection, and response for such an event.
- Review Recommended Practices for Control Systems, and Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies (pdf).

The following is a list of the Indicators of Compromise (IOCs) that can be added to network security solutions to determine whether they are present on a network.

MD5s:

SMB worm tool:

MD5: f6f48551d7723d87daeef2e840ae008f

Characterization: File Hash Watchlist

Notes: "SMB worm tool"

Earliest PE compile Time: 20141001T072107Z

Most Recent PE compile Time: 20141001T072107Z

MD5: 194ae075bf53aa4c83e175d4fa1b9d89

Characterization: File Hash Watchlist

Notes: "SMB worm tool"

Earliest PE compile Time: 20141001T120954Z

Most Recent PE compile Time: 20141001T142138Z

Lightweight backdoor:

MD5: f57e6156907dc0f6f4c9e2c5a792df48

Characterization: File Hash Watchlist

Notes: "Lightweight backdoor"

Earliest PE compile time: 20110411T225224Z

Latest PE compile time: 20110411T225224Z

MD5: 838e57492f632da79dcd5aa47b23f8a9

Characterization: File Hash Watchlist

Notes: "Lightweight backdoor"

Earliest PE compile time: 20110517T050015Z

Latest PE compile time: 20110605T204508Z

MD5: 11c9374cea03c3b2ca190b9a0fd2816b

Characterization: File Hash Watchlist

Notes: "Lightweight backdoor"

Earliest PE compile time: 20110729T062417Z

Latest PE compile time: 20110729T062958Z

MD5: 7fb0441a08690d4530d2275d4d7eb351

Characterization: File Hash Watchlist

Notes: "Lightweight backdoor"

Earliest PE compile time: 20120128T071327Z

Latest PE compile time: 20120128T071327Z

MD5: 7759c7d2c6d49c8b0591a3a7270a44da

Characterization: File Hash Watchlist

Notes: "Lightweight backdoor"

Earliest PE compile time: 20120309T105837Z

Latest PE compile time: 20120309T105837Z

MD5: 7e48d5ba6e6314c46550ad226f2b3c67

Characterization: File Hash Watchlist

Notes: "Lightweight backdoor"

Earliest PE compile time: 20120311T090329Z

Latest PE compile time: 20120311T090329Z

MD5: 0a87c6f29f34a09acecce7f516cc7fdb

Characterization: File Hash Watchlist

Notes: "Lightweight backdoor"

Earliest PE compile time: 20120325T053138Z

Latest PE compile time: 20130513T090422Z

MD5: 25fb1e131f282fa25a4b0dec6007a0ce

Characterization: File Hash Watchlist

Notes: "Lightweight backdoor"

Earliest PE compile time: 20130802T054822Z

Latest PE compile time: 20130802T054822Z

MD5: 9761dd113e7e6673b94ab4b3ad552086

Characterization: File Hash Watchlist

Notes: "Lightweight backdoor"

Earliest PE compile time: 20130913T013016Z

Latest PE compile time: 20130913T013016Z

MD5: c905a30badb458655009799b1274205c

Characterization: File Hash Watchlist

Notes: "Lightweight backdoor"

Earliest PE compile time: 20140205T090906Z

Latest PE compile time: 20140205T090906Z

MD5: 40adcd738c5bdc5e1cc3ab9a48b3df39

Characterization: File Hash Watchlist

Notes: "Lightweight backdoor"

Earliest PE compile time: 20140320T152637Z

Latest PE compile time: 20140402T023748Z

MD5: 68a26b8eaf2011f16a58e4554ea576a1

Characterization: File Hash Watchlist

Notes: "Lightweight backdoor"

Earliest PE compile time: 20140321T014949Z

Latest PE compile time: 20140321T014949Z

MD5: 74982cd1f3be3d0acfb0e6df22dbcd67

Characterization: File Hash Watchlist

Notes: "Lightweight backdoor"

Earliest PE compile time: 20140506T020330Z

Latest PE compile time: 20140506T020330Z

Proxy tool:

MD5: 734740b16053ccc555686814a93dfbeb

Characterization: File Hash Watchlist

Notes: "Proxy tool"

Earliest PE compile time: 20140611T064905Z

Latest PE compile time: 20140611T064905Z

MD5: 3b9da603992d8001c1322474aac25f87

Characterization: File Hash Watchlist

Notes: "Proxy tool"

Earliest PE compile time: 20140617T035143Z

Latest PE compile time: 20140617T035143Z

MD5: e509881b34a86a4e2b24449cf386af6a

Characterization: File Hash Watchlist

Notes: "Proxy tool"

Earliest PE compile time : 20140618T064527Z

Latest PE compile time: 20140618T064527Z

MD5: 9ab7f2bf638c9d911c2c742a574db89e

Characterization: File Hash Watchlist

Notes: "Proxy tool"

Earliest PE compile time: 20140724T011233Z

Latest PE compile time: 20140724T011233Z

MD5: a565e8c853b8325ad98f1fac9c40fb88

Characterization: File Hash Watchlist

Notes: "Proxy tool"

Earliest PE compile time: 20140724T065031Z

Latest PE compile time: 20140902T135050Z

MD5: 0bb82def661dd013a1866f779b455cf3

Characterization: File Hash Watchlist

Notes: "Proxy tool"

Earliest PE compile time: 20140819T024812Z

Latest PE compile time: 20140819T024812Z

MD5: b8ffff8b57586d24e1e65cd0b0ad9173

Characterization: File Hash Watchlist

Notes: "Proxy tool"

Earliest PE compile time: 20140902T172442Z

Latest PE compile time: 20140902T172442Z

MD5: 4ef0ad7ad4fe3ef4fb3db02cd82bface

Characterization: File Hash Watchlist

Notes: "Proxy tool"

Earliest PE compile time: 20141024T134136Z

Latest PE compile time: 20141024T134136Z

MD5: eb435e86604abced7c4a2b11c4637a52

Characterization: File Hash Watchlist

Notes: "Proxy tool"

Earliest PE compile time: 20140526T010925Z

Latest PE compile time: 20140526T010925Z

MD5: ed7a9c6d9fc664afe2de2dd165a9338c

Characterization: File Hash Watchlist

Notes: "Proxy tool"

Earliest PE compile time: 20140611T064904Z

Destructive hard drive tool:

MD5: 8dec36d7f5e6cbd5e06775771351c54e

Characterization: File Hash Watchlist

Notes: "Destructive hard drive tool"

Earliest PE compile time: 20120507T151820Z

Latest PE compile time: 20120507T151820Z

MD5: a385900a36cad1c6a2022f31e8aca9f7

Characterization: File Hash Watchlist

Notes: "Destructive target cleaning tool"

Earliest PE compile time: 20130318T003315Z

Latest PE compile time: 20130318T003315Z

MD5: 7bea4323807f7e8cf53776e24cbd71f1

Characterization: File Hash Watchlist

Notes: "Destructive target cleaning tool"

Earliest PE compile time: 20130318T003319Z

Latest PE compile time: 20130318T003319Z

Name: d1c27ee7ce18675974edf42d4eea25c6.bin

Size: 268579 bytes (268.6 KB)

MD5: D1C27EE7CE18675974EDF42D4EEA25C6

PE Compile Time: 2014-11-22 00:06:54

The malware has the following characteristics:

While the original filename of this file is unknown, it was likely “diskpartmg16.exe”. This file serves as a dropper. It drops destructive malware: “igfxtrayex.exe”. When the dropper file was executed, it started a second instance of itself with “-i” as an argument, and then terminated. The second instance of the dropper file installed itself as the “WinsSchMgmt” service with “-k” as a command line argument, started the service, and then terminated. The “WinsSchMgmt” service executed the file with “-k” as an argument, which started another instance of the file using “-s” as an argument. The “-s” instance dropped and executed “igfxtrayex.exe”, created “net_ver.dat”, and began generating network traffic over TCP ports 445 and 139 to victim IP addresses.

Name: net_ver.dat

Size: 4572 bytes (4.6 KB) (size will vary)

MD5: 93BC819011B2B3DA8487F964F29EB934 (hash will vary)

This is a log file created by the dropper, and appended to as the scans progress It contains what appear to be hostnames, IP addresses, and the number 2. Entries in the file have the structure “HOSTNAME | IP Address | 2”.

Name: igfxtrayex.exe

Size: 249856 bytes (249.9 KB)

MD5: 760C35A80D758F032D02CF4DB12D3E55

PE Compile Time: 2014-11-24 04:11:08

This file is destructive malware: a disk wiper with network beacon capabilities. If “igfxtrayex.exe” is run with no parameters, it creates and starts a copy of itself with the “–i” argument. After 10 minutes, the “igfxtrayex.exe” makes three copies of itself and places them in the same directory from which it was executed. These copies are named according to the format “taskhostXX.exe” (where X is a randomly generated ASCII character). These copies are then executed, each with a different argument (one being “-m”, one being “-d” and the other “-w”). Network connection attempts are made to one of three hard-coded IP addresses in a random order to port 8080 or 8000. If a connection to the IP address cannot be made, it attempts to connect to another of the three IP addresses, until connections to all three IP addresses have been attempted. The following command-line string is then executed: “cmd.exe /c net stop MSExchangeIS /y”. A 120-minute (2 hour) sleep command is issued after which the computer is shut down and rebooted.

Name: iissvr.exe

Size: 114688 bytes (114.7 KB)

MD5: E1864A55D5CCB76AF4BF7A0AE16279BA

PE Compile Time: 2014-11-13 02:05:35

This file, when executed, starts a listener on localhost port 80. It has 3 files contained in the resource section; all xor’d with 0x63.

Name: usbdrv3_32bit.sys

Size: 24280 bytes (24.3 KB)

MD5: 6AEAC618E29980B69721158044C2E544

PE Compile Time: 2009-08-21 06:05:32

This SYS file is a commercially available tool that allows read/write access to files and raw disk sectors for user mode applications in Windows 2000, XP, 2003, Vista, 2008 (32-bit). It is dropped from resource ID 0x81 of “igfxtrayex.exe”.

Name: usbdrv3_64bit.sys

Size: 28120 bytes (28.1 KB)

MD5: 86E212B7FC20FC406C692400294073FF

PE Compile Time: 2009-08-21 06:05:35

This SYS file is a also a commercially available tool that allows read/write access to files and raw disk sectors for user mode applications in Windows 2000, XP, 2003, Vista, 2008 (64-bit). It is dropped from resource ID 0x83 of “igfxtrayex.exe”.

Name: igfxtpers.exe

Size: 91888 bytes (91.9 KB)

MD5: e904bf93403c0fb08b9683a9e858c73e

PE Compile Time: 2014-07-07 08:01:09

A summary of the C2 IP addresses:

IP Address	Country	Port	Filename
203.131.222.102	Thailand	8080	Diskpartmg16.exe igfxtrayex.exe igfxtpers.exe
217.96.33.164	Poland	8000	Diskpartmg16.exe igfxtrayex.exe
88.53.215.64	Italy	8000	Diskpartmg16.exe igfxtrayex.exe
200.87.126.116	Bolivia	8000	File 7
58.185.154.99	Singapore	8080	File 7
212.31.102.100	Cypress	8080	File 7
208.105.226.235	United States	--	igfxtpers.exe

Snort signatures:

SMB Worm Tool (not necessarily the tool itself):

alert tcp any any -> any any (msg:"Wiper1";content:"|be 64 ba f2 a8 64|";offset:16;depth:6;sid:1;)

alert tcp any any -> any any (msg:"Wiper2";content:"|c9 06 d9 96 fc 37 23 5a fe f9 40 ba 4c 94 14 98|";offset:0;depth:16;sid:3;)

alert tcp any any -> any any (msg:"Wiper3";content:"|aa 64 ba f2 56 9b|";offset:0;depth:50;sid:2;)

alert ip any any -> any any (msg:"Wiper4";content:"|aa 74 ba f2 b9 75|";offset:0;depth:74;sid:4;)

Listening Implant:

alert tcp any any -> any any (msg:"Backdoor1";content:"|0c 1f 1f 1f 4d 5a 4c 4f 50 51 4c 5a 3f 2d 2f 2f 3f 50 54 3e 3e 3e|";offset:0;depth:22;sid:9;)

alert tcp any any -> any any (msg:"Backdoor2";content:"|d3 c4 d2 d1 ce cf d2 c4 a1 b3 b1 b1 a1 ce ca a0 a0 a0|";offset:0;depth:18;sid:12;)

alert ip any any -> any any (msg:"Backdoor3";content:"|17 08 14 13 67 0f 13 13 17 67 15 02 16 12 02 14 13 78 47 47|";depth:24;sid:1;)

alert ip any any -> any any (msg:"Backdoor4";content:"|4f 50 4c 4b 3f 57 4b 4b 4f 3f 4d 5a 4e 4a 5a 4c 4b 20 1f|";depth:23;sid:2;)

alert ip any any -> any any (msg:"Backdoor5";content:"|15 02 14 17 08 09 14 02 67 75 77 77 67 08 0c 66 66 66|";depth:22;sid:3;)

alert tcp any any -> any any (msg:"Backdoor6";content:"|09 22 33 30 28 35 2c|";sid:4;)

alert tcp any any -> any any (msg:"Backdoor7";content:"|13 2f 22 35 22 67 26 35 22 29 27 33 67 28 37 22 29 67 37 28 35 33 34 69|";sid:5;)

alert tcp any any -> any any (msg:"Backdoor8";content:"|43 47 47 47 45 67 47 47 43 47 47 47 44 67 47 47|";sid:6;)

alert tcp any any -> any any (msg:"Backdoor9";content:"|43 47 47 47 42 67 47 47 43 47 47 47 4f 67 47 47 43 47 47 47 43 67 47 47 43 47 47 47 4e 67 47 47|";sid:7;)

alert tcp any any -> any any (msg:"Backdoor10";content:"|d1 ce d2 d5 a1 c9 d5 d5 d1 a1 d3 c4 d0 d4 c4 d2 d5 be|";offset:0;depth:18;sid:8;)

alert tcp any any -> any any (msg:"Backdoor11";content:"|17 08 14 13 67 0f 13 13 17 67 15 02 16 12 02 14 13 78|";offset:0;depth:18;sid:10;)

alert tcp any any -> any any (msg:"Backdoor12";content:"|0c 1f 1f 1f 4f 50 4c 4b 3f 57 4b 4b 4f 3f 4d 5a 4e 4a 5a 4c 4b 20|";sid:11;)

Lightweight Backdoor:

alert tcp any 488 <> any any (msg:"Proxy1";content:"|60 db 37 37 37 37 37 37|";sid:3;)

alert tcp any any -> any 488 (msg:"Proxy2";content:"|60 db 37 37 37 37 37 37|";sid:4;)

alert tcp any any -> any any (msg:"Proxy3";content:"|4c 4c|";offset:16;depth:2;content:"|75 14 2a 2a|";distance:4;within:4;sid:4;)

alert tcp any any -> any any (msg:"Proxy4";content:"|8A 10 80 C2 67 80 F2 24 88 10|";content:"8A 10 80 F2 24 80 EA 67 88 10";sid:2;)

alert tcp any 488 <> any any (msg:"Proxy5";content:"|65 db 37 37 37 37 37 37|";sid:2;)

alert tcp any any -> any 488 (msg:"Proxy6";content:"|65 db 37 37 37 37 37 37|";sid:2;)

alert tcp any [547,8080,133,117,189,159] -> any any (msg:"Proxy7";content:"|7b 08 2a 2a|";offset:17;content:"|08 2a 2a 01 00|";distance:0;sid:1;)

alert tcp any any -> any any (msg:"Proxy8";content:"|8A 10 80 EA 62 80 F2 B4 88 10|";content:"|8A 10 80 F2 B4 80 C2 62 88 10|";sid:1;)

alert tcp any any -> any any (msg:"Proxy9";content:"|8A 10 80 C2 4E 80 F2 79 88 10|";content:"|8A 10 80 F2 79 80 EA 4E 88 10[";sid:3;)

alert tcp any any -> any any (msg:"Proxy10";content:"Sleepy!@#qaz13402scvsde890";nocase;content:"BC435@PRO62384923412!@3!";nocase;sid:5;)

Proxy Tool:

alert tcp any any -> any any (msg:"Wiper1";content:"|8A 10 80 C2 3A 80 F2 73 88 10|";content:"|8A 10 80 F2 73 80 EA 3A 88 10|";sid:4;)

alert tcp any any -> any any (msg:"Wiper2";content:!"HTTP/1";content:"|e2 1d 49 49|";offset:O;depth:4;content:"|49 49 49 49|";distance:4;within:4;sid:6;)

alert tcp any any -> any any (msg:"Wiper3";content:"|82 F4 DE D4 D3 C2 CA F5 C8 C8 D3 82 FB F4 DE D4 D3 C2 CA 94 95 FB D4 D1 C4 CF C8 D4 D3 89 C2 DF C2 87 8A CC 87 00|";sid:1;)

Malware associated with the cyber threat actor:

alert tcp any any -> any [8000,8080] (msg:"WIPER4";flow: established, to_server;dsize:42;content:"|28 00|";depth:2;content:"|04 00 00 00|";offset:38;depth:4;sid:123;)

Host Based Indicators

Below are potential YARA signatures to detect malware binaries on host machines:

SMB Worm Tool:

strings:

$STR1 = "Global\\FwtSqmSession106829323_S-1-5-19"

$STR2 ="EVERYONE"

$STR3 = "y0uar3@s!llyid!07,ou74n60u7f001"

$STR4 = "\\KB25468.dat" condition:

(uintl6(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) ==0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and all of them

Lightweight Backdoor:

strings:

$STR1 = "NetMgStart"

$STR2 = "Netmgmt.srg"

condition:

(uint16(0) == 0x5A4D) and all of them

Lightweight Backdoor:

strings:

$STR1 = "prxTroy" ascii wide nocase

condition:

(uintl6(0) == 0x5A4D or uint16(0) == 0xCFD0 or uintl6(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and all of them

Lightweight Backdoor:

strings:

$strl = { C6 45 E8 64 C6 45 E9 61 C6 45 EA 79 C6 45 EB 69 C6 45 EC 70 C6 45 ED 6D C6 45 EE 72 C6 45 EF 2E C6 45 F0 74 C6 45 F1 62 C6 45 F2 6C } // 'dayipmr.tbl' being moved to ebp

condition:

(uintl6(0) == 0x5A4D or uintl6(0) == 0xCFD0 or uint16(0) == 0xC3D4 or

uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and all of them

Lightweight Backdoor:

strings:

$strl = { C6 45 F4 61 C6 45 F5 6E C6 45 F6 73 C6 45 F7 69 C6 45 F8 2E C6 45 F9 6E C6 45 FA 6C C6 45 FB 73 } // 'ansi.nls' being moved to ebp

condition:

(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uintl6(0) == 0xC3D4 or

uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and all of them

Lightweight Backdoor:

strings:

$strl = { C6 45 F4 74 C6 45 F5 6C C6 45 F6 76 C6 45 F7 63 C6 45 F8 2E C6 45 F9 6E C6 45 FA 6C C6 45 FB 73 } // 'tlvc.nls' being moved to ebp

condition:

(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and all of them

Lightweight Backdoor:

strings:

$STR1 = { 8A 10 80 ?? 4E 80 ?? 79 88 10}

$STR2 = {SA 10 80?? 79 80 ?? 4E 88 10}

condition:

(uintl6(0) == 0x5A4D or uintl6(0) == 0xCFD0 or uint16(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and all of them

Proxy Tool:

strings:

$STR1 = "pmsconfig.msi" wide

$STR2 = "pmslog.msi" wide

condition:

(uint16(0) == 0x5A4D or uint16(0) == 0xCFD0 or uintl6(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and any of them

Proxy Tool:

strings:

$STR1 = { 82 F4 DE D4 D3 C2 CA F5 C8 C8 D3 82 FB F4 DE D4 D3 C2 CA 94 95 FB D4 DI C4 CF C8 D4 D3 89 C2 DF C2 87 8A CC 87 00 } //
'%SystemRoot%\System32\svchost.exe -k' xor A7

condition:

(uint16(0) == 0x5A4D or uintl6(0) == 0xCFD0 or uint16(0) == 0xC3D4 or

uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and all of them

Proxy Tool:

strings:

$STR2 = {8A 04 17 8B FB 34 A7 46 88 02 83 C9 FF}

condition:

(uintl6(0) == 0x5A4D or uint16(0) == 0xCFD0 or uintl6(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and $STR2

Destructive Hard Drive Tool:

strings:

$str0= "MZ"

$str1 = {c6 84 24 ?? (00 | 01) 00 00 }

$xorInLoop = { 83 EC 20 B9 08 00 00 00 33 D2 56 8B 74 24 30 57 8D 7C 24 08

F3 A5 8B 7C 24 30 85 FF 7E 3A 8B 74 24 2C 8A 44 24 08 53 8A 4C 24 21 8A 5C 24 2B 32 C1 8A 0C 32 32 C3 32 C8 88 0C 32 B9 1E 00 00 00 8A 5C 0C 0C 88 5C 0C 0D 49 83 F9 FF 7F F2 42 88 44 24 0C 3B D7 7C D0 5B 5F 5E 83 C4 20 C3 }

condition:

$str0 at 0 and $xorInLoop and #str1 > 300

Destructive Target Cleaning Tool:

strings:

$s1 = {d3000000 [4] 2c000000 [12] 95000000 [4] 6a000000 [8] 07000000}

condition:

(uintl6(0) == 0x5A4D and uintl6(uint32(0x3c)) == 0x4550) and all of them

Destructive Target Cleaning Tool:

strings

$secureWipe= { 83 EC 34 53 55 8B 6C 24 40 56 57 83 CE FF 55 C7 44 24 2C D3 00 00 00 C7 44 24 30 2C 00 00 00 89 74 24 34 89 74 24 38 C7 44 24 3C 95 00 00 00 C7 44 24 40 6A 00 00 00 89 74 24 44 C7 44 24 14 07 00 00 00 FF 15 ?? ?? ?? ?? 3B C6 89 44 24 1C OF 84 (D8 | d9) 01 00 00 33 FF 68 00 00 01 00 57 FF 15 ?? ?? ?? ?? 8B D8 3B DF 89 5C 24 14 OF 84 (BC | BD) 01 00 00 8B 44 24 1C A8 01 74 0A 24 FE 50 55 FF 15 ?? ?? ?? ?? 8B 44 24 4C 2B C7 74 20 48 74 0F 83 E8 02 75 1C C7 44 24 10 03 00 00 00 EB 12 C7 44 24 10 01 00 00 00 89 74 24 28 EB 04 89 7C 24 10 8B 44 24 10 89 7C 24 1C 3B C7 OF 8E (5C | 5d) 01 00 00 8D 44 24 28 89 44 24 4C EB 03 83 CE FF 8B 4C 24 4C 8B 01 3B C6 74 17 8A D0 B9 00 40 00 00 8A F2 8B FB 8B C2 C1 E0 10 66 8B C2 F3 AB EB (13 | 14) 33 F6 (E8 | ff 15) ?? ?? ?? ?? 88 04 1E 46 81 FE 00 00 01 00 7C (EF | ee) 6A 00 6A 00 6A 03 6A 00 6A 03 68 00 00 00 C0 55 FF 15 ?? ?? ?? ?? 8B F0 83 FE FF OF 84 FA 00 00 00 8D 44 24 20 50 56 FF 15 ?? ?? ?? ?? 8B 2D ?? ?? ?? ?? 6A 02 6A 00 6A FF 56 FF D5 8D 4C 24 18 6A 00 51 6A 01 53 56 FF 15 ?? ?? ?? ?? 56 FF 15 ?? ?? ?? ?? 6A 00 6A 00 6A 00 56 FF D5 8B 44 24 24 8B 54 24 20 33 FF 33 DB 85 CO 7C 5A 7F 0A 85 D2 76 54 EB 04 8B 54 24 20 8B CA BD 00 00 01 00 2B CF 1B C3 85 C0 7F 0A 7C 04 3B CD 73 04 2B D7 8B EA 8B 44 24 14 8D 54 24 18 6A 00 52 55 50 56 FF 15 ?? ?? ?? ?? 8B 6C 24 18 8B 44 24 24 03 FD 83 D3 00 3B D8 7C BE 7F 08 8B 54 24 20 3B FA 72 B8 8B 2D ?? ?? ?? ?? 8B 5C 24 10 8B 7C 24 1C 8D 4B FF 3B F9 75 17 56 FF 15 ?? ?? ?? ?? 6A 00 6A 00 6A 00 56 FF D5 56 FF 15 ?? ?? ?? ?? 56 FF 15 ?? ?? ?? ?? 56 FF 15 ?? ?? ?? ?? 8B 4C 24 4C 8B 6C 24 48 47 83 C1 04 3B FB 8B 5C 24 14 89 7C 24 1C 89 4C 24 4C 0F 8C (AE | AD) FE FF FF 6A 00 55 E8 ?? ?? ?? ?? 83 C4 08 53 FF 15 ?? ?? ?? ?? 5F 5E 5D 5B 83 C4 34 C3}

condition:

$secureWipe

Destructive Target Cleaning Tool:

strings:

$S1_CMD_Arg = ""/install"" fullword

$S2_CMD_Parse= ""\""%s"" /install \""%s\""""" fullword

$S3_CMD_Builder= ""\""%s\"" \""%s\"" \""%s\"" %s"" fullword

condition:

all of them

Destructive Target Cleaning Tool:

strings:

$BATCH_SCRIPT_LN1_0 = ""goto x"" fullword

$BATCH_SCRIPT_LN1_1 = ""del"" fullword

$BATCH_SCRIPT_LN2_0 = ""if exist"" fullword

$BATCH_SCRIPT_LN3_0 = "":x"" fullword

$BATCH_SCRIPT_LN4_0 = ""zz%d.bat"" fullword

condition:

(#BATCH_SCRIPT_LNl_l == 2) and all of them"

Destructive Target Cleaning Tool:

strings:

$MCU_DLL_ZLIB_COMPRESSED2=

{5CECABAE813CC9BCD5A542F4549104283434798O6F71D5521E2AOD}

condition:

$MCU_DLL_ZLIB_COMPRESSED2"

Destructive Target Cleaning Tool:

strings:

$MCU_INF_StartHexDec =

{010346080A30D63633000B6263750A5052322A00103D1B570A30E67F2A00130952690A50 3A0D2A000E00A26El5104556766572636C7669642E657865}

$MCU_INF_StartHexEnc =

{6C3272386958BF075230780A0A54676166024968790C7A6779588F5E47312739310163615B3D59686721CF5F2120263EIF5413531FIE004543544C55}

condition:

$MCU_INF_StartHexEnc or

$MCU_INF_StartHexDec

Destructive Target Cleaning Tool:

strings:

$ = "SetFilePointer"

$ = "SetEndOfFile"

$ = {75 17 56 ff 15 ?? ?? ?? ?? 6a 00 6a 00 6a 00 56 ffD5 56 ff 15?? ?? ??

?? 56}

condition:

(uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them

Destructive Target Cleaning Tool:

strings:

$license=

{E903FFFF820050006F007200740069006F006E007300200063006F007000790072006900670068007400200052006F006200650072007400200064006500200042006100740680

$PuTTY= {50007500540054005900}

condition:

(uint16(0) == 0x5A4D and uintl6(uint32(0x3c)) == 0x4550) and $license and not $PuTTY

Malware used by cyber threat actor:

strings:

$heapCreateFunction_0 = {33C06A00394424086800100000F94C050FF15????????85C0A3???????07436E893FEFFFF83F803A3???????
0750D68F8030000E8??00000059EB0A83F8027518E8????000085C0750FFF35???????0FF15???????033C0C36A0158C3}

$heapCreateFunction =

{558BECB82C120000E8????FFFF8D8568FFFFFF5350C78568FFFFFF94000000FF1????????
085C0741A83BD78FFFFFF02751183BD6CFFFFFF0572086A0158E9020100008D85D4EDFFF68901000005068???????0FF15???????
085C00F84D000000033DB8D8DD4EDFFFF389DD4EDFFFF74138A013C617C083C7A7F042C20880141381975ED8D85D4EDFFFF6A165068???????0E8????
000083C40C85C075088D85D4EDFFFFEB498D8564FEFFFF68040100005053FF15???????
0389D64FEFFFF8D8D64FEFFFF74138A013C617C083C7A7F042C20880141381975ED8D8564FEFFFF508D85D4EDFFFF50E8????????
59593BC3743E6A2C50E8????????593BC3597430408BC83818740E80393B75048819EB0141381975F26A0A5350E8????
000083C40C83F802741D83F803741883F80174138D45FC50E898FEFFFF807DFC06591BC083C0035BC9C3}

$getMajorMinorLinker =

{568B7424086A00832600FF15???????06681384D5A75148B483C85C9740D03C18A481A880E8A401B8846015EC3}

$openServiceManager =

{FF15???0?0?08B?885??74????????????????5?FF15???0?0?08B?????0?0?08BF?85F?74}

condition:

all of them

Malware used by cyber threat actor:

strings:

$str1 = "_quit"

$str2 = "_exe"

$str3 = "_put"

$str4 = "_got"

$str5 = "_get"

$str6 ="_del"

$str7 = "_dir"

$str8 = { C7 44 24 18 1F F7}

condition:

(uintl6(0) == 0x5A4D or uintl6(0) == 0xCFD0 or uintl6(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and all of them

Malware used by cyber threat actor:

strings:

$STR1 = { 50 68 80 00 00 00 68 FF FF 00 00 51 C7 44 24 1C 3a 8b 00 00 }

condition:

(uintl6(0) == 0x5A4D or uint16(0) == 0xCFD0 or uintl6(0) == 0xC3D4 or uint32(0) == 0x46445025 or uint32(1) == 0x6674725C) and all of them

Recommended Security Practices

Because of the highly destructive functionality of the malware, an organization infected with the malware could experience operational impacts including loss of intellectual property (IP) and disruption of critical systems. Actual impact to organizations may vary depending on the type and number of systems impacted.

Tactical Mitigations

- Implement the indicators of compromise within your systems for detection and mitigation purposes.
- Encourage users to transfer critical files to network shares, to allow for central backed up.
- Execute daily backups of all critical systems.
- Periodically execute an “offline” backup of critical files to removable media.
- Establish emergency communications plans should network resources become unavailable.
- Isolate any critical networks (including operations networks) from business systems.

- Identify critical systems and evaluate the need for having on-hand spares to quickly restore service.
- Ensure antivirus is up to date.
- Disable credential caching for all desktop devices with particular importance on critical systems such as servers and restrict the number of cached credential for all portable devices to no more than three if possible. This can be accomplished through a Group Policy Object (GPO).
- Disable AutoRun and Autoplay for any removable media device.
- Prevent or limit the use of all removable media devices on systems to limit the spread or introduction of malicious software and possible exfiltration data, except where there is a valid business case for use. This business case must be approved by the organization Chief IT Security Officer, with policy/guidance on how such media should be used.
- Consider restricting account privileges. It is our recommendation that all daily operations should be executed using standard user accounts unless administrative privileges are required for that specific function. Configure all standard user accounts to prevent the execution and installation of any unknown or unauthorized software. Both standard and administrative accounts should have access only to services required for nominal daily duties, enforcing the concept of separation of duties. Lastly, disable Web and email capabilities on administrative accounts. Compromise of admin accounts is one vector that allows malicious activity to become truly persistent in a network environment.
- Ensure that password policy rules are enforced and Admin password values are changed periodically.
- Consider prohibiting hosts within the production environment or DMZ from sharing an Active Directory enterprise with hosts on other networks. Each environment should have separate forests within Active Directory, with no trust relationships allowed between the forests if at all possible. If necessary, the trust relationships should be one-way with the low integrity environment trusting the higher integrity environment.
- Consider deployment of a coaching page with click through acceptance; these are traditionally deployed in an environment to log the acceptance of network acceptable use policy or to notify users of monitoring. Coaching pages also provide some measure of protection from automated malicious activity. This occurs because automated malware is normally incapable of physically clicking an acceptance radial button. Automated malware is traditionally hardcoded to execute, then retrieve commands or additional executables from the Internet. If the malware is unable to initiate an active connection, the full train of infection is potentially halted. The danger still exists that the physical user will authorize access, but through the use of coaching pages, infections can be limited or at least the rate of infection reduced.
- Monitor logs -- Maintain and actively monitor a centralized logging solution that keeps track of all anomalous and potentially malicious activity.
- Ensure that all network operating systems, web browsers, and other related network hardware and software remain updated with all current patches and fixes.

Strategic Mitigations

- Organizations should review Security Tip Handling Destructive Malware #ST13-003 and evaluate their capabilities encompassing planning, preparation, detection, and response for such an event.
- Always keep your patch levels up to date, especially on computers that host public services accessible through the firewall, such as HTTP, FTP, mail, and DNS services.
- Build host systems, especially critical systems such as servers, with only essential applications and components required to perform the intended function. Any unused applications or functions should be removed or disabled, if possible, to limit the attack surface of the host.
- Implement network segmentation through V-LANs to limit the spread of malware.
- Consider the deployment of Software Restriction Policy set to only allow the execution of approved software (application whitelisting)
- Recommend the whitelisting of legitimate executable directories to prevent the execution of potentially malicious binaries.
- Consider the use of two-factor authentication methods for accessing privileged root level accounts or systems.
- Consider deploying a two-factor authentication through a hardened IPsec/VPN gateway with split-tunneling prohibited for secure remote access.
- Deny direct Internet access, except through the use of proxies for Enterprise servers and workstations. Perform regular content filtering at the proxies or external firewall points of presence. Also consider the deployment of an explicit versus transparent proxy policy.
- Implement a Secure Socket Layer (SSL) inspection capability to inspect both ingress and egress encrypted network traffic for potential malicious activity.
- Isolate network services, such as email and Web application servers by utilizing a secure multi-tenant virtualization technology. This will limit the damage sustained from a compromise or attack of a single network component.
- Implement best practice guidance and policy to restrict the use of non-Foundation assets for processing or accessing Foundation-controlled data or systems (e.g., working from home, or using a personal device while at the office). It is difficult to enforce corporate policies, detect intrusions, and conduct forensic analysis or remediate compromises on non-corporate owned devices.
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Place control system networks behind firewalls, and isolate or air gap them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.
- Industrial Control System (ICS)-CERT and US-CERT remind organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

References

- N/A

Revisions

- December 19, 2014: Initial Release