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

Malware Analysis Report (MAR) - 10135536-A

2017-11-01

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distr buted without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

Summary

Description

This submission included two PE files. These files allow a remote operator or a server to perform various remote operations.

Files

Processed	2 1216da2b3d6e64075e8434be1058de06 (1216DA2B3D6E64075E8434BE1058DE06) e48fe20eb1f5a5887f2ac631fed9ed63 (E48FE20EB1F5A5887F2AC631FED9ED63)

IPs

Identified	3 10.10.30.110 175.100.189.174 125.212.132.222

Files

E48FE20EB1F5A5887F2AC631FED9ED63

Details	
Name	E48FE20EB1F5A5887F2AC631FED9ED63
Size	94208
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	e48fe20eb1f5a5887f2ac631fed9ed63
SHA1	f83f30bd284074d1daaf2e262a280ca780791f2c
ssdeep	1536:qJhDLw1yDhhzoN/e/C/O/C/a/D/I26251K06Zk/XrqqitM4NvL:qvfw1ahEVOS+Sq7IN251ikzq5tM4NvL
Entropy	5.49321665686

Antivirus	
McAfee	RDN/Generic BackDoor
K7	Trojan (004f5bbb1)
F-secure	Trojan.Generic.20336523
Cyren	W32/Trojan.CYVO-5810
Symantec	Backdoor.Destover!gen2
VirusBlokAda	Backdoor.Agent
Zillya!	Trojan.Agent.Win32.751098
Kaspersky	Backdoor.Win32.Agent.dpfu
BitDefender	Trojan.Generic.20336523
TrendMicro House Call	BKDR_DE.AF7FD435
TrendMicro	BKDR_DE.AF7FD435
Emsisoft	Trojan.Generic.20336523 (B)
Avira	TR/Agent.oohzt
Ahnlab	Win-Trojan/Hwdoor.Gen
NANOAV	Trojan.Win32.Agent.ekrztl
Quick Heal	Trojan.Skeeyah
Ikarus	Trojan.Win32.Agent
AVG	Agent5.AWXL

PE Information	
Compiled	2016-03-30T04:26:15Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	9c58c3fe5f463b33e9d2bc488bf4ae82	4096	0.679032290586
.text	5e856b2016485f5d844d07ebc461690c	61440	6.61326217629
.rdata	063ef94aa302b3de760bbf4ce2f3ef9d	8192	4.01399640315
.data	59ad2089dfe1a9456b4b456e62933a32	16384	1.37171881187
.rsrc	3e47af504a67377daffd633c5ee43c50	4096	1.66535231443

Packers

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

Relationships

(F) E48FE20EB1F5A5887F2AC631FED9ED63 (e48fe)	Connected_To	(I) 10.10.30.110
(F) E48FE20EB1F5A5887F2AC631FED9ED63 (e48fe)	Connected_To	(I) 175.100.189.174
(F) E48FE20EB1F5A5887F2AC631FED9ED63 (e48fe)	Connected_To	(I) 125.212.132.222

Description

This artifact is a malicious PE32 executable that allows a remote operator or a server to perform various remote operations.

The malware contains encoded APIs functions, RC4 encrypted and XOR encoded strings. When executed, the malware will XOR decode and RC4 decrypt its strings.

Displayed below is the hard-coded RC4 key used to decrypt data and strings:

--Begin Key--
0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82
--End Key--

Displayed below are decrypted strings of interest:

--Begin strings--
"5mkfJY7kjmHcj4jlxG6jhsdRT7Faw7fj"
"CMUPD.bat"
"CMA25C.tmp"
"Software\\Microsoft\\Windows\\CurrentVersion\\Run"
"443"
"125.212.132.222"
"175.100.189.174"
"1992"
"10.10.30.110"
--End strings--

The malware attempts to read data from the registry "HKEY_LOCAL_MACHINE\Hex encoded data sub key\." Analysis indicates that the data stored in this registry is RC4 encrypted using the RC4 Key and is XOR encoded.

The malware collects the following system information and generates a unique ID:

--Begin information--
Private network IP (hexadecimal)
System name
OS Version information
Processor Information
Generated ID
Physical address(MAC).
--End information--

It attempts to connect to the following IPs and listen for commands or access requests from a remote server.

--Begin IPs--
"125.212.132.222:443"
"175.100.189.174:443"
"10.10.30.110:1992"
--End IPs--

Note: The IP address '10.10.30.110' is a private address found on many networks using NAT (Network Address Translation); the reason it's used here is not known for certain. Although it's poss ble the malware author had knowledge of the victim's network, it's more likely this IP was used by the author to test C2 functionality and was not removed.

The malware contains the following built-in functions for remote operations. Displayed below are the functions:

--Begin functionality--
Retrieves information about all installed disk, including the disk type and the amount of free space on the disk
Create, start, and terminate a new process and its primary thread
Search, read, write, move, and execute files
Get and modify file or directory timestamps
Change the current directory for a process or file
Delete malware and artifacts associated with the malware from the infected system.
--End functionality--

1216DA2B3D6E64075E8434BE1058DE06

Details

Name	1216DA2B3D6E64075E8434BE1058DE06

Size	157184
Type	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
MD5	1216da2b3d6e64075e8434be1058de06
SHA1	5ee752a1b2bcdb84243e615cd67397d965b16490
ssdeep	3072:GxXIbbVcpID+5/MiPDH8QnO3oMc+i+TN85mQLPgpnejnceJEOED:Gx4bbVZD+5/MiPDchdi+TN85muP0SlO
Entropy	6.27082111511

Antivirus

nProtect	Backdoor/W32.Agent.157184.BA
F-secure	Backdoor.Agent.ABWL
Symantec	Backdoor.Akdoor!g1
BitDefender	Backdoor.Agent.ABWL
Emsisoft	Backdoor.Agent.ABWL (B)
Ahnlab	Backdoor/Win32.Akdoor
Ikarus	Backdoor.Agent
AVG	BackDoor.Agent.BBQX

PE Information

Compiled	2016-03-21T15:45:19Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	08697ebe4017d27c904c7117bb109ca8	1024	2.73746441609
.text	cacb1aba3ba5bddfc2f023bb4ff3c54d	118784	6.45109982594
.rdata	0a36c62d9bd091d84219f7d34cf59284	23552	5.18722073535
.data	5c31589e75fc435a827c73e1b5bb4bca	5632	2.04007824221
.pdata	afc6eebc27a713b8010efe7f16ee8fab	6144	5.29206002541
.rsrc	9a33838895830247744985365b8b2948	512	5.11576737858
.reloc	d5815368ff7a4f0c4b82c70660aa7028	1536	2.80507847061

Description

This artifact is a malicious PE64 DLL that allows a remote operator or a server to perform various remote operations.

The malware strings and API functions are RC4 encrypted and XOR encoded. When executed, the malware XOR decodes and RC4 decrypts its strings and API functions. Displayed below are strings of interest observed during analysis:

--Begin strings--
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application
Config
--End strings--

Displayed below is the hard-coded RC4 key used to decrypt data, strings, and API functions:

--Begin Key--
0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82
--End Key--

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

--Begin registry--
hKey = "HKEY_LOCAL_MACHINE"
Subkey = "SYSTEM\CurrentControlSet\services\eventlog\Application\Config"
ValueName = "Malware name"
--Begin registry--

The configuration data the malware attempted to read was not available for analysis. Based on static analysis, this data contains the network capability functions for the malware, without it the malware lacks network activity. Analysis indicates the data stored in the registry key is RC4 encrypted using the RC4 Key and is XOR encoded.

The malware collects the following information about the infected system:

--Begin information--
Private network IP (hexadecimal)
System name
OS Version information
Processor Information
Generated ID
Physical address (MAC).
--End information--

It will RC4 encrypt and XOR encode the infected system data.

The malware has built-in functions for remote operations. Displayed below are the functions:

--Begin functionality--
Retrieves information about all installed disk, including the disk type and the amount of free space on the disk
Create, start, and terminate a new process and its primary thread
Search, read, write, move, and execute files
Get and modify file or directory timestamps
Change the current directory for a process or file
Delete all artifacts associated with the malware from the infected system.
--End functionality--

IPs

10.10.30.110

Ports

- 1992

Whois

PRIVATE-IP ADDRESS

Relationships

(I) 10.10.30.110	Related_To	(P) 1992
(I) 10.10.30.110	Characterized_By	(W) PRIVATE-IP ADDRESS
(I) 10.10.30.110	Connected_From	(F) E48FE20EB1F5A5887F2AC631FED9ED63 (e48fe)

175.100.189.174

Ports

- 443

Whois

inetnum: 175.100.189.0 - 175.100.189.255
netname: Ent-Cust
descr: Microscan Computers. Pvt. Ltd.
country: IN
admin-c: MCPL1-AP
tech-c: MCPL1-AP
status: ALLOCATED NON-PORTABLE
mnt-by: MAINT-MCPL-IN
mnt-lower: MAINT-MCPL-IN
mnt-routes: MAINT-MCPL-IN
mnt-irt: IRT-MCPL-IN
changed: uzair[@]microscan.co.in 20140118
source: APNIC

irt: IRT-MCPL-IN
address: A301/303, Everest Grande,
address: Mahakali caves rd., Andheri (E),
address: Mumbai - 400 093. India
e-mail: noc[@]vovinet.in
abuse-mailbox: abuse[@]vovinet.in
admin-c: MCPL1-AP
tech-c: MCPL1-AP

auth: # Filtered
mnt-by: MAINT-MCPL-IN
changed: clifford[@]microscan.co.in 20130109
phone: +91 (022) 66870600
fax-no: +91 (022) 66870800
changed: hm-changed[@]apnic.net 20140312
source: APNIC

role: MICROSCAN COMPUTERS PRIVATE LIMITED - network admi
address: Ground Floor , Heritage Plaza ,Telli galli Cross Road
country: IN
phone: +918879971867
fax-no: +912266870600
e-mail: uzair[@]microscan.co.in
admin-c: MCPL1-AP
tech-c: MCPL1-AP
nic-hdl: MCPL1-AP
mnt-by: MAINT-MCPL-IN
changed: hm-changed[@]apnic.net 20091230
source: APNIC

Relationships

(I) 175.100.189.174	Related_To	(P) 443
(I) 175.100.189.174	Characterized_By	(W) inetnum: 175.
(I) 175.100.189.174	Connected_From	(F) E48FE20EB1F5A5887F2AC631FED9ED63 (e48fe)

125.212.132.222

Ports

- 443

Whois

inetnum: 125.212.128.0 - 125.212.143.255
netname: hcmccable-net
country: VN
descr: ip range assign for Internet Cable Service in HCMC
descr: Vung dia chi danh cho dich vu Internet Cable tai Tp HCM
admin-c: VIG4-AP
tech-c: VIG4-AP
status: ASSIGNED NON-PORTABLE
changed: hm-changed[@]vnnic.net.vn 20080320
changed: hm-changed[@]vnnic.net.vn 20131211
mnt-by: MAINT-VN-VNNIC
mnt-irt: IRT-VNNIC-AP
source: APNIC

irt: IRT-VNNIC-AP
address: Ha Noi, VietNam
phone: +84-4-35564944
fax-no: +84-4-37821462
e-mail: hm-changed[@]vnnic.net.vn
abuse-mailbox: hm-changed[@]vnnic.net.vn
admin-c: PT174-AP
tech-c: NTTT1-AP
auth: # Filtered
mnt-by: MAINT-VN-VNNIC
changed: hm-changed[@]vnnic.net.vn 20101108
source: APNIC

role: VIETEL IPADMIN GROUP
address: 1 Tran Huu Duc, My Dinh, Tu Liem, Hanoi
country: VN
phone: +84-4-62989898
e-mail: soc[@]viettel.com.vn
remarks: send spam and abuse report to soc[@]viettel.com.vn
admin-c: TVT8-AP

tech-c: NDT9-AP
nic-hdl: VIG4-AP
mnt-by: MAINT-VN-VIETEL
changed: hm-changed[@]vnnic.vn 20160621
source: APNIC

% Information related to '125.212.128.0/17AS7552'

route: 125.212.128.0/17
descr: Viettel Corporation
descr: Internet service/exchange provider
descr: VIETEL-AS-AP
country: VN
origin: AS7552
member-of: rs-viettel
remarks: mailto: tiennd[@]viettel.com.vn
mnt-by: MAINT-VN-VIETEL
changed: hm-changed[@]vnnic.net.vn 20121211
changed: hm-changed[@]vnnic.net.vn 20131211
source: APNIC

Relationships

(I) 125.212.132.222	Related_To	(P) 443
(I) 125.212.132.222	Characterized_By	(W) inetnum: 125.
(I) 125.212.132.222	Connected_From	(F) E48FE20EB1F5A5887F2AC631FED9ED63 (e48fe)

Relationship Summary

(F) E48FE20EB1F5A5887F2AC631FED9ED63 (e48fe)	Connected_To	(I) 10.10.30.110
(F) E48FE20EB1F5A5887F2AC631FED9ED63 (e48fe)	Connected_To	(I) 175.100.189.174
(F) E48FE20EB1F5A5887F2AC631FED9ED63 (e48fe)	Connected_To	(I) 125.212.132.222
(I) 10.10.30.110	Related_To	(P) 1992
(I) 10.10.30.110	Characterized_By	(W) PRIVATE-IP ADDRESS
(I) 10.10.30.110	Connected_From	(F) E48FE20EB1F5A5887F2AC631FED9ED63 (e48fe)
(I) 175.100.189.174	Related_To	(P) 443
(I) 175.100.189.174	Characterized_By	(W) inetnum: 175.
(I) 175.100.189.174	Connected_From	(F) E48FE20EB1F5A5887F2AC631FED9ED63 (e48fe)
(I) 125.212.132.222	Related_To	(P) 443
(I) 125.212.132.222	Characterized_By	(W) inetnum: 125.
(I) 125.212.132.222	Connected_From	(F) E48FE20EB1F5A5887F2AC631FED9ED63 (e48fe)
(P) 443	Related_To	(I) 125.212.132.222
(W) inetnum: 125.	Characterizes	(I) 125.212.132.222
(P) 443	Related_To	(I) 175.100.189.174
(W) inetnum: 175.	Characterizes	(I) 175.100.189.174
(P) 1992	Related_To	(I) 10.10.30.110
(W) PRIVATE-IP ADDRESS	Characterizes	(I) 10.10.30.110

Mitigation Recommendations

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

- 175.100.189.174
- 125.212.132.222

US-CERT would like to remind users and administrators of the following best practices to strengthen the security posture of their organization's systems:

- Maintain up-to-date antivirus signatures and engines.
- Restrict users' ability (permissions) to install and run unwanted software applications.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Keep operating system patches up-to-date.
- Enable a personal firewall on agency workstations.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumbdrives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats; implement appropriate ACLs.

Contact Information

- 1-888-282-0870
- soc@us-cert.gov (UNCLASS)
- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

US-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/

Document FAQ

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

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.

Can I submit malware to US-CERT? Malware samples can be submitted via three methods. Contact us with any questions.

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

US-CERT encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on US-CERT's homepage at www.us-cert.gov.