MAR-10135536-10 – North Korean Trojan: BADCALL

us-cert.gov/ncas/analysis-reports/ar19-252a

Summary

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of ar information contained herein. 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 foreseeab accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distribut more information on the Traffic Light Protocol (TLP), see http://www.us-cert.gov/tlp.

Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts between the Department of Homeland Security (DHS), the Federal Bureau of the Department of Defense (DoD). Working with U.S. Government partners, DHS, FBI, and DoD identified Trojan malware variants used by the N referred to by the U.S. Government as BADCALL. The U.S. Government refers to malicious cyber activity by the North Korean government as HI information on HIDDEN COBRA activity, visit https[:]//www[.]us-cert.gov /hiddencobra.

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

This MAR includes malware descriptions related to HIDDEN COBRA, suggested response actions and recommended mitigation techniques. Use should flag activity associated with the malware, report the activity to the DHS National Cybersecurity and Communications Integration Center (N Watch (CyWatch), and give the activity the highest priority for enhanced mitigation.

This report provides analysis of four (4) malicious executable files. The first three (3) files are 32-bit Windows executables that function as proxy s "Fake TLS" method similar to the behavior described in a previously published NCCIC report, MAR-10135536-B. The fourth file is an Android Pac designed to run on Android platforms as a fully functioning Remote Access Tool (RAT).
For a downloadable copy of IOCs, see:

MAR-10135536-10.stix

Submitted Files (4)

4257bb11570ed15b8a15aa3fc051a580eab5d09c2f9d79e4b264b752c8e584fc (C01DC42F65ACAF1C917C0CC29BA63A...)

93e13ffd2a2f1a13fb9a09de1d98324f75b3f0f8e0c822857ed5ca3b73ee3672 (22082079AB45CCC256E73B3A7FD547...)

d1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212ae6be9e7 (C6F78AD187C365D117CACBEE140F62...)

edd2aff8fad0c76021adc74fe3cb3cb1a02913a839ad0f2cf31fdea8b5aa8195 (D93B6A5C04D392FC8ED30375BE17BE...)

Additional Files (2)

91650e7b0833a34abc9e51bff53cc05ef333513c6be038df29929a0a55310d9c (z)

da353b2845a354e1a3f671e4a12198e2c6f57a377d02dfaf90477869041a044f (hc.zip)

Findings

d1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212ae6be9e7

Tags

backdoordownloadertrojan

Details

Name	C6F78AD187C365D117CACBEE140F6230
Size	208896 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	c6f78ad187c365d117cacbee140f6230
SHA1	5116f281c61639b48fd58caaed60018bafdefe7a
SHA256	d1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212ae6be9e7
SHA512	f03fe686fac20714a6a7141bff1471c9187b0d4630752fb5eb922605dbb74105c1ecced7e1980a0d79195c1a7f1b2f221e483bc9f7e2164
ssdeep	1536:X86D0r4QxG5+XCFpaG7+esyzktLYUwnZ7hUOKYUwnZ7hUOaeYUwnZ7hUOKYUwnZr:X8O0IgCvH7+UzktMxzxgRxzx9

Entropy	6.833120

Antivirus

Ahnlab	Backdoor/Win32.Akdoor
Antiy	Trojan/Win32.BTSGeneric
BitDefender	Trojan.Agent.CUTNUnclassified
ClamAV	Win.Trojan.BadCall-6473322-0
Cyren	W32/Trojan.DCIV-3872
ESET	Win32/NukeSped.CX trojan
Emsisoft	Trojan.Agent.CUTN (B)
Ikarus	Trojan.Win32.NukeSped
K7	Trojan (005272fc1)
Microsoft Security Essentials	Backdoor:Win32/Hidcob.A
NANOAV	Trojan.Win32.NukeSped.eydshe
Sophos	Troj/Cruprox-C
Symantec	Trojan Horse
TACHYON	Backdoor/W32.Agent.208896.DD
TrendMicro	BKDR_NUKESPED.A
TrendMicro House Call	BKDR_NUKESPED.A
Vir.IT eXplorer	Trojan.Win32.Dnldr26.BAYE
VirusBlokAda	Trojan.Downloader
Zillya!	Trojan.NukeSped.Win32.49

Yara Rules

hidden_cobra_consolidated.yara	rule NK_SSL_PROXY { meta: Author = "CISA Code & Media Analysis" Incident = "10135536" Date = "201 "Hidden_Cobra" Family = "BADCALL" Description = "Detects NK SSL PROXY" MD5_1 = "C6F78AD187C365D117CACBEE140F6230" MD5_2 = "C01DC42F65ACAF1C917C0CC29BA63ADC" str {8B4C24088A140880F24780C228881408403BC67CEF5E} $s1 = {568B74240C33C085F67E158B4C24088A140880EA2880F247881408403BC67CEF5E} $s2 = {4775401F71343574797536686776686 9375E2524736466} $s3 = {67686667686A7579756667646766747 {6D2A5E265E676866676534776572} $s5 = {3171617A5853444332337765} $s6 = "ghfghjuyufgdgftr" $s7 "q45tyu6hgvhi7^%$sdf" $s8 = "m*^&^ghfge4wer" condition: ($s0 and $s1 and $s2 and $s3 and $s4 and $s $s8) }
hidden_cobra_consolidated.yara	rule xor_add { meta: Author = "CISA trusted 3rd party" Incident = "10135536" Date = "2018-04-19" Categor Family = "n/a" Description = "n/a" strings: $decode = { 80 ea 28 80 f2 47} $encode = { 80 f2 47 80 c2 28} c 0x5A4D and uint16(uint32(0x3c)) == 0x4550 and all of them }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2016-02-06 22:17:51-05:00
Import Hash	3f197f5c6469421f4472504b1bada91e

PE Sections

MD5	Name	Raw Size	Entropy
a8f97910c62034b318e17aa17fb97f1c	header	4096	0.688106
08112b571663ff5ed42e331a00ccce0c	.text	53248	6.508967
ca61927558a4dfe9305eb037a5432960	.rdata	8192	4.573237

bb49b2fb00c1ae88ad440971914711a7	.data	139264	6.941279
c58b62cf949e8636ebd5c75f482207c3	.sxdata	4096	0.181138

Packers/Compilers/Cryptors

Microsoft Visual C++ v6.0

Description

This file is a malicious 32-bit Windows executable. Analysis indicates this application is designed to force a compromised system to function as a executed, the malware binds and listens for incoming connections on port 8000 of the compromised system. The proxy session traffic is protected cipher based on rotating XOR and ADD. The cipher will XOR each byte sent with 47h and added by 28h. Each byte received by the malware will subtracted by 28h. See Figures 1, 2 and 3 for code examples. Notably, this malware attempts to disable the Windows firewall before binding to po following registry key:

--Begin Firewall Reg Key Modified--

SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\\List

--End Firewall Reg Key Modified--

Analysis of this malware indicates it is designed to turn a victim host into a "hop point" by relaying traffic to a remote system. When the adversary victim's machine via port 8000, the adversary must first authenticate (over a session secured with the XOR/ADD cipher described above) by provi "1qazXSDC23we". If the malware does not receive this value, it will terminate the session, responding with the value "m*^&^ghfge4wer".

If the operator authenticates successfully, they can then issue the command "ghfghjuyufgdgftr" which instructs the malware to begin functioning a respond to the operator with the value "q45tyu6hgvhi7^%$sdf". Next, the malware attempts to create a proxy session between the operator and a process, the malware will attempt to authenticate with the destination server by sending the value "ghfghjuyufgdgftr" as a challenge. To complete sequence, the malware expects to receive a response value of "q45tyu6hgvhi7^%$sdf". All challenge and response traffic is encoded using the A described earlier.

The proxy session begins with a remote operator connecting to this implant via a "fake TLS" connection attempt, similar to the behavior described NCCIC report, MAR-10135536-B. Essentially, the malware initiates the TLS session using one of several public SSL certificates obtained from we internet services and embedded in the malware. However, the traffic from the operator to this implant is not protected with SSL / TLS encryption. protected via the ADD/XOR cipher embedded within this implant (see Figure 2-3.). If the remote operator authenticates correctly as detailed abov begin a proxy session with the remote target system. The traffic to the remote systems from this implant are sent and received via the SSL_read a available in OpenSSL. However, the malware does not appear to attempt to load an SSL private key or certificate.

The malware contains public SSL certificates for the following list of domains, which are used for initiating the "fake TLS" session:

--Begin SSL Certificate Strings--

myservice.xbox.com
uk.yahoo.com
web.whatsapp.com
www[.]apple.com
www[.]baidu.com
www[.]bing.com
www[.]bitcoin.org
www[.]comodo.com
www[.]debian.org
www[.]dropbox.com
www[.]facebook.com
www[.]github.com
www[.]google.com
www[.]lenovo.com
www[.]microsoft.com
www[.]paypal.com
www[.]tumblr.com
www[.]twitter.com
www[.]wetransfer.com
www[.]wikipedia.org

--End SSL Certificate Strings--

Screenshots

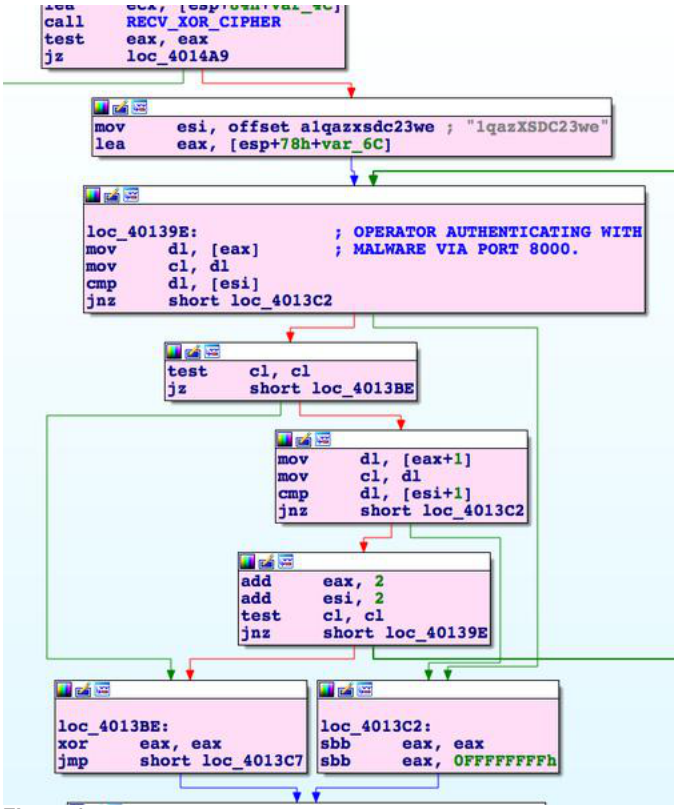

Figure 1 -

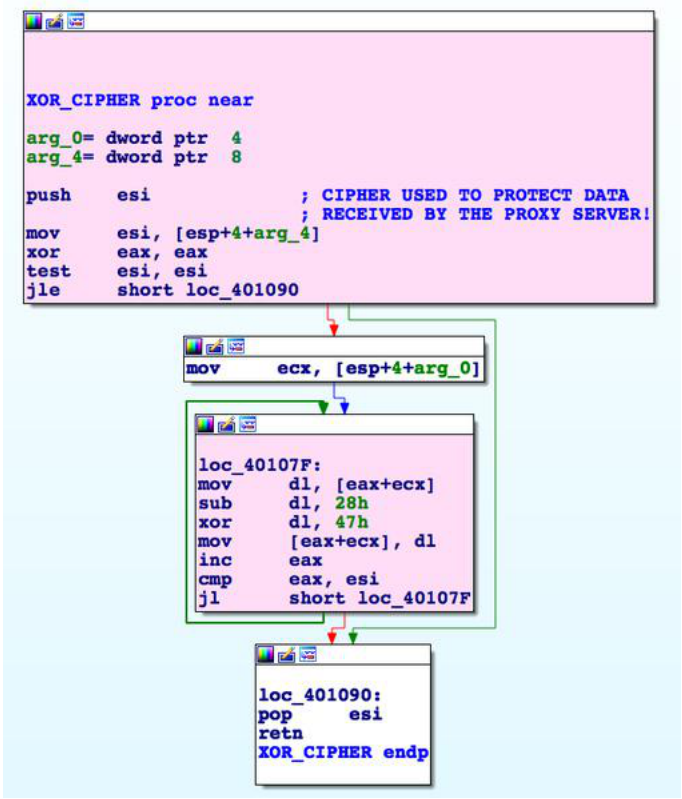

Figure 2 -

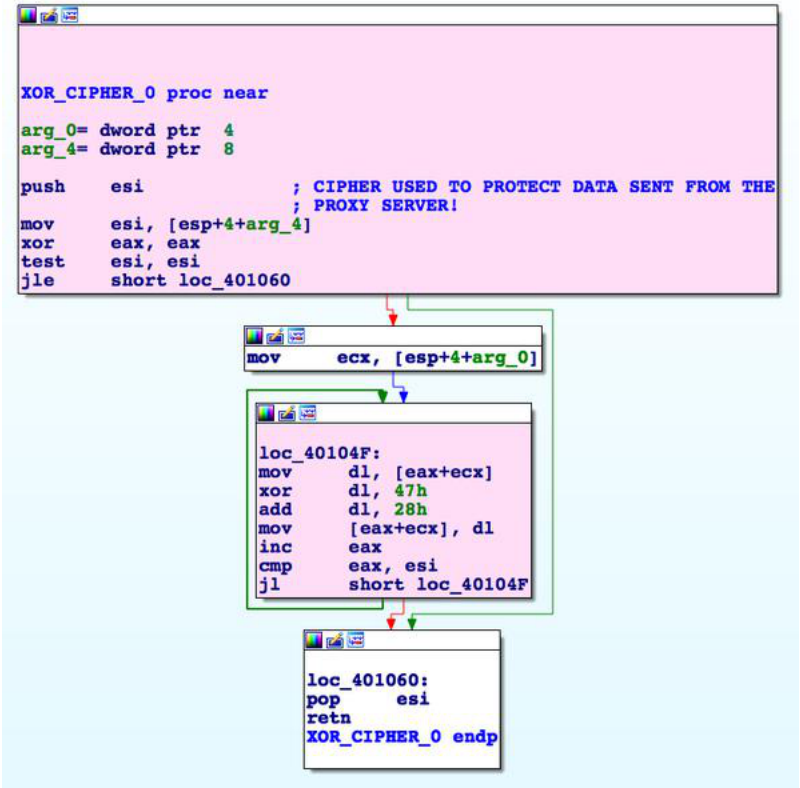

Figure 3 -

Figure 4 -

4257bb11570ed15b8a15aa3fc051a580eab5d09c2f9d79e4b264b752c8e584fc

Tags

backdoortrojan

Details

Name	C01DC42F65ACAF1C917C0CC29BA63ADC
Size	233472 bytes
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	c01dc42f65acaf1c917c0cc29ba63adc
SHA1	d288766fa268bc2534f85fd06a5d52264e646c47
SHA256	4257bb11570ed15b8a15aa3fc051a580eab5d09c2f9d79e4b264b752c8e584fc
SHA512	0ff6745ef787e89bd0f154bd96571f086f6b6596621e7211bb8ce8f970a26a72770a44b9aa1b906e6599dd5f421e0dd50895e2cde9ba85

ssdeep	1536:cseScclTQDYY3TSF00sK/LVtKYUwnZ7hUO1YUwnZ7hUOAeYUwnZ7hUO7YUwnZ7hj:cseScjYY3Tyc0LVt9xsxuRxSxzxg0j
Entropy	6.861843

Antivirus

Ahnlab	Backdoor/Win32.Akdoor
Antiy	Trojan/Win32.BTSGeneric
Avira	TR/NukeSped.ydcjt
BitDefender	Trojan.Agent.CBEJUnclassified
ClamAV	Win.Trojan.Agent-6449123-0
Cyren	W32/Agent.OOKJ-8303
ESET	Win32/NukeSped.CX trojan
Emsisoft	Trojan.Agent.CBEJ (B)
Ikarus	Trojan.Agent
K7	Trojan (005272fc1)
Kaspersky	Backdoor.Win32.Agent.texxz
McAfee	Generic.ayf
Microsoft Security Essentials	Trojan:Win32/Autophyte.B!dha
NANOAV	Trojan.Win32.NukeSped.eyembk
Quick Heal	Trojan.Multi
Sophos	Troj/BadCall-A
Symantec	Trojan Horse
TACHYON	Trojan/W32.Agent.233472.APN
TrendMicro	BKDR_NUKESPED.B
TrendMicro House Call	BKDR_NUKESPED.B
Vir.IT eXplorer	Backdoor.Win32.Agent.LX
VirusBlokAda	Backdoor.Agent
Zillya!	Trojan.Agent.Win32.879097

Yara Rules

hidden_cobra_consolidated.yara	rule NK_SSL_PROXY { meta: Author = "CISA Code & Media Analysis" Incident = "10135536" Date = "201 "Hidden_Cobra" Family = "BADCALL" Description = "Detects NK SSL PROXY" MD5_1 = "C6F78AD187C365D117CACBEE140F6230" MD5_2 = "C01DC42F65ACAF1C917C0CC29BA63ADC" str {8B4C24088A140880F24780C228881408403BC67CEF5E} $s1 = {568B74240C33C085F67E158B4C24088A140880EA2880F247881408403BC67CEF5E} $s2 = {4775401F7134357479753668677668869375E2524736466} $s3 = {67686667686A7579756667646766747 {6D2A5E265E676866676534776572} $s5 = {3171617A5853444332337765} $s6 = "ghfghjuyufgdgftr" $s7 "q45tyu6hgvhi7^%$sdf" $s8 = "m*^&^ghfge4wer" condition: ($s0 and $s1 and $s2 and $s3 and $s4 and $s $s8) }
hidden_cobra_consolidated.yara	rule xor_add { meta: Author = "CISA trusted 3rd party" Incident = "10135536" Date = "2018-04-19" Categor Family = "n/a" Description = "n/a" strings: $decode = { 80 ea 28 80 f2 47} $encode = { 80 f2 47 80 c2 28} c 0x5A4D and uint16(uint32(0x3c)) == 0x4550 and all of them }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2016-02-05 13:16:54-05:00
Import Hash	0b10d6fde1b7cdd778e0338a2d7e5046

PE Sections

MD5	Name	Raw Size	Entropy
f0cb80c557b1172362064c51bbb9b271	header	4096	0.696473
e9d0219343e64c8c8aa6f084db44b92c	.text	45056	6.324040
1092801819f120298e2ddac6a96e3fd0	.rdata	8192	3.775333
5109fb1db61b533c23762d9044579db7	.data	167936	7.045393
9ce04d3e820fa7056f351dbcfa05b0fb	.reloc	8192	2.767666

Packers/Compilers/Cryptors

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

Description

This file is a malicious 32-bit Windows DLL. Static analysis indicates this application is very similar in structure and function to C6F78AD187C365
However, rather than being a PE32 executable this application is a Windows 32-bit DLL, which must be loaded by an external loader. This externa
within this submission.

This DLL is designed to force a compromised system to act as a proxy server. This implant is designed to proxy network traffic from an operator t
that is being operated by the adversary on a remote system. The traffic to and from this proxy server will be protected with the same simple XOR
malware C6F78AD187C365D117CACBEE140F6230. Static analysis indicates sessions from the remote operator connecting directly to this impla
SSL / TLS, however the proxy sessions to the remote systems will not be protected via TLS but will instead use a "fake TLS" session. The traffic f
implant and traffic from the implant to the remote systems will be protected via the embedded XOR / ADD cipher (view screenshot). To implement
operator, the malware loads a private key from a file named 'wbemhost.dll' and a certificate from a file named 'netconf.dll'. This malware does not
(see Figure. 7).

Analysis of this malware indicates it is designed to bind to and listen for incoming connections to the victim's system after disabling the firewall by
registry key. The firewall is disabled by allowing incoming access on port 443.

--Begin Firewall Reg Key Modified--

SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfileGloballyOpenPorts\\List

--End Firewall Reg Key Modified--

After connecting to this malware, the operator must issue the challenge value "qwertyuiop" to authenticate with the implant (see Figure 5). This m
added capability of allowing an operator to collect information about the compromised system. This information is collected using the Windows AP
gethostbyname, and GetAdaptersInfo. In order to use this feature, the operator must issue the instruction value "ghfghjuyufgdgftr" after authentica
C6F78AD187C365D117CACBEE140F6230, this malware uses the OpenSLL functions ssl_read() and ssl_write() to exchange data with the opera
malware additionally uses a simple XOR cipher (as earlier described) to decrypt incoming traffic.

Analysis indicates this malware must also authenticate with the destination server to which the operator wishes to proxy traffic. To do so, this malv
remote server the challenge value "1qazXSDC23we." The malware must then receive the following response from the destination server before it
proxy traffic to it: "m*^&^ghfge4wer" (see Figure 6). The authentication values sent to and from this proxy server will be protected via the same XO
by the malware C6F78AD187C365D117CACBEE140F6230 (see Figures 8-9).

The following is a list of the domains for which the malware contains public SSL certificates, used for initiating the "FAKE TLS" sessions:

--Begin SSL cert list--

myservice.xbox.com
uk.yahoo.com
web.whatsapp.com
www[.]apple.com
www[.]baidu.com
www[.]bing.com
www[.]bitcoin.org
www[.]comodo.com
www[.]debian.org
www[.]dropbox.com
www[.]facebook.com
www[.]github.com
www[.]google.com
www[.]lenovo.com
www[.]microsoft.com
www[.]paypal.com
www[.]tumblr.com
www[.]twitter.com
www[.]wetransfer.com
www[.]wikipedia.org

--End SSL cert list--
Screenshots

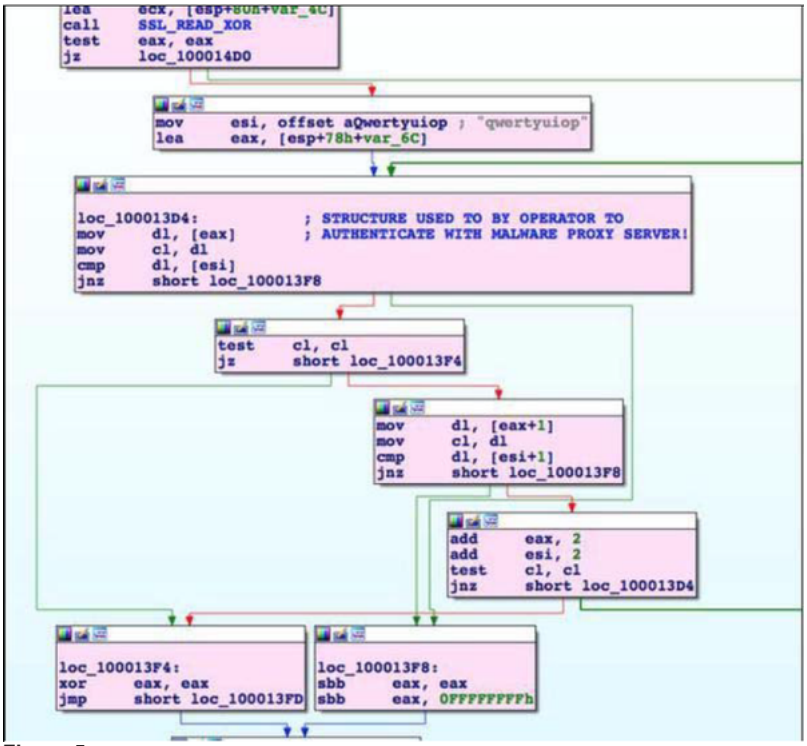

Figure 5 -

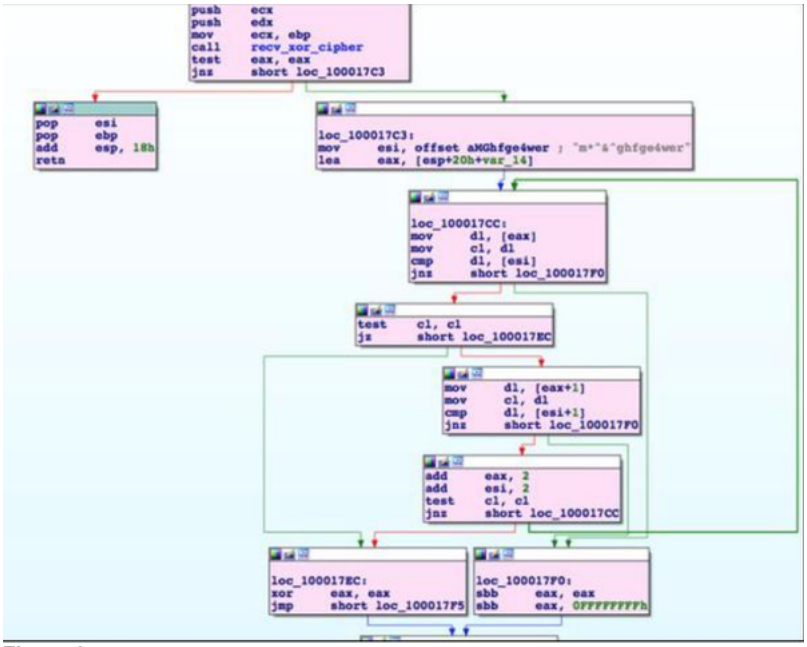

Figure 6 -

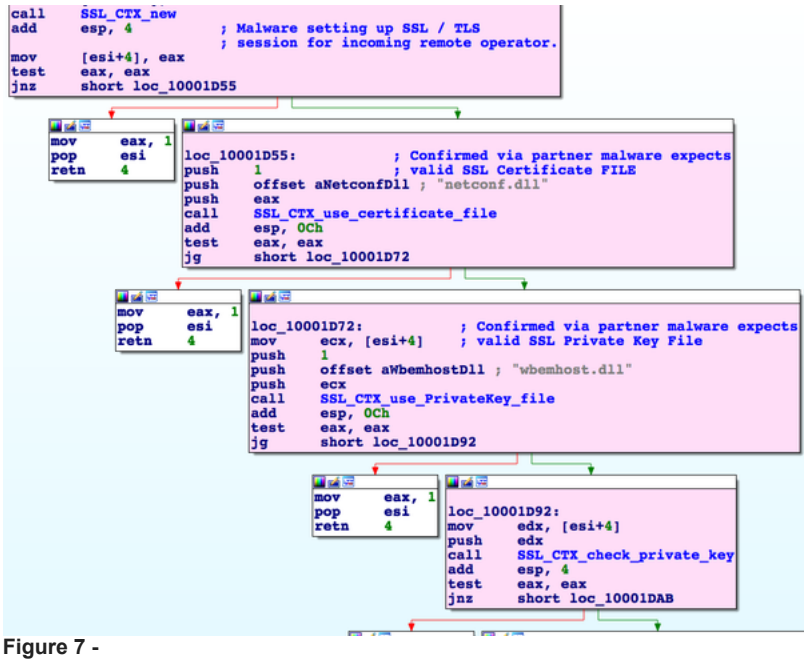

Figure 7 -

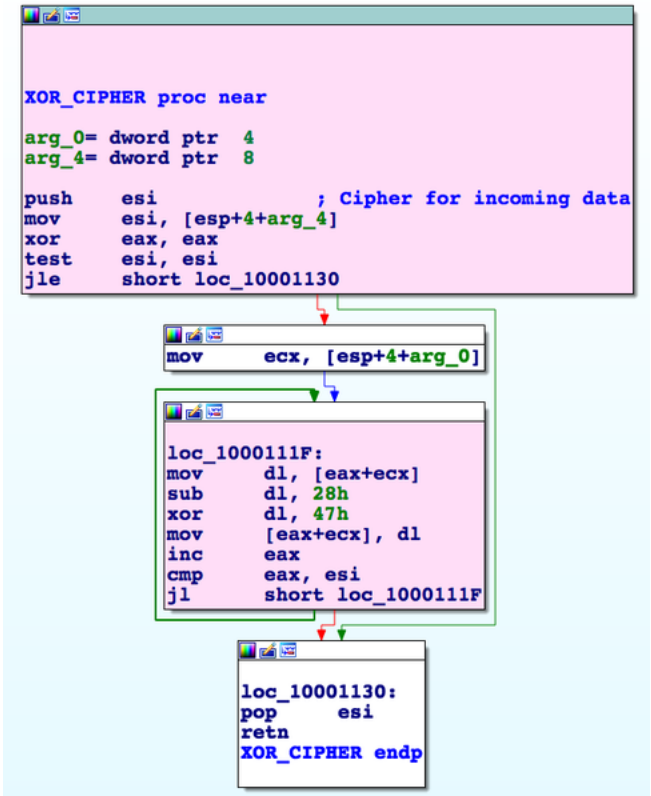

Figure 9 -

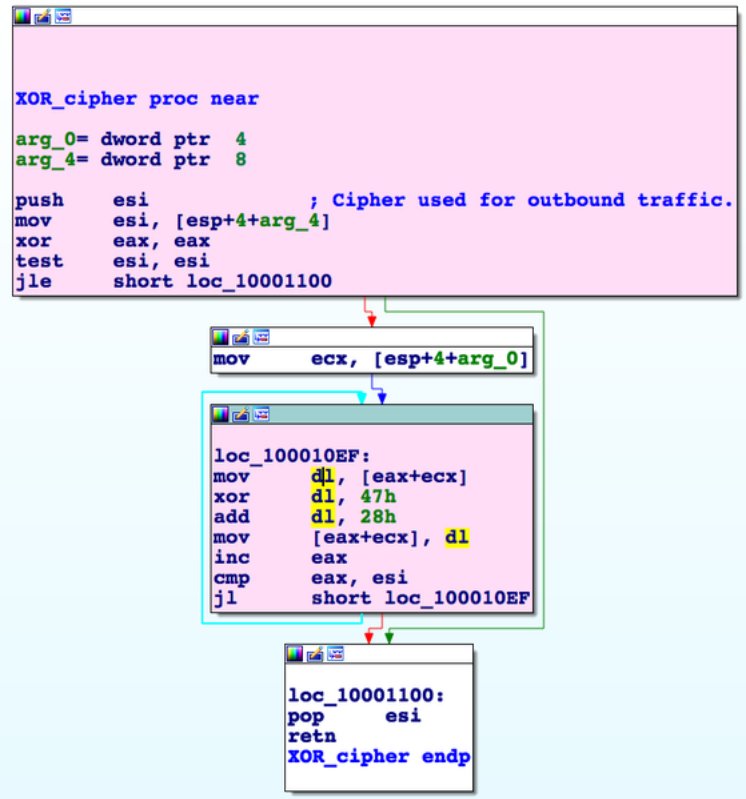

Figure 8 -

93e13ffd2a2f1a13fb9a09de1d98324f75b3f0f8e0c822857ed5ca3b73ee3672

Tags

backdoortrojan

Details

Name	22082079AB45CCC256E73B3A7FD54791
Size	118784 bytes
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	22082079ab45ccc256e73b3a7fd54791
SHA1	029bb15a2ba0bea98934aa2b181e4e76c83282ce
SHA256	93e13ffd2a2f1a13fb9a09de1d98324f75b3f0f8e0c822857ed5ca3b73ee3672
SHA512	1b8c3e6da2e43f14d291c6e850eb6a0a51947bb2e87ce378a1b08119667509c36046b73a2e3528054b2b04925abecdc385478b3ff542
ssdeep	3072:zO+bv42IGfT/EpdIS+aYy8Wt9QopUuul/WRaKj1gv:aov42T/EptldpZugQK
Entropy	6.824890

Antivirus

Ahnlab	Trojan/Win32.Casdet
Antiy	Trojan/Win32.Casdet
Avira	TR/Agent.tsurv
BitDefender	Trojan.GenericKD.41577128Unclassified
Cyren	W32/Trojan.DKUU-0798
ESET	Win32/NukeSped.FU trojan
Emsisoft	Trojan.GenericKD.41577128 (B)
K7	Trojan (005560611)

McAfee	RDN/Generic.dx
Quick Heal	Trojan.Casdet
Symantec	Backdoor.Trojan

Yara Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2018-07-17 00:59:05-04:00
Import Hash	16829b63f8ecedc02fa379016636a7b3

PE Sections

MD5	Name	Raw Size	Entropy
1e0638185a7f70a39e8366d293736868	header	4096	0.696223
7c0e47bb01059f413f0aac60be01708b	.text	36864	6.564904
bf754906211b615d5a32284c3e3c97ad	.rdata	12288	4.513552
c31a6726d1210b6c5e8c622e9fc91c3d	.data	57344	7.684244
f9f1af8f7d13e1321806e125559cde91	.reloc	8192	1.955731

Packers/Compilers/Cryptors

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

Relationships

93e13ffd2a...	Contains	da353b2845a354e1a3f671e4a12198e2c6f57a377d02dfaf90477869041a044f

Description

This file is a 32-bit Windows DLL. This file is an implant loader for a DLL and is designed to be called from the ServiceMain export function. The n
decrypt an embedded chunk of data that is 50896 bytes in size. This decryption is performed utilizing an RC4 algorithm. The key used for this dec
below:

--Begin RC4 Key--

CC E5 71 D9 B5 88 9D 53 EF 74 D1 9A E5 A4 1E B3

--End RC4 Key--

This decrypted file is a zip file which contains a malicious DLL file named 'z' (2733A9069F0B0A57BF9831FE582E35D9).

Screenshots

Figure 10 -

da353b2845a354e1a3f671e4a12198e2c6f57a377d02dfaf90477869041a044f

Tags

trojan

Details

Name	hc.zip
Size	50896 bytes
Type	Zip archive data, at least v2.0 to extract
MD5	eb7da5f1e86679405aa255aa4761977d
SHA1	880cb39fee291aa93eb43d92f7af6b500f6d57dc
SHA256	da353b2845a354e1a3f671e4a12198e2c6f57a377d02dfaf90477869041a044f
SHA512	f1bc07f218e266d10a3f4d4a76388d3dc37fe51134877fcf071a745214a4309ff6ec71cdf5e7943b08dd68824cf4883a1f4c493911bef4d57
ssdeep	768:wu4/k7m28PNNc5lepsSIDq/TlF6u7ODBHGslr5XRdBXSCF8bbbbbb0gbvbbb9fG+:4M/sfqrD6THl7OlFXRbXhFM++
Entropy	7.993615

Antivirus

Microsoft Security Essentials	Trojan:Win32/Autophyte.B!dha
Quick Heal	Trojan.Autophyte

Yara Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

da353b2845...	Contains	91650e7b0833a34abc9e51bff53cc05ef333513c6be038df29929a0a55310d9c
da353b2845...	Contained_Within	93e13ffd2a2f1a13fb9a09de1d98324f75b3f0f8e0c822857ed5ca3b73ee3672

Description

This file is a zip compressed archive that was extracted from the file 22082079AB45CCC256E73B3A7FD54791. The zip file contains the maliciou (2733a9069f0b0a57bf9831fe582e35d9).

91650e7b0833a34abc9e51bff53cc05ef333513c6be038df29929a0a55310d9c

Tags

backdoortrojan

Details

Name	z
Size	221184 bytes
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	2733a9069f0b0a57bf9831fe582e35d9
SHA1	f06f9d015c2f445ee0f13da5708f93c381f4442d
SHA256	91650e7b0833a34abc9e51bff53cc05ef333513c6be038df29929a0a55310d9c
SHA512	78dde154425ff447d9f7d38dacd707227a9375f6b8890f3da99f97f93acf9fb12db3f678db799920fac0854235aaeb558d49578d5f443d85
ssdeep	1536:kkRTTvge1l5HFXCtTX/Mo1xaft0YUwnZ7hUOSYUwnZ7hUOAeYUwnZ7hUOCYUwnZl:kkRTTRj5HlkMsaft7xfxuRx3xzxN
Entropy	7.062074

Antivirus

Ahnlab	Backdoor/Win32.Akdoor
Antiy	Trojan/Win32.Autophyte
Avira	TR/NukeSped.kaqej
BitDefender	Gen:Variant.Zusy.290461Unclassified
ClamAV	Win.Trojan.BadCall-6473322-0
ESET	Win32/NukeSped.FU trojan
Emsisoft	Gen:Variant.Zusy.290461 (B)
Ikarus	Trojan.Win32.Autophyte
K7	Trojan (005562ef1)
McAfee	RDN/Generic BackDoor
Microsoft Security Essentials	Trojan:Win32/Autophyte.B!dha
Quick Heal	Trojan.Autophyte
Symantec	Trojan.Proxabop

Yara Rules

hidden_cobra_consolidated.yara	rule NK_SSL_PROXY { meta: Author = "CISA Code & Media Analysis" Incident = "10135536" Date = "201 "Hidden_Cobra" Family = "BADCALL" Description = "Detects NK SSL PROXY" MD5_1 = "C6F78AD187C365D117CACBEE140F6230" MD5_2 = "C01DC42F65ACAF1C917C0CC29BA63ADC" str {8B4C24088A140880F24780C228881408403BC67CEF5E} $s1 = {568B74240C33C085F67E158B4C24088A140880EA2880F247881408403BC67CEF5E} $s2 = {4775401F7134357479753668677668869375E2524736466} $s3 = {67686667686A7579756667646766747 {6D2A5E265E676866676534776572} $s5 = {3171617A5853444332337765} $s6 = "ghfghjuyufgdgftr" $s7 "q45tyu6hgvhi7^%$sdf" $s8 = "m*^&^ghfge4wer" condition: ($s0 and $s1 and $s2 and $s3 and $s4 and $s $s8) }
hidden_cobra_consolidated.yara	rule xor_add { meta: Author = "CISA trusted 3rd party" Incident = "10135536" Date = "2018-04-19" Categor Family = "n/a" Description = "n/a" strings: $decode = { 80 ea 28 80 f2 47} $encode = { 80 f2 47 80 c2 28} c 0x5A4D and uint16(uint32(0x3c)) == 0x4550 and all of them }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2018-07-17 00:53:11-04:00
Import Hash	6a279f14835aa138eab03b57a6e45825

PE Sections

MD5	Name	Raw Size	Entropy
79d8ca8726a734aef20f898f5e2fbb50	header	4096	0.711446

e2d8cd2675a9cf155d8a84a98e91726a	.text	40960	6.486031
9dd07afaecfd084b82051ce7ad1b4bc1	.rdata	8192	4.848305
20de8f78ea78fe96c41dd8926438fdab	.data	159744	7.189385
5aff5f4cc16000bc502b6eec007c9e31	.reloc	8192	2.586704

Packers/Compilers/Cryptors

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

Relationships

91650e7b08...	Contained_Within	da353b2845a354e1a3f671e4a12198e2c6f57a377d02dfaf90477869041a044f

Description

This file is a 32-bit DLL file. Static analysis indicates this application is very similar in structure and function to C6F78AD187C365D117CACBEE1

This DLL is designed to force a compromised system to act as a proxy server. This implant is designed to proxy network traffic from an operator t that is being operated by the adversary on a remote system. The traffic to and from this proxy server will be protected with the same simple XOR malware C6F78AD187C365D117CACBEE140F6230.

Static analysis indicates the OpenSSL library is used to implement a TLS/SSL initialization between the operator and this implant. The malware w XOR / ADD cipher to secure communications from the remote operator -- in addition to the SSL encryption. During this initialization process the m key from a file named 'wbemhost.dll' (see Figure 11.) and a certificate from a file named 'netconf.dll'. The malware does not drop these two files, t be already dropped on the system using another method.

Analysis of this malware indicates it is designed to bind to and listen for incoming connections on port 443 of a victim's system after disabling the following registry key:

--Begin Firewall Reg Key Modified--

SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile

GloballyOpenPorts\\List

--End Firewall Reg Key Modified--

Static analysis indicates the malware attempts to read configuration data from the following registry key:

--Begin Config Registry Key --

Key: SOFTWARE\Microsoft\windows\CurrentVersion\NetConfigs
Value: Description

--End Config Registry Key--

The registry key name is decrypted via RC4 and the malware will attempt to decrypt the contents by using RC4 if the key is present on the victim's binds and listens for C2 sessions on the victim's system (see Figure 12.). Once a C2 session is received on a binded port the malware will read th OpenSSL library and will decode it using a simple rotating XOR / ADD cipher.

After decrypting the incoming traffic the implant ensures it contains the following authentication value:

--Begin Auth Value--

qwertyuiop

--End Auth Value--

If the authentication value exists, the implant knows the external operator wants to proxy traffic through to another location. The malware will resp encoded value "asdfghjkl" to let the operator know it is ready to proceed with the proxy requests. Static analysis indicates the malware will connec via the Fake TLS protocol mentioned in prior analysis. SSL encryption will not be used to secure communications between this implant and the re will simply use its embedded XOR / ADD cipher (view screenshot). The malware notifies the remote proxy server it wants to open a session by se "1qazXSDC23we". It then expects the remote proxy server to respond with the value "m*^&^ghfge4wer". If the remote proxy server does not resp proxy session will not continue.

Analysis indicates the malware also contains a large structure capable of gathering a great deal of information about the victim's system including and attached adapters. If the following authentication value is received from the external operator, the malware knows the operator wants to gathe victim's system:

--Begin Auth Value--

ghfghjuyufgdgftr

--End Auth Value--

The malware will then respond with the XOR / ADD encoded value "q45tyu6hgvhi7^%$sdf" to let the remote operator know that it received the co system information (see Figure 13.). Static analysis indicates all network traffic received and sent from this implant will be protected via a rotating Additionally, the connection to the binded port by the C2 operator will be protected via SSL encryption. Whereas, the connections to the remote h proxy session) will be protected only via the cipher mentioned above (see Figures 14-15.).

Screenshots

Figure 13 -

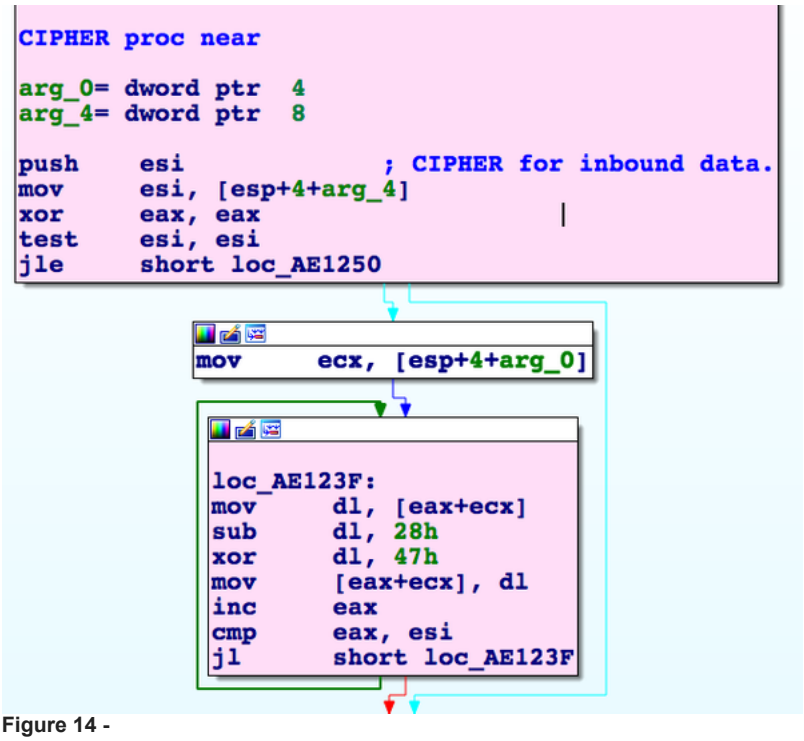

Figure 14 -

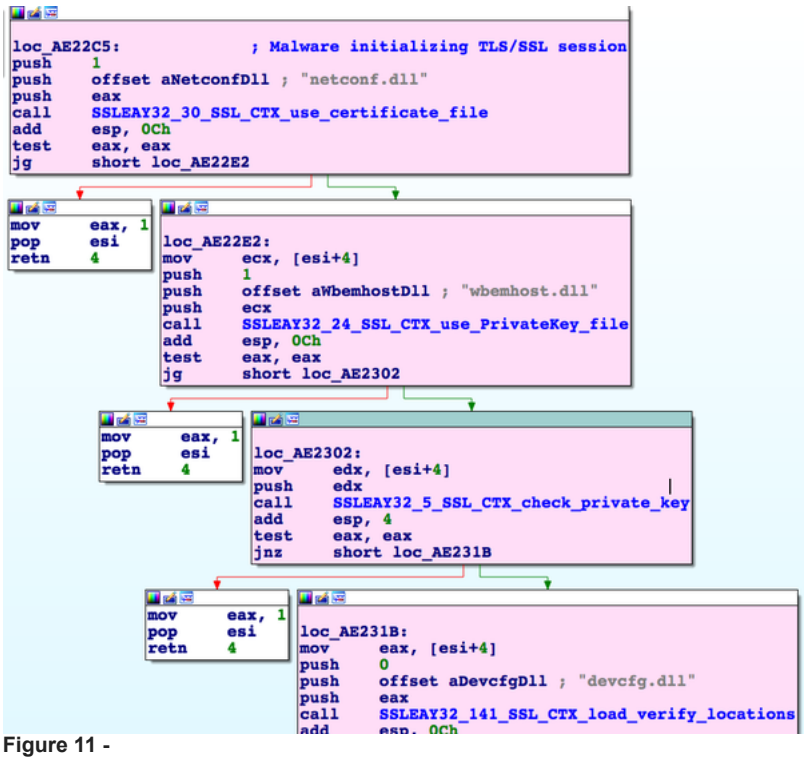

Figure 11 -

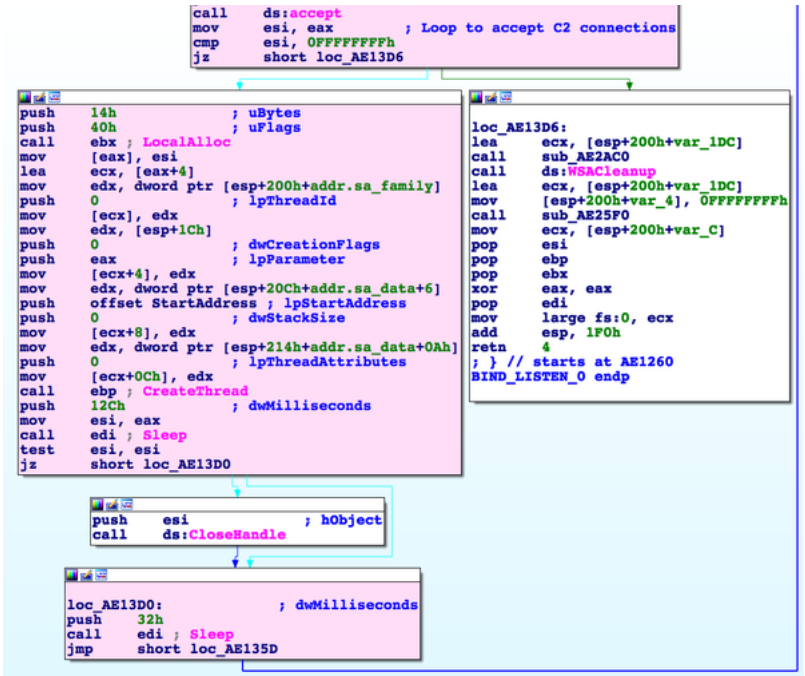

Figure 12 -

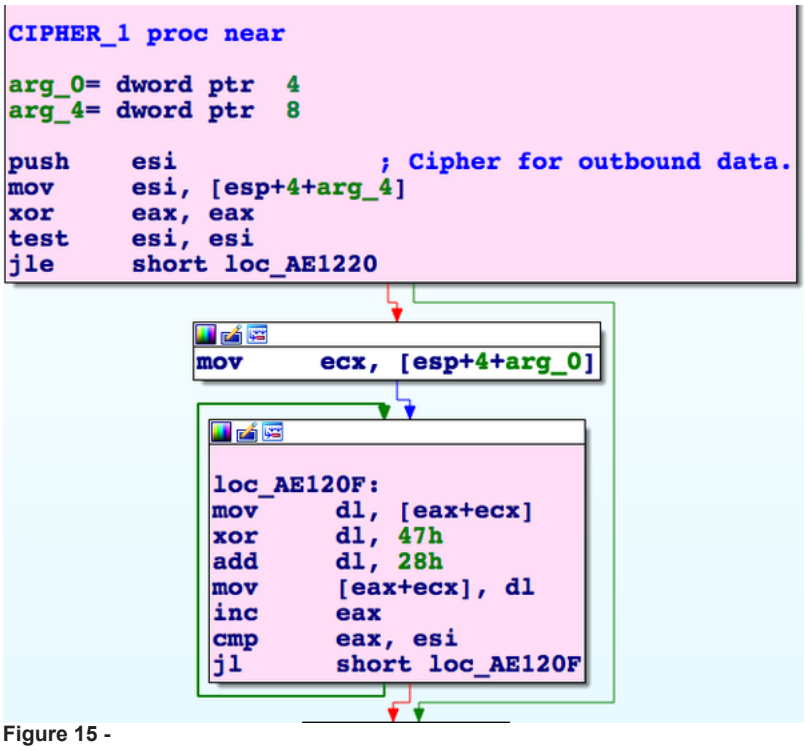

Figure 15 -

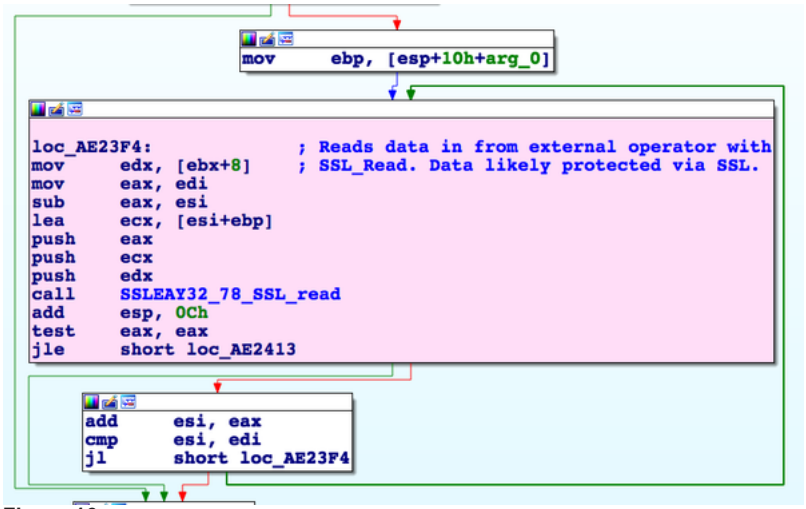

Figure 16 -

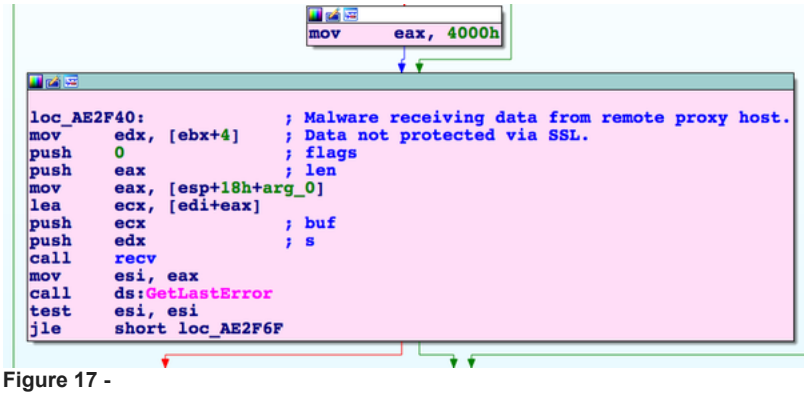

Figure 17 -

edd2aff8fad0c76021adc74fe3cb3cb1a02913a839ad0f2cf31fdea8b5aa8195

Tags

backdoorspywaretrojan

Details

Name	D93B6A5C04D392FC8ED30375BE17BEB4
Size	321730 bytes
Type	Java archive data (JAR)
MD5	d93b6a5c04d392fc8ed30375be17beb4
SHA1	f862c2899c41a4d1120a7739cdaff561d2490360
SHA256	edd2aff8fad0c76021adc74fe3cb3cb1a02913a839ad0f2cf31fdea8b5aa8195
SHA512	709931cec37cedf4c5f84f1a2242e48c8465b97217be96a77627a83f317cbb1d0a1a1886955b982b0bf9b92ccf7ab1bef8d782622f81ce1
ssdeep	6144:1c35mQ6aHY0wxxp/2o0uK1uv8q8lY1pr/Cc800a0sdOQypHIKO9kxZ4:+J5Hlwxmo0Tuv8q8i3+c800NsdFyKKOR
Entropy	7.989671

Antivirus

Ahnlab	Android-Spyware/Susdama.74c94
Avira	ANDROID/Agent.uytoi
Ikarus	Trojan.AndroidOS.Agent
NANOAV	Trojan.Android.Mlw.femarh
Quick Heal	Android.Manuscrypt.GEN21990
Sophos	Andr/Spy-ANK
Symantec	Backdoor.Trojan

Yara Rules

No matches found.

ssdeep Matches

No matches found.

Description

This file is a malicious Android APK file. Static analysis indicates it is a RAT, which is designed to listen for incoming connections to a compromise
60000.

Analysis indicates the Android app is capable of recording phone calls, taking screenshots using the device's embedded camera, reading data fro
manager, and downloading and uploading data from the compromised Android device. The application is also capable of executing commands or
system and scanning for open Wi-Fi channels.

Relationship Summary

93e13ffd2a...	Contains	da353b2845a354e1a3f671e4a12198e2c6f57a377d02dfaf90477869041a044f
da353b2845...	Contains	91650e7b0833a34abc9e51bff53cc05ef333513c6be038df29929a0a55310d9c
da353b2845...	Contained_Within	93e13ffd2a2f1a13fb9a09de1d98324f75b3f0f8e0c822857ed5ca3b73ee3672
91650e7b08...	Contained_Within	da353b2845a354e1a3f671e4a12198e2c6f57a377d02dfaf90477869041a044f

Recommendations

CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organizatio
configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unl
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

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

Contact Information

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

Document FAQ

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

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

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document shoul
at 1-888-282-0870 or soc@us-cert.gov.

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

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

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

Revisions

September 9, 2019: Initial version

Please share your thoughts.

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