MAR-10301706-1.v1 - North Korean Remote Access Tool: ECCENTRICBANDWAGON

Notification

Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts between the Department of Homeland Security (DHS), the Federal Bureau of and the Department of Defense (DoD). Working with U.S. Government partners, DHS, FBI, and DoD identified Remote Access Tool (RAT) malwa the North Korean government. This malware variant has been identified as ECCENTRICBANDWAGON. The U.S. Government refers to malicious North Korean government as HIDDEN COBRA. For more information on HIDDEN COBRA activity, visit https[:]//www[.]us-cert.gov/hiddencobra.

FBI has high confidence that HIDDEN COBRA actors are using malware variants in conjunction with proxy servers to maintain a presence on vict further network exploitation. DHS, FBI, and DoD are distributing this MAR to enable network defense and reduce exposure to North Korean gover cyber activity.

This MAR includes malware descriptions related to HIDDEN COBRA, suggested response actions and recommended mitigation techniques. Use should flag activity associated with the malware and report the activity to the Cybersecurity and Infrastructure Security Agency (CISA) or the FBI C (CyWatch), and give the activity the highest priority for enhanced mitigation.

This report looks at malware samples known as ECCENTRICBANDWAGON. This family of malware is used as a reconnaissance tool. The samp used for keylogging and screen capture functionality. The samples are very similar, but differ slightly in the location that they store the key logs an variants have RC4 encrypted strings within the executable and conduct a simple, ineffective cleanup, whereas others do not.
For a downloadable copy of IOCs, see MAR-10301706-1.v1.stix.

Submitted Files (4)

32a4de070ca005d35a88503717157b0dc3f2e8da76ffd618fca6563aec9c81f8 (PSLogger .dll)

9ea5aa00e0a738b74066c61b1d35331170a9e0a84df1cc6cef58fd46a8ec5a2e (PSLogger .dll)

c6930e298bba86c01d0fe2c8262c46b4fce97c6c5037a193904cfc634246fbec (PSLogger .dll)

efd470cfa90b918e5d558e5c8c3821343af06eedfd484dfeb20c4605f9bdc30e (PSLogger .dll)

Findings

efd470cfa90b918e5d558e5c8c3821343af06eedfd484dfeb20c4605f9bdc30e

Tags

HIDDEN-COBRAbackdoorkeyloggerreconnaissancescreen-capturespywaretrojan

Details

Name	PSLogger .dll
Size	138240 bytes
Type	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
MD5	d45931632ed9e11476325189ccb6b530
SHA1	081d5bd155916f8a7236c1ea2148513c0c2c9a33
SHA256	efd470cfa90b918e5d558e5c8c3821343af06eedfd484dfeb20c4605f9bdc30e
SHA512	fd1b7ea95f66a660e9183c22755ac7d741823ba45a009bf9929546213308f89fd9ce8fcc2e70b56e427f0daa1b0965817d45dd9c2f5598
ssdeep	3072:t+N02CVLOJdCPQhVNRTzcb/YrgHdnG6ioaa5IR:sO2qO3CPkRTz8YrgHdGBoa1
Entropy	6.096739

Antivirus

Ahnlab	Trojan/Win64.Agent
Antiy	Trojan[Spy]/Win64.Agent

Avira	TR/Spy.Agent.ftmjo
BitDefender	Trojan.GenericKD.40337042
Cyren	W64/Trojan.WFEO-4014
ESET	a variant of Win64/Spy.Agent.AP trojan
Emsisoft	Trojan.GenericKD.40337042 (B)
Filseclab	W64.Spy.Agent.AP.feaw
Ikarus	Trojan-Spy.Win64.Agent
K7	Spyware (00538f7c1)
Lavasoft	Trojan.GenericKD.40337042
McAfee	RDN/Generic PWS.nq
Microsoft Security Essentials	Trojan:Win32/Tiggre!plock
NANOAV	Trojan.Win64.Mlw.fgbvfi
NetGate	Trojan.Win32.Malware
Sophos	Troj/Spy-AUK
Symantec	Trojan.Crobaruko
Systweak	malware.agent
TrendMicro	TSPY64_.F7315F7E
TrendMicro House Call	TSPY64_.F7315F7E
Vir.IT eXplorer	Backdoor.Win32.Lazarus.BGM
VirusBlokAda	TrojanSpy.Win64.Agent
Zillya!	Trojan.Agent.Win64.2215

YARA Rules

```
rule CISA_3P_10301706_01 : HiddenCobra ECCENTRICBANDWAGON backdoor keylogger reconnaissance screencapture spyware trojar
{
  meta:
    Author = "CISA Trusted Third Party"
    Incident = "10301706.r1.v1"
    Date = "2020-08-11"
    Actor = "Hidden Cobra"
    Category = "Backdoor Keylogger Reconnaissance Screen-Capture Spyware Trojan"
    Family = "ECCENTRICBANDWAGON"
    Description = "Detects strings in ECCENTRICBANDWAGON proxy tool"
    MD5_1 = "d45931632ed9e11476325189ccb6b530"
    SHA256_1 = "efd470cfa90b918e5d558e5c8c3821343af06eedfd484dfeb20c4605f9bdc30e"
    MD5_2 = "acd15f4393e96fe5eb920727dc083aed"
    SHA256_2 = "32a4de070ca005d35a88503717157b0dc3f2e8da76ffd618fca6563aec9c81f8"
    MD5_3 = "34404a3fb9804977c6ab86cb991fb130"
    SHA256_3 = "c6930e298bba86c01d0fe2c8262c46b4fce97c6c5037a193904cfc634246fbec"
    MD5_4 = "3122b0130f5135b6f76fca99609d5cbe"
    SHA256_4 = "9ea5aa00e0a738b74066c61b1d35331170a9e0a84df1cc6cef58fd46a8ec5a2e"
  strings:
    $sn1 = { FB 19 9D 57 [1-6] 9A D1 D6 D1 [1-6] 42 9E D8 FD }
    $sn2 = { 4F 03 43 83 [1-6] 48 E0 1A 2E [1-6] 3B FD FD FD }
    $sn3 = { 68 56 68 9A [1-12] 4D E1 1F 25 [1-12] 3F 38 54 0F [1-12] 73 30 62 A1 [1-12] DB 39 BD 56 }
    $sn4 = "%s\\chromeupdater_ps_%04d%02d%02d_%02d%02d%02d_%03d_%d" wide ascii nocase
    $sn5 = "c:\\windows\\temp\\TMP0389A.tmp" wide ascii nocase
  condition:
    any of them
}
```

ssdeep Matches

100 32a4de070ca005d35a88503717157b0dc3f2e8da76ffd618fca6563aec9c81f8

PE Metadata

Compile Date	2018-04-27 22:53:06-04:00
Import Hash	f0faa229b086ea5053b4268855f0c8ba

PE Sections

MD5	Name	Raw Size	Entropy
09745305cbad67b17346f0f6dba1e700	header	1024	2.729080
5c2242b56a31d64b6ce82671d97a82a4	.text	92160	6.415763
0d022eff24bc601d97d2088b4179bd18	.rdata	31232	4.934652
578e5078ccb878f1aa9e309b4cfc2be5	.data	6144	2.115729
09924946b47ef078f7e9af4f4fcb59dc	.pdata	5632	4.803615
7ead0113095bc6cb3b2d82f05fda25f3	.rsrc	512	5.115767
7937397e0a31cdc87f5b79074825e18e	.reloc	1536	2.931043

Description

This file is a 64-bit dynamic link library (DLL). This malware uses 3 files that will be used to store the key logs, screen shots, and log intervals. The logs can be found in C:\windows\temp\TMP0389A.tmp.

--Begin Log Files--
1. Keylog: %temp%\GoogleChrome\chromeupdate_pk
2. Screenshots: %temp%\GoogleChrome\chromeupdate_ps_<YYYMMDD>_<HHMMSS>_<sss>_<ThreadID>
3. Log intervals: C:\ProgramData\2.dat
--End Log Files--

The malware creates 3 threads to populate the log files listed above. Each one will continue to execute until a global kill variable is set to 1. This v set to 1 by calling an export called “Process” from within this DLL. When the export is called, the threads will return and the program will exit.
32a4de070ca005d35a88503717157b0dc3f2e8da76ffd618fca6563aec9c81f8

Tags

HIDDEN-COBRAbackdoorkeyloggerreconnaissancescreen-capturespywaretrojan

Details

Name	PSLogger .dll
Size	138243 bytes
Type	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
MD5	acd15f4393e96fe5eb920727dc083aed
SHA1	c92529097cad8996f3a3c8eb34b56273c29bdce5
SHA256	32a4de070ca005d35a88503717157b0dc3f2e8da76ffd618fca6563aec9c81f8
SHA512	82a946c2d0c9fffdd23d8e6b34028ac1b0368d4fd78302268aa4d954bead8a82ea15873a28d69946dceaf80fcafd0c52aeb59f47df5a029
ssdeep	3072:t+N02CVLOJdCPQhVNRTzcb/YrgHdnG6ioaa5IR:sO2qO3CPkRTz8YrgHdGBoa1
Entropy	6.096652

Antivirus

Ahnlab	Trojan/Win64.Agent
Antiy	Trojan[Spy]/Win64.Agent
Avira	TR/Spy.Agent.ftmjo
BitDefender	Trojan.GenericKD.40337042
Comodo	Malware
Cyren	W64/Trojan.WFEO-4014
ESET	a variant of Win64/Spy.Agent.AP trojan
Emsisoft	Trojan.GenericKD.40337042 (B)

Ikarus	Trojan-Spy.Win64.Agent
K7	Spyware (00538f7c1)
Lavasoft	Trojan.GenericKD.40337042
Microsoft Security Essentials	Trojan:Win32/Tiggre!plock
NANOAV	Trojan.Win64.Mlw.fgbtfv
Symantec	Trojan.Crobaruko
Systweak	malware.agent
Vir.IT eXplorer	Backdoor.Win32.Lazarus.BGM
VirusBlokAda	TrojanSpy.Win64.Agent
Zillya!	Trojan.Agent.Win64.2215

YARA Rules

```
rule CISA_3P_10301706_01 : HiddenCobra ECCENTRICBANDWAGON backdoor keylogger reconnaissance screencapture spyware trojar
{
  meta:
    Author = "CISA Trusted Third Party"
    Incident = "10301706.r1.v1"
    Date = "2020-08-11"
    Actor = "Hidden Cobra"
    Category = "Backdoor Keylogger Reconnaissance Screen-Capture Spyware Trojan"
    Family = "ECCENTRICBANDWAGON"
    Description = "Detects strings in ECCENTRICBANDWAGON proxy tool"
    MD5_1 = "d45931632ed9e11476325189ccb6b530"
    SHA256_1 = "efd470cfa90b918e5d558e5c8c3821343af06eedfd484dfeb20c4605f9bdc30e"
    MD5_2 = "acd15f4393e96fe5eb920727dc083aed"
    SHA256_2 = "32a4de070ca005d35a885037171570b0dc3f2e8da76ffd618fca6563aec9c81f8"
    MD5_3 = "34404a3fb9804977c6ab86cb991fb130"
    SHA256_3 = "c6930e298bba86c01d0fe2c8262c46b4fce97c6c5037a193904cfc634246fbec"
    MD5_4 = "3122b0130f5135b6f76fca99609d5cbe"
    SHA256_4 = "9ea5aa00e0a738b74066c61b1d35331170a9e0a84df1cc6cef58fd46a8ec5a2e"
  strings:
    $sn1 = { FB 19 9D 57 [1-6] 9A D1 D6 D1 [1-6] 42 9E D8 FD }
    $sn2 = { 4F 03 43 83 [1-6] 48 E0 1A 2E [1-6] 3B FD FD FD }
    $sn3 = { 68 56 68 9A [1-12] 4D E1 1F 25 [1-12] 3F 38 54 0F [1-12] 73 30 62 A1 [1-12] DB 39 BD 56 }
    $sn4 = "%s\\chromeupdater_ps_%04d%02d%02d_%02d%02d%02d_%03d_%d" wide ascii nocase
    $sn5 = "c:\\windows\\temp\\TMP0389A.tmp" wide ascii nocase
  condition:
    any of them
}
```

ssdeep Matches

100 efd470cfa90b918e5d558e5c8c3821343af06eedfd484dfeb20c4605f9bdc30e

PE Metadata

Compile Date	2018-04-27 22:53:06-04:00
Import Hash	f0faa229b086ea5053b4268855f0c8ba

PE Sections

MD5	Name	Raw Size	Entropy
09745305cbad67b17346f0f6dba1e700	header	1024	2.729080
5c2242b56a31d64b6ce82671d97a82a4	.text	92160	6.415763
0d022eff24bc601d97d2088b4179bd18	.rdata	31232	4.934652
578e5078ccb878f1aa9e309b4cfc2be5	.data	6144	2.115729
09924946b47ef078f7e9af4f4fcb59dc	.pdata	5632	4.803615
7ead0113095bc6cb3b2d82f05fda25f3	.rsrc	512	5.115767
7937397e0a31cdc87f5b79074825e18e	.reloc	1536	2.931043

Description

This file is a 64-bit DLL. This sample and "efd470cfa90b918e5d558e5c8c3821343af06eedfd484dfeb20c4605f9bdc30e" are nearly identical with tl being that this sample has 3 extra NULL bytes at the end of the file.

This malware uses 3 files that will be used to store the key logs, screen shots, and log intervals. The location of these logs can be found in C:\windows\temp\TMP0389A.tmp.

--Begin Log Files--
1. Keylog: %temp%\GoogleChrome\chromeupdate_pk
2. Screenshots: %temp%\GoogleChrome\chromeupdate_ps_<YYYMMDD>_<HHMMSS>_<sss>_<ThreadID>
3. Log intervals: C:\ProgramData\2.dat
--End Log Files--

The malware creates 3 threads to populate the log files listed above. Each one will continue to execute until a global kill variable is set to 1. This v set to 1 by calling an export called “Process” from within this DLL. When the export is called, the threads will return and the program will exit.
c6930e298bba86c01d0fe2c8262c46b4fce97c6c5037a193904cfc634246fbec

Tags

HIDDEN-COBRAbackdoorkeyloggerreconnaissancescreen-capturetrojan

Details

Name	PSLogger .dll
Size	175104 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	34404a3fb9804977c6ab86cb991fb130
SHA1	b345e6fae155bfaf79c67b38cf488bb17d5be56d
SHA256	c6930e298bba86c01d0fe2c8262c46b4fce97c6c5037a193904cfc634246fbec
SHA512	01a8c8b66f6895387c6a347d02d00ea09619888f2727096a19d4c4ff50e6bf72367cbd41f09e89a57f7f3862efbb2db8177dbec086c4ce2
ssdeep	3072:AeO51bvWZElWhKQGhvNdx2GYZj+utNfBtZl7mGwwZWyNGVxBqu:A77beClWhKQG36UutNfB077Bqu
Entropy	6.491987

Antivirus

Ahnlab	Malware/Gen.Generic
Antiy	GrayWare/Win32.Presenoker
BitDefender	Trojan.GenericKD.43188225
Cyren	W32/Trojan.MZDN-2436
ESET	a variant of Generik.HKZTFCG trojan
Emsisoft	Trojan.GenericKD.43188225 (B)
Ikarus	Trojan.SuspectCRC
K7	Trojan (005506c81)
Lavasoft	Trojan.GenericKD.43188225
NANOAV	Trojan.Win32.KeyLogger.fnwztc
NetGate	Malware.Generic
Symantec	Hacktool.Keylogger
Vir.IT eXplorer	Backdoor.Win32.Lazarus.BGM
VirusBlokAda	TrojanSpy.Keylogger
Zillya!	Trojan.Keylogger.Win32.9

YARA Rules

```
rule CISA_3P_10301706_01 : HiddenCobra ECCENTRICBANDWAGON backdoor keylogger reconnaissance screencapture spyware trojar
{
  meta:
    Author = "CISA Trusted Third Party"
    Incident = "10301706.r1.v1"
    Date = "2020-08-11"
    Actor = "Hidden Cobra"
    Category = "Backdoor Keylogger Reconnaissance Screen-Capture Spyware Trojan"
    Family = "ECCENTRICBANDWAGON"
    Description = "Detects strings in ECCENTRICBANDWAGON proxy tool"
    MD5_1 = "d45931632ed9e11476325189ccb6b530"
    SHA256_1 = "efd470cfa90b918e5d558e5c8c3821343af06eedfd484dfeb20c4605f9bdc30e"
    MD5_2 = "acd15f4393e96fe5eb920727dc083aed"
    SHA256_2 = "32a4de070ca005d35a88503717157b0dc3f2e8da76ffd618fca6563aec9c81f8"
    MD5_3 = "34404a3fb9804977c6ab86cb991fb130"
    SHA256_3 = "c6930e298bba86c01d0fe2c8262c46b4fce97c6c5037a193904cfc634246fbec"
    MD5_4 = "3122b0130f5135b6f76fca99609d5cbe"
    SHA256_4 = "9ea5aa00e0a738b74066c61b1d35331170a9e0a84df1cc6cef58fd46a8ec5a2e"
  strings:
    $sn1 = { FB 19 9D 57 [1-6] 9A D1 D6 D1 [1-6] 42 9E D8 FD }
    $sn2 = { 4F 03 43 83 [1-6] 48 E0 1A 2E [1-6] 3B FD FD FD }
    $sn3 = { 68 56 68 9A [1-12] 4D E1 1F 25 [1-12] 3F 38 54 0F [1-12] 73 30 62 A1 [1-12] DB 39 BD 56 }
    $sn4 = "%s\\chromeupdater_ps_%04d%02d%02d_%02d%02d%02d_%03d_%d" wide ascii nocase
    $sn5 = "c:\\windows\\temp\\TMP0389A.tmp" wide ascii nocase
  condition:
    any of them
}
```

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2018-11-14 09:44:18-05:00
Import Hash	a8623b2da60776df129ebe0430d48d85

PE Sections

MD5	Name	Raw Size	Entropy
37ecb293f01edad89fcee1ce48e4cde3	header	1024	2.949326
36fd9d805b7c591ab71eda922662e30a	.text	124928	6.650973
1d3132305f18961b86c1fda0a2f4eea9	.rdata	38912	5.166660
9e17ac76df46fd523a11378398cf026f	.data	3072	2.367308
bbee55723eaad8c7f73a5fa9bf2159d4	.gfids	512	2.275750
264e317304c9b21a342169b33c0a791a	.rsrc	512	4.717679
a1ab3dce319437b49198eeff43f4d847	.reloc	6144	6.422499

Packers/Compilers/Cryptors

Microsoft Visual C++ ?.?

Description

This sample is nearly identical to "efd470cfa90b918e5d558e5c8c3821343af06eedfd484dfeb20c4605f9bdc30e" with the exception that this sampl some of its strings and use different log files.

The following strings are RC4 encrypted with the key “key”:

--Begin RC4 encrypted strings--
Downloads
c:\windows\temp\TMP0389A.tmp
c:\windows\temp\tmp1105.tmp
[CLIPBOARD]
[/CLIPBOARD]
--End RC4 encrypted strings--

This malware uses 3 files that will be used to store the key logs, screen shots, and log intervals. The location of these logs can be found in C:\windows\temp\TMP0389A.tmp.

--Begin log files--
1. Keylog: %temp%\Downloads\tmp_<USERNAME>
2. Screenshots: %temp%\Downloads\tmp_<USERNAME>_<MMDD>_<HHMMSS>
3. Log intervals: c:\windows\temp\tmp1105.tmp
--End log files--

The malware creates 3 threads to populate the log files listed above. Each one will continue to execute until a global kill variable is set to 1. This v
set to 1 by calling an export called “Process” from within this DLL. When the export is called, the threads will return and the program will exit.
9ea5aa00e0a738b74066c61b1d35331170a9e0a84df1cc6cef58fd46a8ec5a2e

Tags

HIDDEN-COBRAkeyloggerreconnaissancescreen-capturespywaretrojan

Details

Name	PSLogger .dll
Size	210944 bytes
Type	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
MD5	3122b0130f5135b6f76fca99609d5cbe
SHA1	ce6bc34b887d60f6d416a05d5346504c54cff030
SHA256	9ea5aa00e0a738b74066c61b1d35331170a9e0a84df1cc6cef58fd46a8ec5a2e
SHA512	788c666efeb664c7691a958d15eac2b80d3d17241f5e7c131e5dec2f761bcb70950018c1f8a85fd6600eff0d0fab0ce31fbcd364d16b6ef8
ssdeep	3072:6usGRlrmZ8LP/LqdmpWOY9Y9EbyBFWnqD5W3P4Tp31oItN7W0rVu6eRDP/fJkkj7:67GTjOdCWOKXbyCnCEQTp2CE0/gh2W
Entropy	6.246368

Antivirus

Ahnlab	Trojan/Win64.Redbanc
Antiy	Trojan[Banker]/Win32.Alreay
Avira	TR/Spy.Agent.kdvkr
BitDefender	Trojan.GenericKD.41368668
ESET	a variant of Win64/Spy.Agent.BG trojan
Emsisoft	Trojan.GenericKD.41368668 (B)
Ikarus	Trojan-Spy.Keylogger.Lazarus
K7	Spyware (005501401)
Lavasoft	Trojan.GenericKD.41368668
McAfee	RDN/Generic PWS.tf
NANOAV	Trojan.Win64.Alreay.hoqvyj
Quick Heal	Trojan.Alreay
Sophos	Troj/Alreay-A
TACHYON	Unknown-Type/Alreay.210944
Zillya!	Trojan.Alreay.Win32.91

YARA Rules

```
rule CISA_3P_10301706_01 : HiddenCobra ECCENTRICBANDWAGON backdoor keylogger reconnaissance screencapture spyware trojar
{
  meta:
    Author = "CISA Trusted Third Party"
    Incident = "10301706.r1.v1"
    Date = "2020-08-11"
    Actor = "Hidden Cobra"
    Category = "Backdoor Keylogger Reconnaissance Screen-Capture Spyware Trojan"
    Family = "ECCENTRICBANDWAGON"
    Description = "Detects strings in ECCENTRICBANDWAGON proxy tool"
    MD5_1 = "d45931632ed9e11476325189ccb6b530"
    SHA256_1 = "efd470cfa90b918e5d558e5c8c3821343af06eedfd484dfeb20c4605f9bdc30e"
    MD5_2 = "acd15f4393e96fe5eb920727dc083aed"
    SHA256_2 = "32a4de070ca005d35a88503717157b0dc3f2e8da76ffd618fca6563aec9c81f8"
    MD5_3 = "34404a3fb9804977c6ab86cb991fb130"
    SHA256_3 = "c6930e298bba86c01d0fe2c8262c46b4fce97c6c5037a193904cfc634246fbec"
    MD5_4 = "3122b0130f5135b6f76fca99609d5cbe"
    SHA256_4 = "9ea5aa00e0a738b74066c61b1d35331170a9e0a84df1cc6cef58fd46a8ec5a2e"
  strings:
    $sn1 = { FB 19 9D 57 [1-6] 9A D1 D6 D1 [1-6] 42 9E D8 FD }
    $sn2 = { 4F 03 43 83 [1-6] 48 E0 1A 2E [1-6] 3B FD FD FD }
    $sn3 = { 68 56 68 9A [1-12] 4D E1 1F 25 [1-12] 3F 38 54 0F [1-12] 73 30 62 A1 [1-12] DB 39 BD 56 }
    $sn4 = "%s\\chromeupdater_ps_%04d%02d%02d_%02d%02d%02d_%03d_%d" wide ascii nocase
    $sn5 = "c:\\windows\\temp\\TMP0389A.tmp" wide ascii nocase
  condition:
    any of them
}
```

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2019-04-08 07:26:25-04:00
Import Hash	b113cba285f3c4ed179422f54692f4e3

PE Sections

MD5	Name	Raw Size	Entropy
fd81e5f6ab156dcdba2e2b92826ca192	header	1024	3.015020
88ecd4fac45e45b294de415ca514a93c	.text	137728	6.457660
af0dab081123c1ad835c86f134138e7f	.rdata	57344	5.118317
e7c661026f7ecf701bbcbdd15ff2b825	.data	3584	2.244033
4b406030a4a3dcaea845c14124010691	.pdata	8192	5.172064
f623a10ca467aac404ec6fda8e4810d4	.gfids	512	2.000422
3695113543a23c53791caa70b4bd8874	.rsrc	512	4.724729
f9f31f1689409c8834b7f0c28d948a65	.reloc	2048	4.924204

Description

This sample is nearly identical to "c6930e298bba86c01d0fe2c8262c46b4fce97c6c5037a193904cfc634246fbec" with the exception that it RC4 en strings, uses different log files, and has a simple cleanup routine.

The following strings are RC4 encrypted with the key “key”:

--Begin RC4 encrypted strings--
TrendMicroUpdate
c:\windows\temp\TMP0389A.tmp
c:\windows\temp\tmp1105.tmp
[CLIPBOARD]
[/CLIPBOARD]
--End RC4 encrypted strings--

This malware uses 3 files that will be used to store the key logs, screen shots, and log intervals. The location of these logs can be found in C:\windows\temp\TMP0389A.tmp.

--Begin log files--
1. Keylog: %temp%\TrendMicroUpdate\update_<USERNAME>
2. Screenshots: %temp%\TrendMicroUpdate\update_<MMDD>_<HHMMSSI>

3. Log Intervals: c:\windows\temp\tmp1105.tmp
--End log files--

This malware creates 3 threads to populate the log files listed above. Each one will continue to execute until the file C:\windows\temp\tmp0207 co particular location. At this point, the program will signal an exit to the other threads and begin a cleanup thread. The cleanup thread will delete C:\windows\temp\tmp0207 and then call WinExec(cmd.exe /c taskkill /f /im explorer.exe). This will crash explorer.exe, which could potentially alert using the device at the time.

Recommendations

CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organizatio 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 unl
- 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
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology (NIST) Specia **"Guide to Malware Incident Prevention & Handling for Desktops and Laptops".**

Contact Information

CISA continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at t https://www.cisa.gov/forms/feedback/

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most will provide initial indicators for computer and network defense. To request additional analysis, please contact CISA and provide information regar desired analysis.

What is a MAR? A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manua 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 CISA at 1-888-282-0870 or CISA Service Desk.

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 ph Reporting forms can be found on CISA's homepage at www.cisa.gov.

Revisions

August 26, 2020: Initial Version

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.