MAR-10135536-3 - HIDDEN COBRA RAT/Worm | CISA

Published: 2018-05-31 · Archived: 2026-04-05 13:48:04 UTC

Notification

Summary

Description

This submission includes four unique files. The first is an installer for additional malware: a Remote Access Trojan (RAT) and a malicious Dynamic Link Library (DLL) that functions as a Server Message Block (SMB) Worm. The fourth file is another SMB worm in the form of a Windows 32-bit executable.

Both SMB worms attempt to spread locally and to random IP addresses on the public Internet by attempting to brute force vulnerable systems using a built-in list of common passwords. The RAT included with the SMB worm provides the attacker with the ability to deliver additional malware, run local commands, and exfiltrate data.

As of May 31, 2018, this report has been updated to correct the email addresses used by Wmmvsvc.dll (ea46ed5aed900cd9f01156a1cd446cbb3e10191f9f980e9f710ea1c20440c781).

For a downloadable copy of IOCs, see:

- MAR-10135536-3.stix

Emails (2)

misswang8107@gmail.com

redhat@gmail.com

Submitted Files (4)

077d9e0e12357d27f7f0c336239e961a7049971446f7a3f10268d9439ef67885 (4731CBAEE7ACA37B596E38690160A7...)

a1c483b0ee740291b91b11e18dd05f0a460127acfc19d47b446d11cd0e26d717 (scardprv.dll)

ea46ed5aed900cd9f01156a1cd446cbb3e10191f9f980e9f710ea1c20440c781 (Wmmvsvc.dll)

fe7d35d19af5f5ae2939457a06868754b8bdd022e1ff5bdbe4e7c135c48f9a16 (298775B04A166FF4B8FBD3609E7169...)

Findings

077d9e0e12357d27f7f0c336239e961a7049971446f7a3f10268d9439ef67885

Tags

backdoortrojanworm

Details

Name	4731CBAEE7ACA37B596E38690160A749
Size	208896 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	4731cbaee7aca37b596e38690160a749
SHA1	80fac6361184a3e24b33f6acb8688a6b7276b0f2

SHA256	077d9e0e12357d27f7f0c336239e961a7049971446f7a3f10268d9439ef67885
SHA512	9fdc1bf087d3e2fa80ff4ed749b11a2b3f863bed7a59850f6330fc1467c38eed052eee0337d2f82f9fe8e145f68199b966ae3c08f7ad1475b665bel
ssdeep	6144:M6atGpHk4NdSksOBbNUyb4ajb1TWiYW9ebYwtJEGLYMYR4:Msdk4NdSksOv
Entropy	7.731026

Antivirus

AVG	BackDoor.Generic14.ARHX
Ahnlab	Trojan/Win32.Npkon
Avira	BDS/Joanap.A.11
BitDefender	Gen:Variant.Barys.57573
ClamAV	Win.Trojan.Agent-1388737
Cyren	W32/Zegost.AA.gen!Eldorado
ESET	Win32/Scadprv.A trojan
Emsisoft	Gen:Variant.Barys.57573 (B)
F-secure	Gen:Variant.Barys.57573
Filseclab	Worm.Agent.age.ebwv
Ikarus	Worm.Win32.Agent
K7	Backdoor (04c4b9d11)
McAfee	W32/FunCash!worm
Microsoft Security Essentials	Backdoor:Win32/Joanap.J!dha
NANOAV	Trojan.Win32.Agent.crilzb
Quick Heal	Backdoor.Joanap
Sophos	Mal/EncPk-AGS
Symantec	Trojan.Gen.2
Systweak	trojan.agent
TrendMicro	BKDR_JOANAP.AC
TrendMicro House Call	BKDR_JOANAP.AC
Vir.IT eXplorer	Backdoor.Win32.Generic.ARHX
VirusBlokAda	Worm.Agent
Zillya!	Worm.Agent.Win32.3373
nProtect	Worm/W32.Agent.208896.AK

Yara Rules

hidden_cobra_consolidated.yara	rule Enfal_Generic { meta: author = "NCCIC trusted 3rd party" incident = "10135536" date = "2018-04-12" category = "hidden_cobra" family = "BRAMBUL,JOANAP" MD5_1 = "483B95B1498B615A1481345270BFF87D" MD5_2 = "4731CBAEE7ACA37B596E38690160A749" MD5_3 = "CD60FD107BAACCAFA6C24C1478C345C8" MD5_4 = "298775B04A166FF4B8FBD3609E716945" Info = "Detects Hidden Cobra SMB Worm / RAT" strings: $s0 = {6D737373636172647072762E6178} $s1 = {6E34726268726971383930763930 3D3032333D30312A2628542D30513332354A314E3B4C4B} $s2 = {72656468617440676D61696C2E636F6D} $s3 = {6D69737377616E673831303740676D61696C2E636F6D} $s4 = {534232755365435632564474} $s5 = {794159334D6559704275415756426341} $s6 = {705641325941774242347A41346167664B6232614F7A4259} $s7 =

	{AE8591916D586DE4F6FB8EE2F0BBF1F9} $s8 = {F96D5DD36D6D9A87DD6D506D6D6D516D} $s9 = {43616E6E6F74206372656174652072656D6F74652066696C652E} $s10 = {43616E6E6F74206F70656E2072656D6F74652066696C65} $s11 = {663D547D75128D85FCFEFFFF5056} $s12 = {663D547D75128D85FCFEFFFF5056E88C060000E9A9000000663D557D7512} $s13 = {663D567D750F8D85FCFEFFFF5056E891070000EB7C663D577D} $s14 = {3141327A33423479354336783744387739453076244 65F754774487349724A71} $s15 = {393032356A6864686F333965686532} condition: ($s0) or ($s1) or ($s2) or ($s3) or ($s4 and $s5 and $s6) or ($s7 and $s8) or ($s9 and $s10 and $s11) or ($s12 and $s13) or ($s14 and $s15) }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2011-09-14 01:53:24-04:00
Import Hash	e8cd12071a8e823ebc434c8ee3e23203

PE Sections

MD5	Name	Raw Size	Entropy
bf69e0e64bdafa28b31e3c2134e1d696	header	4096	0.658046
27f1df91dc992ababc89460f771a6026	.text	24576	6.227301
249e10a4ad0a58c3db84eb2f69db5db5	.rdata	4096	4.367702
88b5582d4d361c92e9234abf0942ed9e	.data	4096	2.546586
a18b7869b3bfd4a2ef0d03c96fa09221	.rsrc	172032	7.969250

Packers/Compilers/Cryptors

Process List

Process	PID	PPID
077d9e0e12357d27f7f0c336239e961a7049971446f7a3f10268d9439ef67885.exe	2628	(2588)

Relationships

077d9e0e12...	Dropped	a1c483b0ee740291b91b11e18dd05f0a460127acfc19d47b446d11cd0e26d717
077d9e0e12...	Dropped	ea46ed5aed900cd9f01156a1cd446cbb3e10191f9f980e9f710ea1c20440c781

Description

This 32-bit Windows executable file drops two malicious applications.

The first (a1c483b0ee740291b91b11e18dd05f0a460127acfc19d47b446d11cd0e26d717) is a fully functioning RAT.

The second application (ea46ed5aed900cd9f01156a1cd446cbb3e10191f9f980e9f710ea1c20440c781) is a SMB worm that will spread to local subnets and external networks.

a1c483b0ee740291b91b11e18dd05f0a460127acfc19d47b446d11cd0e26d717

Tags

backdoorbottrojanworm

Details

Name	scardprv.dll

Size	77824 bytes
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	4613f51087f01715bf9132c704aea2c2
SHA1	6b1ddf0e63e04146d68cd33b0e18e668b29035c4
SHA256	a1c483b0ee740291b91b11e18dd05f0a460127acfc19d47b446d11cd0e26d717
SHA512	37fa5336d1554557250e4a3bcb4ccfca79f4873264cb161dee340d35a2f8f17f7853fe942809bb343ac1eae0a37122b5e8fd703a9b820ec96abb6
ssdeep	768:qtT2AxNtcgpqLepcy2y6/chYdP8KuSFM+Cs5CBaho9S4AJKqBz8MZdVsrQVBnVGa:qwONtBqL1dDMrs5CN9S4A3HOYBnVL
Entropy	6.138177

Antivirus

AVG	Agent3.BAPF
Ahnlab	Trojan/Win32.Dllbot
Avira	TR/Gendal.6762100
BitDefender	Gen:Variant.Graftor.Elzob.3935
ClamAV	Win.Trojan.Agent-1388765
ESET	a variant of Win32/Scadprv.A trojan
Emsisoft	Gen:Variant.Graftor.Elzob.3935 (B)
F-secure	Gen:Variant.Graftor.Elzob.3935
Filseclab	Worm.Agent.ago.thfj.dll
Ikarus	Worm.Win32.Agent
K7	Trojan (0001659c1)
McAfee	W32/FunCash!worm
Microsoft Security Essentials	Backdoor:Win32/Joanap.B!dha
NANOAV	Trojan.Win32.Agent.cwccco
Quick Heal	Backdoor.Duzzer.A5
Sophos	Mal/Generic-L
Symantec	Backdoor.Joanap
Systweak	malware.gen-20120501
TrendMicro	BKDR_JOANAP.AC
TrendMicro House Call	BKDR_JOANAP.AC
Vir.IT eXplorer	Trojan.Win32.Agent3.BAPF
VirusBlokAda	Worm.Agent
Zillya!	Worm.Agent.Win32.5702
nProtect	Worm/W32.Agent.77824.CJ

Yara Rules

hidden_cobra_consolidated.yara	rule Enfal_Generic { meta: author = "NCCIC trusted 3rd party" incident = "10135536" date = "2018-04-12" category = "hidden_cobra" family = "BRAMBUL,JOANAP" MD5_1 = "483B95B1498B615A1481345270BFF87D" MD5_2 = "4731CBAEE7ACA37B596E38690160A749" MD5_3 = "CD60FD107BAACCAFA6C24C1478C345C8" MD5_4 = "298775B04A166FF4B8FBD3609E716945" Info = "Detects Hidden Cobra SMB Worm / RAT" strings: $s0 = {6D737373636172647072762E6178} $s1 =

	{6E34726268726971383930763 93D3032333D30312A2628542D30513332354A314E3B4C4B} $s2 = {72656468617440676D61696C2E636F6D} $s3 = {6D69737377616E673831303740676D61696C2E636F6D} $s4 = {534232755365435632564474} $s5 = {794159334D6559704275415756426341} $s6 = {705641325941774242347A41346167664B6232614F7A4259} $s7 = {AE8591916D586DE4F6FB8EE2F0BBF1F9} $s8 = {F96D5DD36D6D9A87DD6D506D6D6D516D} $s9 = {43616E6E6F74206372656174652072656D6F74652066696C652E} $s10 = {43616E6E6F74206F70656E2072656D6F74652066696C65} $s11 = {663D547D75128D85FCFEFFFF5056} $s12 = {663D547D75128D85FCFEFFFF5056E88C060000E9A9000000663D557D7512} $s13 = {663D567D750F8D85FCFEFFFF5056E891070000EB7C663D577D} $s14 = {3141327A33423479354336783744387739453076244 65F754774487349724A71} $s15 = {393032356A6864686F333965686532} condition: ($s0) or ($s1) or ($s2) or ($s3) or ($s4 and $s5 and $s6) or ($s7 and $s8) or ($s9 and $s10 and $s11) or ($s12 and $s13) or ($s14 and $s15) }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2011-09-14 01:38:38-04:00
Import Hash	f6f7b2e00921129d18061822197111cd

PE Sections

MD5	Name	Raw Size	Entropy
c745765d5ae0458d76c721b8a82eca52	header	4096	0.763991
f16ff24a6d95e0e0711eccae4283bbe5	.text	40960	6.506011
b89bb8a288d739a27d7021183336413c	.rdata	20480	6.655349
fcd7ede94211c9d653bd8cc776feb8be	.data	4096	4.326483
56dc69f697f36158eefefdde895f39b6	.rsrc	4096	0.613739
20601cf5d6aecb9837dcc1747847c5a2	.reloc	4096	4.068756

Packers/Compilers/Cryptors

Microsoft Visual C++ 6.0 DLL

Relationships

a1c483b0ee...	Dropped_By	077d9e0e12357d27f7f0c336239e961a7049971446f7a3f10268d9439ef67885

Description

This 32-bit Windows DLL is written to disk and then loaded by the file "4731CBAEE7ACA37B596E38690160A749".

This malware has been identified as a RAT, providing a remote actor with the ability to exfiltrate data, drop and run secondary payloads, and provide proxy capabilities on a compromised Windows device. The malware binds to port 443 and listens for incoming connections from a remote operator, using the Rivest Cipher 4 (RC4) encryption algorithm to protect communications with its Command and Control (C2).

The malware also creates a log entry in a file named “mssscardprv.ax”, located in the %WINDIR%\system32 folder. The log entry includes the victim's Internet Protocol (IP) address, host name, and current system time.

ea46ed5aed900cd9f01156a1cd446cbb3e10191f9f980e9f710ea1c20440c781

Tags

backdoorbottrojanworm

Details

Name	Wmmvsvc.dll
Size	91664 bytes
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	e86c2f4fc88918246bf697b6a404c3ea
SHA1	9b7609349a4b9128b9db8f11ac1c77728258862c
SHA256	ea46ed5aed900cd9f01156a1cd446cbb3e10191f9f980e9f710ea1c20440c781
SHA512	f6097c66a526ba7a3c918b1c7fccae03c812046d642a4adb62ee7a24cbcee889c0348020ae7e2e82ee3f284b311f049ed596edb22b90153cadc11
ssdeep	768:9eY/pEwKWcwP/bY4XxlGLup3Tq1LpDLJkDcw3f9zj:MitnU4viJJDw3Z
Entropy	3.156854

Antivirus

AVG	PSW.Generic9.ACQQ
Ahnlab	Trojan/Win32.Dllbot
Avira	BDS/Joanap.A.8
BitDefender	Gen:Variant.Symmi.49274
ClamAV	Win.Trojan.Agent-1388727
Cyren	W32/Trojan.WXKV-0327
ESET	a variant of Win32/Agent.NJF worm
Emsisoft	Gen:Variant.Symmi.49274 (B)
F-secure	Gen:Variant.Symmi.49274
Filseclab	Trojan.Agent.NJF.cuzy.dll
Ikarus	Worm.Win32.Agent
K7	Trojan (00515bda1)
McAfee	Generic PWS.tr
Microsoft Security Essentials	Backdoor:Win32/Joanap.A!dha
NANOAV	Trojan.Win32.Agent.cqilax
NetGate	Trojan.Win32.Malware
Quick Heal	Backdoor.Joanap
Sophos	Mal/Generic-L
Symantec	W32.Brambul
Vir.IT eXplorer	Trojan.Win32.Generic.ACQQ
VirusBlokAda	Worm.Agent
Zillya!	Worm.Agent.Win32.3549
nProtect	Worm/W32.Agent.91664

Yara Rules

hidden_cobra_consolidated.yara	rule Enfal_Generic { meta: author = "NCCIC trusted 3rd party" incident = "10135536" date = "2018-04-12" category = "hidden_cobra" family = "BRAMBUL,JOANAP" MD5_1 = "483B95B1498B615A1481345270BFF87D" MD5_2 = "4731CBAEE7ACA37B596E38690160A749" MD5_3 = "CD60FD107BAACCAFA6C24C1478C345C8" MD5_4 = "298775B04A166FF4B8FBD3609E716945" Info = "Detects Hidden Cobra SMB Worm / RAT"

	strings: $s0 = {6D7373736361726470727 62E6178} $s1 = {6E34726268726971383930763 93D3032333D30312A2628542D30513332354A314E3B4C4B} $s2 = {72656468617440676D61696C2E636F6D} $s3 = {6D69737377616E673831303740676D61696C2E636F6D} $s4 = {534232755365435632564474} $s5 = {794159334D6559704275415756426341} $s6 = {705641325941774242347A41346167664B6232614F7A4259} $s7 = {AE8591916D586DE4F6FB8EE2F0BBF1F9} $s8 = {F96D5DD36D6D9A87DD6D506D6D6D516D} $s9 = {43616E6E6F74206372656174652072656D6F74652066696C652E} $s10 = {43616E6E6F74206F70656E2072656D6F74652066696C65} $s11 = {663D547D75128D85FCFEFFFF5056} $s12 = {663D547D75128D85FCFEFFFF5056E88C060000E9A9000000663D557D7512} $s13 = {663D567D750F8D85FCFEFFFF5056E891070000EB7C663D577D} $s14 = {3141327A33423479354336783744387739453076244 65F754774487349724A71} $s15 = {393032356A6864686F333965686532} condition: ($s0) or ($s1) or ($s2) or ($s3) or ($s4 and $s5 and $s6) or ($s7 and $s8) or ($s9 and $s10 and $s11) or ($s12 and $s13) or ($s14 and $s15) }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2011-09-14 11:42:30-04:00
Import Hash	f0087d7b90876a2769f2229c6789fcf3
Company Name	Microsoft Corporation
File Description	Microsoft XML Encoder/Transcoder
Internal Name	xpsshrm.dll
Legal Copyright	© Microsoft Corporation. All rights reserved.
Original Filename	xpsshrm.dll
Product Name	Microsoft® Windows Media Services
Product Version	9.00.00.4503

PE Sections

MD5	Name	Raw Size	Entropy
037e97300efd533dd48d334d30bdc408	header	4096	0.759334
4b5019185bb0b82273442dae3f15f105	.text	24576	6.083997
9e5a1cfda72f8944cd5e35e33a2a73b0	.rdata	4096	3.267725
47982ac1b20cac03adcfd62f5881b79c	.data	49152	1.087883
b971ab49349a660c70cb6987b7fb3ed3	.rsrc	4096	1.140488
ad5750c9584c0eba32643810ab6e8a53	.reloc	4096	2.515288

Packers/Compilers/Cryptors

Microsoft Visual C++ 6.0 DLL

Relationships

ea46ed5aed...	Dropped_By	077d9e0e12357d27f7f0c336239e961a7049971446f7a3f10268d9439ef67885
ea46ed5aed...	Connected_To	misswang8107@gmail.com
ea46ed5aed...	Contains	redhat@gmail.com

Description

This file is a malicious 32-bit Windows DLL that is written to disk then loaded by the file "4731CBAEE7ACA37B596E38690160A749".

When executed, the DLL attempts to contact all of the Internet Protocol (IP) addresses on the victim's local subnet. If the malware is able to connect to these IP addresses, it will attempt to gain unauthorized access via the SMB protocol on port 445 using a brute-force password attack. The malware contains an embedded password list consisting of commonly used passwords and generates random external IP addresses, which it attempts to attack.

If the malware successfully gains access to another system, it will send an email containing the system's IP address, hostname, username, and password to the following address:

--Begin email address--
misswang8107@gmail.com
--End email address--

The email will appear to be from the following address (Refer to Figure 1):

--Begin email address--
redhat@gmail.com
--End email address--

The malware uses the victim's system folder to create a shared folder named "adnim$" by running the following commands via a remotely run service:

--Begin commands utilized to create SMB share--
cmd.exe /q /c net share adnim$=%SystemRoot%
cmd.exe /q /c net share adnim$=%%SystemRoot%% /GRANT:%s,FULL
--End commands utilized to create SMB share--

The malware will then copy itself to newly created shared folder as a file named "mssscardprv.ax". After copying the malware to the new system it then runs the file on the victim system using a malicious service. The adnim$ share will then be deleted from the remote system using the following command:

--Begin command used to delete share--
'cmd.exe /q /c net share adnim$ /delete'
--End command used to delete share--

The malware determines if Remote Desktop Protocol (RDP) is enabled by attempting to connect to port 3389. If it is able to connect to this port, the malware will report RDP is available on the compromised system. This information is provided to the operator using the malicious email address provided earlier.

This malware can communicate with the RAT identified as "scardprv.dll" (4613f51087f01715bf9132c704aea2c2). The communication is protected with the Rivest Cipher 4 (RC4) encryption protocol. When attempting to propagate, the malware uses the following three usernames combined with a password brute-force attack:

--Begin malicious usernames used by SMB worm--
Administrateur
Administrador
Administrator
--End malicious usernames used by SMB worm--

Although the malware uses numerous embedded passwords in its brute force attacks, within our environment the malware consistently used the following "Lan Manager Response" in its SMB attacks:

--Begin static Lan Manager response--
8C15084FA541079A000000000000000000
--End static Lan Manager response--

This hexadecimal value may be useful in detecting this worm as it communicates over port 445 and attempts to spread. Specifically, when the malware attempts to run a remote service to create the "adnim$" share, the following network traffic is generated:

--Begin network signature--
ASCII: cmd.exe /q /c net share adnim$=%SystemRoot% /GRANT:Administrator,FULL
HEX:
636D642E657865202F71202F63206E6574207368617265206461646E696D243D2553797374656D526F6F7425202F4752414E543A41646D696E6973747
--End network signature--

Screenshots

Figure 1 - The screenshot illustrates the to and from email addresses for data exfiltration.

fe7d35d19af5f5ae2939457a06868754b8bdd022e1ff5bdbe4e7c135c48f9a16

Tags

backdoortrojanworm

Details

Name	298775B04A166FF4B8FBD3609E716945
Size	86016 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	298775b04a166ff4b8fbd3609e716945
SHA1	2e0f666831f64d7383a11b444e2c16b38231f481
SHA256	fe7d35d19af5f5ae2939457a06868754b8bdd022e1ff5bdbe4e7c135c48f9a16
SHA512	adc9bb5a2116134ddf57d1b1765d5981c55828aa8c6719964b0e2eeb6c9068a2acaa98c2e03227a406a4fbfa2f007f5eb9f57a61e3749b8eb0d73
ssdeep	768:i+cDn8nAQ5Toz4c0+u5jrdXs+W+aCNkiC8xeC3cs:i+M8ndTozOn5jxF/US0s
Entropy	2.873816

Antivirus

ClamAV	Win.Trojan.Agent-1388727
ESET	a variant of Win32/Agent.NVC worm
McAfee	GenericRXCB-TI!298775B04A16
Microsoft Security Essentials	Backdoor:Win32/Joanap.A!dha
Symantec	Heur.AdvML.B

Yara Rules

hidden_cobra_consolidated.yara	rule Enfal_Generic { meta: author = "NCCIC trusted 3rd party" incident = "10135536" date = "2018-04-12" category = "hidden_cobra" family = "BRAMBUL,JOANAP" MD5_1 = "483B95B1498B615A1481345270BFF87D" MD5_2 = "4731CBAEE7ACA37B596E38690160A749" MD5_3 = "CD60FD107BAACCAFA6C24C1478C345C8" MD5_4 = "298775B04A166FF4B8FBD3609E716945" Info = "Detects Hidden Cobra SMB Worm / RAT" strings: $s0 = {6D737373636172647072762E6178} $s1 = {6E34726268726971383930763 93D3032333D30312A2628542D30513332354A314E3B4C4B} $s2 = {72656468617440676D61696C2E636F6D} $s3 = {6D69737377616E673831303740676D61696C2E636F6D} $s4 = {53423275536543563256447 4} $s5 = {794159334D6559704275415756426341} $s6 = {7056413259417742423 47A41346167664B6232614F7A4259} $s7 = {AE8591916D586DE4F6FB8EE2F0BBF1F9} $s8 = {F96D5DD36D6D9A87DD6D506D6D6D516D} $s9 = {43616E6E6F74206372656174652072656D6F74652066696C652E} $s10 = {43616E6E6F74206F70656E2072656D6F74652066696C65} $s11 = {663D547D75128D85FCFEFFFF5056} $s12 = {663D547D75128D85FCFEFFFF5056E88C060000E9A9000000663D557D7512} $s13 = {663D567D750F8D85FCFEFFFF5056E891070000EB7C663D577D} $s14 = {3141327A33423479354336783743877394530762446 5F754774487349724A71} $s15 = {393032356A6864686F333965686532} condition: ($s0) or ($s1) or ($s2) or ($s3) or ($s4 and $s5 and $s6) or ($s7 and $s8) or ($s9 and $s10 and $s11) or ($s12 and $s13) or ($s14 and $s15) }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2018-01-05 01:22:45-05:00
Import Hash	9f298eba36baa47b98a60cf36fdb2301

PE Sections

MD5	Name	Raw Size	Entropy
8a5b06109c3bd4323fa3318f9874d529	header	4096	0.703885
413f30d4d86037b75958b45b9efbe1de	.text	20480	6.302858
82b41fefc9aa74a2430f1421fd5fe5b3	.rdata	4096	3.748024
b6f17870ca5f45d4c75e18024e6e1180	.data	53248	1.067897
cda5ef1038742e5ef46b9cfa269b0434	.rsrc	4096	0.608792

Packers/Compilers/Cryptors

Microsoft Visual C++ v6.0

Process List

Process	PID	PPID
fe7d35d19af5f5ae2939457a06868754b8bdd022e1ff5bdbe4e7c135c48f9a16.exe	2436	(2408)

Description

This file is a malicious 32-bit Windows executable file designed to scan the local network and the Internet for machines that are accessible and have open SMB ports. Once the malware gains access to a remote machine, it will deliver a malicious payload. This file accepts the following command-line arguments for execution:

--Begin arguments--
-i ==> Create service
-u ==> Control and delete service
-s ==> Start service
-r ==> Run not as a service
-k ==> ControlService
--End arguments--

When executed with the "-i" argument, the malware installs and executes itself as the following service:

--Begin service information--
ServiceName = "RdpCertification"
DisplayName = "Remote Desktop Certification Services"
DesiredAccess = SERVICE_ALL_ACCESS
ServiceType = SERVICE_WIN32_OWN_PROCESS|SERVICE_INTERACTIVE_PROCESS
StartType = SERVICE_AUTO_START
BinaryPathName = "%current directory%\298775B04A166FF4B8FBD3609E716945.exe"
--End service information--

The malware creates a mutual exclusion (Mutex) object named "PlatFormSDK20150201", then generates a list of IP addresses using a domain generation algorithm (DGA). The DGA uses the system time in the algorithm to create the list of IP addresses.

It generates network traffic over Transmission Control Protocol (TCP) ports 80 and 445 via the victims' IP addresses and the generated IP addresses.

Sample HTTP request:

--Begin HTTP request--
OPTIONS / HTTP/1.1
translate: f
User-Agent: Microsoft-WebDAV-MiniRedir/5.1.2600
Host: 159.154.100.0

Content-Length: 0
Connection: Keep-Alive
--End HTTP request--

Once successfully connected to other Windows hosts or the generated IP addresses using port 445, the malware attempts to use a hard-coded list of passwords for SMB connections. If the password is correctly guessed, a file share is established. The malware uses the following methods to access shares on the remote systems:

To gain access to remote systems it uses ($IPC) share via “\\remote system IP\$IPC”
It checks for existing shares by using “\\hostname\adnim$\system32”

It will create a new share named "adnim$" using the following command:

--Begin new share command--
“cmd.exe /q /c net share adnim$=%SystemRoot%”
“cmd.exe /q /c net share adnim$=%%SystemRoot%% /GRANT:%s,FULL”
--End new share command—

Once a file share is successfully established, the malware uploads a copy of a payload "C:\WINDOWS\TEMP\TMP1.tmp" and installs it as a service. The malware payload that is uploaded and then run on the newly infected host was not available at the time of analysis.

The remote network share is removed after infection using the following command:

--Begin command--
“cmd.exe /q /c net share adnim$ /delete”
--End command--

Once the payload has been uploaded and executed, the malware uses Simple Mail Transfer Protocol (SMTP) to send collected data. The data provides infection status to a remote operator.

Displayed below are the domain names of the service providers used to send data:

--Begin SMTP domain information--
"www.hotmail.com"
--End SMTP domain information--

Displayed is the structure of the email sent:

--Begin email structure format--
SUBJECT: %s%s%s
TO: Joana <%s>%s
FROM: <%s>%s
DATA%s
RCPT TO: <%s>%s
MAIL FROM: <%s>%s
AUTH LOGIN%s
HELO %s%s
--End email structure format--

Displayed is a list of brute force passwords used to establish connections:

--Begin brute force password--
!@#$
!@#$%
!@#$%^
!@#$%^&
!@#$%^&*
!@#$%^&*()
"KGS!@#$%"
0000
00000
000000
00000000
1111
11111
111111
11111111
11122212

1212
121212
123123
123321
1234
12345
123456
1234567
12345678
123456789
123456^%$#@!
1234qwer
123abc
123asd
123qwe
1313
1q2w3e
1q2w3e4r
1qaz2wsx
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
4321
54321
654321
6969
666666
7777
8888
88888
888888
8888888
88888888
Admin
abc123
abc@123
abcd
admin
admin123
admin!23
admin!@#
administrator
administrador
asdf
asdfg
asdfgh
asdf123
asdf!23
baseball
backup
blank
cisco
compaq
control
computer
cookie123
database

dbpassword
db1234
default
dell
enable
fish
foobar
gateway
guest
golf
harley
home
iloveyou
internet
letmein
Login
login
love
manager
oracle
owner
pass
passwd
password
p@ssword
password1
password!
passw0rd
Password1
pa55w0rd
pw123
q1w2e3
q1w2e3r4
q1w2e3r4t5
q1w2e3r4t5y6
qazwsx
qazwsxedc
qwer
qwert
qwerty
!QAZxsw2
root
secret
server
sqlexec
shadow
super
sybase
temp
temp123
test
test!
test1
test123
test!23
winxp
win2000
win2003
Welcome1
Welcome123
xxxx
yxcv
zxcv
Administrator

Admin
--End brute force password--

redhat@gmail.com

Details

Address	redhat@gmail.com

Relationships

redhat@gmail.com	Contained_Within	ea46ed5aed900cd9f01156a1cd446cbb3e10191f9f980e9f710ea1c20440c781

misswang8107@gmail.com

Details

Address	misswang8107@gmail.com

Relationships

misswang8107@gmail.com	Connected_From	ea46ed5aed900cd9f01156a1cd446cbb3e10191f9f980e9f710ea1c20440c781

Relationship Summary

077d9e0e12...	Dropped	a1c483b0ee740291b91b11e18dd05f0a460127acfc19d47b446d11cd0e26d717
077d9e0e12...	Dropped	ea46ed5aed900cd9f01156a1cd446cbb3e10191f9f980e9f710ea1c20440c781
a1c483b0ee...	Dropped_By	077d9e0e12357d27f7f0c336239e961a7049971446f7a3f10268d9439ef67885
ea46ed5aed...	Dropped_By	077d9e0e12357d27f7f0c336239e961a7049971446f7a3f10268d9439ef67885
ea46ed5aed...	Connected_To	misswang8107@gmail.com
ea46ed5aed...	Contains	redhat@gmail.com
redhat@gmail.com	Contained_Within	ea46ed5aed900cd9f01156a1cd446cbb3e10191f9f980e9f710ea1c20440c781
misswang8107@gmail.com	Connected_From	ea46ed5aed900cd9f01156a1cd446cbb3e10191f9f980e9f710ea1c20440c781

Recommendations

CISA would like to remind users and administrators to consider using the following best practices to strengthen the security posture of their organization's systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- 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.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- 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 and implement appropriate ACLs.

Additional information on malware incident prevention and handling can be found in NIST's Special Publication 800-83, **Guide to Malware Incident Prevention & Handling for Desktops and Laptops.**

Contact Information

Document FAQ

What is a MAR? A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manual reverse engineering. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to CISA at 1-844-Say-CISA or contact@mail.cisa.dhs.gov.

Can I submit malware to CISA? Malware samples can be submitted via three methods:

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

CISA 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 the CISA/US-CERT homepage at www.us-cert.gov.
