MAR-10135536-8 – North Korean Trojan: HOPLIGHT

us-cert.gov/ncas/analysis-reports/AR19-100A

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 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 foreseeabl accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distribut 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 Working with U.S. Government partners, DHS and FBI identified Trojan malware variants used by the North Korean government. This malware va identified as HOPLIGHT. The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA. For more 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. Use should flag activity associated with the malware and report the activity to the Cybersecurity and Infrastructure Security Agency (CISA) or the FBI (and give the activity the highest priority for enhanced mitigation.

This report provides analysis of nine malicious executable files. Seven of these files are proxy applications that mask traffic between the malware operators. The proxies have the ability to generate fake TLS handshake sessions using valid public SSL certificates, disguising network connectio malicious actors. One file contains a public SSL certificate and the payload of the file appears to be encoded with a password or key. The remaini any of the public SSL certificates, but attempts outbound connections and drops four files. The dropped files primarily contain IP addresses and S For a downloadable copy of IOCs, see:

MAR-10135536-8.stix

Submitted Files (9)

05feed9762bc46b47a7dc5c469add9f163c16df4ddaafe81983a628da5714461 (23E27E5482E3F55BF828DAB8855690...)

12480585e08855109c5972e85d99cda7701fe992bc1754f1a0736f1eebcb004d (868036E102DF4CE414B0E6700825B3...)

2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525 (5C3898AC7670DA30CF0B22075F3E8E...)

4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761 (42682D4A78FE5C2EDA988185A34463...)

4c372df691fc699552f81c3d3937729f1dde2a2393f36c92ccc2bd2a033a0818 (C5DC53A540ABE95E02008A04A0D56D...)

70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3 (61E3571B8D9B2E9CCFADC3DDE10FB6...)

83228075a604e955d59edc760e4c4ed16eedabfc8f6ac291cf21b4fcbcd1f70a (3021B9EF74c&BDDF59656A035F94FD...)

d77fdabe17cdba62a8e728cbe6c740e2c2e541072501f77988674e07a05dfb39 (F8D26F2B8DD2AC4889597E1F2FD1F2...)

ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d (BE588CD29B9DC6F8CFC4D0AA5E5C79...)

Additional Files (4)

49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359 (rdpproto.dll)

70902623c9cd0cccc8513850072b70732d02c266c7b7e96d2d5b2ed4f5edc289 (udbcgiut.dat)

96a296d224f285c67bee93c30f8a309157f0daa35dc5b87e410b78630a09cfc7 (MSDFMAPI.INI)

cd5ff67ff773cc60c98c35f9e9d514b597cbd148789547ba152ba67bfc0fec8f (UDPTrcSvc.dll)

IPs (15)

112.175.92.57

113.114.117.122

128.200.115.228

137.139.135.151

181.39.135.126

186.169.2.237

197.211.212.59

21.252.107.198

26.165.218.44

47.206.4.145

70.224.36.194

81.94.192.10

81.94.192.147

84.49.242.125

97.90.44.200

Findings

05feed9762bc46b47a7dc5c469add9f163c16df4ddaafe81983a628da5714461

Tags

trojan

Details

Name	23E27E5482E3F55BF828DAB885569033
Size	242688 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	23e27e5482e3f55bf828dab885569033
SHA1	139b25e1ae32a8768238935a8c878bfbe2f89ef4
SHA256	05feed9762bc46b47a7dc5c469add9f163c16df4ddaafe81983a628da5714461
SHA512	2c481ef42dfc9a7a30575293d09a6f81943e307836ec5b8a346354ab5832c15046dd4015a65201311e33f944763fc55dd44fbe390245be
ssdeep	6144:YnDlYMzUvLFOL9wqk6+pqC8iooIBgajvQlm/Z0cp1:alYiXiooIKajvQeZ3
Entropy	6.537337

Antivirus

ESET	a variant of Win32/NukeSped.AI trojan
Symantec	Heur.AdvML.B

Yara Rules

hidden_cobra_consolidated.yara	rule crypt_constants_2 { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/04/19 "hidden_cobra" family = "n/a" description = "n/a" strings: $ = {efcdab90} $ = {558426fe} $ = {7856b4c2} cor 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }
hidden_cobra_consolidated.yara	rule lsfr_constants { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/04/19" cat "hidden_cobra" family = "n/a" description = "n/a" strings: $ = {efcdab90} $ = {558426fe} $ = {7856b4c2} cor 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }
hidden_cobra_consolidated.yara	rule polarSSL_servernames { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/ "hidden_cobra" family = "n/a" description = "n/a" strings: $polarSSL = "fjiejffndxklfsdkfjsaadiepwn" $sn1 = " $sn2 = "www.naver.com" condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) -- 0x4550) and ($polarS

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-06-05 21:57:29-04:00
Import Hash	ff390ec082b48263a3946814ea18ba46

PE Sections

MD5	Name	Raw Size	Entropy
c06924120c87e2cb79505e4ab0c2e192	header	1024	2.542817

3368eda2d5820605a055596c7c438f0f	.text	197120	6.441545
ec1f06839fa9bc10ad8e183b6bf7c1b5	.rdata	27136	5.956914
1e62b7d9f7cc48162e0651f7de314c8a	.data	8192	4.147893
980effd28a6c674865537f313318733a	.rsrc	512	5.090362
696fd5cac6e744f336e8ab68a4708fcf	.reloc	8704	5.247502

Packers/Compilers/Cryptors

Microsoft Visual C++ ?.?

Description

This artifact is a malicious PE32 executable. When executed the malware will collect system information about the victim machine including OS V Information, and System Time, as well as enumerate the system drives and partitions.

The malware is capable of the following functions:

---Begin Malware Capability---

Read, Write, and Move Files
Enumerate System Drives
Create and Terminate Processes
Inject into Running Processes
Create, Start and Stop Services
Modify Registry Settings
Connect to a Remote Host
Upload and Download Files

---End Malware Capability---

The malware is capable of opening and binding to a socket. The malware uses a public SSL certificate for secure communication. This certificate Naver.com is the largest search engine in Korea and provides a variety of web services to clients around the world.

---Begin SSL Certificate Header---

1 0 UNL10U
PolarSSL10UPolarSSL Test CA0
110212144407Z
2102121144407Z0<1 0 UNL10U
PolarSSL10UPolarSSL Client 200

---End SSL Certificate Header---

When executed, the malware will attempt a TLS Handshake with one of four hardcoded IP addresses embedded in the malware. These IP addres 'udbcgiut.dat' below. The malware also contains an embedded Zlib compression library that appears to further obfuscate the communications pay

The following notable strings have been linked to the use of the SSL certificates and can be used to identify the malware:

---Begin Notable Strings---

fjiejffndxklfsdkfjsaadiepwn
ofuierfsdkljffjoiejftyuir
reykfgkodfgkfdskgdfogpdokgsdfpg
ztretrtireotreotieroptkierert
etudjfirejer
yrty
uiyy
uiyiyj lildvucv
erfdfe poiiumwq

---End Notable Strings---

The next four artifacts contain identical characteristics as those described above. Therefore, only capability that is unique will be described for the
2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525

Tags

trojan

Details

Name	5C3898AC7670DA30CF0B22075F3E8ED6
Size	221184 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows

MD5	5c3898ac7670da30cf0b22075f3e8ed6
SHA1	91110c569a48b3ba92d771c5666a05781fdd6a57
SHA256	2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525
SHA512	700ec4d923cf0090f4428ac3d4d205b551c3e48368cf90d37f9831d8a57e73c73eb507d1731662321c723362c9318c3f019716991073d
ssdeep	3072:nKBzqEHcJw0sqz7vLFOLBAqui1mqLK1VaU9BzNRyHmdMaF0QqWN0Qjpthmu:nKg0cJ19z7vLFOLSqp0q7syHeFhnhm
Entropy	6.346504

Antivirus

ESET	a variant of Win32/NukeSped.AI trojan

Yara Rules

hidden_cobra_consolidated.yara	rule crypt_constants_2 { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/04/19 "hidden_cobra" family = "n/a" description = "n/a" strings: $ = {efcdab90} $ = {558426fe} $ = {7856b4c2} cor 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }
hidden_cobra_consolidated.yara	rule lsfr_constants { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/04/19" cat "hidden_cobra" family = "n/a" description = "n/a" strings: $ = {efcdab90} $ = {558426fe} $ = {7856b4c2} cor 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }
hidden_cobra_consolidated.yara	rule polarSSL_servernames { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/ "hidden_cobra" family = "n/a" description = "n/a" strings: $polarSSL = "fjiejffndxklfsdkfjsaadiepwn" $sn1 = " $sn2 = "www.naver.com" condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) -- 0x4550) and ($polar

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-05-16 02:35:55-04:00
Import Hash	6ffc5804961e26c43256df683fea6922

PE Sections

MD5	Name	Raw Size	Entropy
adb596d3ceae66510778e3bf5d4d9582	header	4096	0.695660
6453931a0b6192e0bbd6476e736ca63f	.text	184320	6.343388
0ba1433cc62ba7903ada2f1e57603e83	.rdata	16384	6.246206
76a08265777f68f08e5e6ed2102cb31d	.data	12288	4.050945
cb8939d6bc1cd076acd850c3850bdf78	.rsrc	4096	3.289605

Packers/Compilers/Cryptors

Microsoft Visual C++ v6.0

Relationships

2151c1977b...	Connected_To	81.94.192.147
2151c1977b...	Connected_To	112.175.92.57
2151c1977b...	Related_To	181.39.135.126
2151c1977b...	Related_To	197.211.212.59
2151c1977b...	Related_To	70902623c9cd0cccc8513850072b70732d02c266c7b7e96d2d5b2ed4f5edc289
2151c1977b...	Dropped	96a296d224f285c67bee93c30f8a309157f0daa35dc5b87e410b78630a09cfc7

Description

This artifact is a malicious PE32 executable with similar characteristics of those described in 23E27E5482E3F55BF828DAB885569033 above.

When this artifact is executed, it will write the file 'udbcgiut.dat' to C:\Users\<user>\AppData\Local\Temp.

The malware will then attempt outbound SSL connections to 81.94.192.147 and 112.175.92.57. Both connection attempts are over TCP Port 443.
The two IP addresses above, as well as the IP addresses 181.39.135.126 and 197.211.212.59 are hard-coded into the malware. However, only c
two IP addresses were attempted during analysis.

197.211.212.59

Ports

7443 TCP

Whois

```
inetnum:        197.211.208.0 - 197.211.215.255
netname:        ZOL-16e-MOBILE-CUSTOMERS
descr:          ZOL Customers on ZTE Mobile WiMAX Platform
country:        ZW
admin-c:        BS10-AFRINIC
admin-c:        GJ1-AFRINIC
admin-c:        JHM1-AFRINIC
tech-c:         BS10-AFRINIC
tech-c:         GJ1-AFRINIC
tech-c:         JHM1-AFRINIC
status:         ASSIGNED PA
mnt-by:         LIQUID-TOL-MNT
source:         AFRINIC # Filtered
parent:         197.211.192.0 - 197.211.255.255

person:         B Siwela
address:        3rd Floor Greenbridge South
address:        Eastgate Center
address:        R. Mugabe Road
address:        Harare
address:        Zimbabwe
phone:          +263774673452
fax-no:         +2634702375
nic-hdl:        BS10-AFRINIC
mnt-by:         GENERATED-DVCNVXWBH3VN3XZXTRPHOT0OJ77GUNN3-MNT
source:         AFRINIC # Filtered

person:         G Jaya
address:        3rd Floor Greenbridge South
address:        Eastgate Center
address:        R. Mugabe Road
address:        Harare
address:        Zimbabwe
phone:          +263773373135
fax-no:         +2634702375
nic-hdl:        GJ1-AFRINIC
mnt-by:         GENERATED-QPEEUIPPW1WPRZ5HLHRXAVHDOKWLC9UC-MNT
source:         AFRINIC # Filtered

person:         John H Mwangi
address:        Liquid Telecom Kenya
address:        P.O.Box 62499 - 00200
address:        Nairobi Kenya
address:        Nairobi, Kenya
address:        Kenya
phone:          + 254 20 556 755
```

Relationships

197.211.212.59	Related_To	2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525
197.211.212.59	Connected_From	ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d
197.211.212.59	Connected_From	70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3

Description

This IP address is listed in the file 'udbcgiut.dat'. Outbound SSL connection attempts are made to this IP by Malware2.exe, Malware3.exe, and Ma
domain, zol-ad-bdc.zol.co.zw is associated with the IP address, however, no DNS query is made for the name.

181.39.135.126

Ports

7443 TCP

Whois

inetnum: 181.39.135.120/29
status: reallocated
owner: Clientes Guayaquil
ownerid: EC-CLGU1-LACNIC
responsible: Tomislav Topic
address: Kennedy Norte Mz. 109 Solar 21, 5, Piso 2
address: 5934 - Guayaquil - GY
country: EC
phone: +593 4 2680555 [101]
owner-c: SEL
tech-c: SEL
abuse-c: SEL
created: 20160720
changed: 20160720
inetnum-up: 181.39/16

nic-hdl: SEL
person: Carlos Montero
e-mail: networking@TELCONET.EC
address: Kennedy Norte MZ, 109, Solar 21
address: 59342 - Guayaquil -
country: EC
phone: +593 42680555 [4601]
created: 20021004
changed: 20170323
Relationships

181.39.135.126	Related_To	2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525
181.39.135.126	Connected_From	ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d
181.39.135.126	Connected_From	70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3

Description

This IP address is listed in the file 'udbcgiut.dat'. Outbound SSL connection attempts are made to this IP by Malware2.exe, Malware3.exe, and Ma
is associated with the IP address.

112.175.92.57

Ports

443 TCP

Whois

inetnum: 112.160.0.0 - 112.191.255.255
netname: KORNET
descr: Korea Telecom
admin-c: IM667-AP
tech-c: IM667-AP
country: KR
status: ALLOCATED PORTABLE
mnt-by: MNT-KRNIC-AP
mnt-irt: IRT-KRNIC-KR
last-modified: 2017-02-03T02:21:58Z
source: APNIC

irt: IRT-KRNIC-KR
address: Seocho-ro 398, Seocho-gu, Seoul, Korea
e-mail: hostmaster@nic.or.kr
abuse-mailbox: hostmaster@nic.or.kr
admin-c: IM574-AP
tech-c: IM574-AP
auth: # Filtered
mnt-by: MNT-KRNIC-AP
last-modified: 2017-10-19T07:36:36Z
source: APNIC

person: IP Manager
address: Gyeonggi-do Bundang-gu, Seongnam-si Buljeong-ro 90
country: KR
phone: +82-2-500-6630
e-mail: kornet_ip@kt.com
nic-hdl: IM667-AP
mnt-by: MNT-KRNIC-AP
last-modified: 2017-03-28T06:37:04Z
source: APNIC
Relationships

112.175.92.57	Connected_From	2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525
112.175.92.57	Connected_From	ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d
112.175.92.57	Connected_From	70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3
112.175.92.57	Connected_From	83228075a604e955d59edc760e4c4ed16eedabfc8f6ac291cf21b4fcbcd1f70a

Description

This IP address is listed in the file 'udbcgiut.dat'. Outbound SSL connection attempts are made to this IP by Malware2.exe, Malware3.exe, and Ma
domain, mail.everzone.co.kr is associated with the IP address, however, no DNS query is made for the name.

81.94.192.147

Ports

443 TCP

Whois

inetnum: 81.94.192.0 - 81.94.192.255
netname: IOMARTHOSTING
descr: iomart Hosting Limited
country: GB
admin-c: RA1415-RIPE
tech-c: RA1415-RIPE
status: ASSIGNED PA
remarks: ABUSE REPORTS: abuse@redstation.com
mnt-by: REDSTATION-MNT
mnt-domains: REDSTATION-MNT
mnt-routes: REDSTATION-MNT
created: 2016-02-14T11:44:25Z
last-modified: 2016-02-14T11:44:25Z
source: RIPE

role: Redstation Admin Role
address: Redstation Limited
address: 2 Frater Gate Business Park
address: Aerodrome Road
address: Gosport
address: Hampshire
address: PO13 0GW
address: UNITED KINGDOM
abuse-mailbox: abuse@redstation.com
e-mail: abuse@redstation.com
nic-hdl: RA1415-RIPE
mnt-by: REDSTATION-MNT
created: 2005-04-22T17:34:33Z
last-modified: 2017-05-02T09:47:13Z
source: RIPE

% Information related to '81.94.192.0/24AS20860'

route: 81.94.192.0/24
descr: Wayne Dalton - Redstation Ltd
origin: AS20860
mnt-by: GB10488-RIPE-MNT
created: 2015-11-03T12:58:00Z
last-modified: 2015-11-03T12:58:00Z
source: RIPE

Relationships

81.94.192.147	Connected_From	2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525
81.94.192.147	Connected_From	ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d
81.94.192.147	Connected_From	70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3

Description

This IP address is listed in the file 'udbcgiut.dat'. Outbound SSL connection attempts are made to this IP by Malware2.exe, Malware3.exe, and Ma
is associated with the IP address.

70902623c9cd0cccc8513850072b70732d02c266c7b7e96d2d5b2ed4f5edc289

Details

Name	udbcgiut.dat

Size	1171 bytes
Type	data
MD5	ae829f55db0198a0a36b227addcdeeff
SHA1	04833210fa57ea70a209520f4f2a99d049e537f2
SHA256	70902623c9cd0cccc8513850072b70732d02c266c7b7e96d2d5b2ed4f5edc289
SHA512	1b4509102ac734ce310b6f8631b1bedd772a38582b4feda9fee09f1edd096006cf5ba528435c844effa97f95984b07bd2c111aa480bb22f
ssdeep	3:ElclFUl8GlFcmzkXlil23X1ll:ElcUXmQkXQ3
Entropy	0.395693

Antivirus

No matches found.

Yara Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

70902623c9...	Dropped_By	70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3
70902623c9...	Related_To	ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d
70902623c9...	Related_To	2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525
70902623c9...	Related_To	70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3
70902623c9...	Related_To	12480585e08855109c5972e85d99cda7701fe992bc1754f1a0736f1eebcb004d

Description

'udbcgiut.dat' is dropped by three of the four PE32 executables. This file contains a 32byte unicode string uniquely generated for the infected syst
socket pairs in hexidecimal.

---Begin Decoded Socket Pairs---

197.211.212.59:443
181.39.135.126:443
112.175.92.57:7443
81.94.192.147:7443

---End Decoded Socket Pairs---

The unicode string generated during this analysis was '8a9b11762b96c4b6'. The socket pairs remain the same for all instances of the malware.
For the PE32 executables, 'udbcgiut.dat' was dropped in the victim's profile at %AppData%\Local\Temp. For the 64bit executables, 'udbcgiut.dat'
C:\Windows.

4c372df691fc699552f81c3d3937729f1dde2a2393f36c92ccc2bd2a033a0818

Tags

trojan

Details

Name	C5DC53A540ABE95E02008A04A0D56D6C
Size	241152 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	c5dc53a540abe95e02008a04a0d56d6c
SHA1	4cfe9e353b1a91a2add627873846a3ad912ea96b
SHA256	4c372df691fc699552f81c3d3937729f1dde2a2393f36c92ccc2bd2a033a0818
SHA512	fc33c99facfbc98d164e63167353bdcff7c1704810e4bb64f7e56812412d84099b224086c04aea66e321cd546d8cf6f14196f5b58d5e931
ssdeep	6144:LA5cWD93YuzTvLFOLoqbWbnuX7ZEAV6efA/Pawzq:Xc93YbLZEAV6mX

Entropy	6.534884

Antivirus

ESET	a variant of Win32/NukeSped.AS trojan

Yara Rules

hidden_cobra_consolidated.yara	rule crypt_constants_2 { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/04/19 "hidden_cobra" family = "n/a" description = "n/a" strings: $ = {efcdab90} $ = {558426fe} $ = {7856b4c2} cor 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }
hidden_cobra_consolidated.yara	rule lsfr_constants { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/04/19" cat "hidden_cobra" family = "n/a" description = "n/a" strings: $ = {efcdab90} $ = {558426fe} $ = {7856b4c2} cor 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }
hidden_cobra_consolidated.yara	rule polarSSL_servernames { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/ "hidden_cobra" family = "n/a" description = "n/a" strings: $polarSSL = "fjiejffndxklfsdkfjsaadiepwn" $sn1 = " $sn2 = "www.naver.com" condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) -- 0x4550) and ($polarS

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-06-04 21:31:07-04:00
Import Hash	c76f6bb3f2ce6f4ce3e83448836f3ddd

PE Sections

MD5	Name	Raw Size	Entropy
64cb3246aafa83129f7fd6b25d572a9f	header	1024	2.625229
e8c15e136370c12020eb23545085b9f6	.text	196096	6.431942
cf0eb4ad22ac1ca687b87a0094999ac8	.rdata	26624	5.990247
b246681e20b3c8ff43e1fcf6c0335287	.data	8192	4.116777
6545248a1e3449e95314cbc874837096	.rsrc	512	5.112624
31a7ab6f707799d327b8425f6693c220	.reloc	8704	5.176231

Packers/Compilers/Cryptors

Microsoft Visual C++ ?.?

Description

This artifact is a malicious PE32 executable with similar characteristics of those described in 23E27E5482E3F55BF828DAB885569033 above.

This artifact appears to be named 'lamp.exe'. The malware contains the following debug pathway:

---Begin Debug Pathway---

Z:\Develop\41.LampExe\Release\LampExe.pdb

---End Debug Pathway---

ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d

Tags

adwaretrojan

Details

Name	BE588CD29B9DC6F8CFC4D0AA5E5C79AA
Name	ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d
Size	267776 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows

MD5	be588cd29b9dc6f8cfc4d0aa5e5c79aa
SHA1	06be4fe1f26bc3e4bef057ec83ae81bd3199c7fc
SHA256	ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d
SHA512	c074ec876350b3ee3f82208041152c0ecf25cc8600c8277eec389c253c12372e78da59182a6df8331b05e0eefb07c142172951115a582
ssdeep	6144:UEFpmt3md/iA3uiyzOvLFOLYqnHGZlDwf/OYy85eqmJKRPg:/PQ3mJxeigqi/OYy+/g
Entropy	6.554499

Antivirus

ESET	a variant of Win32/NukeSped.AI trojan
Filseclab	Adware.Amonetize.heur.xjym.mg

Yara Rules

hidden_cobra_consolidated.yara	rule crypt_constants_2 { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/04/19 "hidden_cobra" family = "n/a" description = "n/a" strings: $ = {efcdab90} $ = {558426fe} $ = {7856b4c2} cor 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }
hidden_cobra_consolidated.yara	rule lsfr_constants { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/04/19" cat "hidden_cobra" family = "n/a" description = "n/a" strings: $ = {efcdab90} $ = {558426fe} $ = {7856b4c2} cor 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }
hidden_cobra_consolidated.yara	rule polarSSL_servernames { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/ "hidden_cobra" family = "n/a" description = "n/a" strings: $polarSSL = "fjiejffndxklfsdkfjsaadiepwn" $sn1 = " $sn2 = "www.naver.com" condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) -- 0x4550) and ($polarS

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-06-06 10:33:38-04:00
Import Hash	8184d5d35e3a4640bb5d21698a4b6021

PE Sections

MD5	Name	Raw Size	Entropy
59b5d567b9b7b9da0ca0936675fd95fe	header	1024	2.658486
c0b6929e0f01a7b61bde3d7400a801e0	.text	218624	6.470188
ce1e5ab830fcfaa2d7bea92f56e9026e	.rdata	27136	5.962575
006bad003b65738ed203a576205cc546	.data	8192	4.157373
992987e022da39fcdbeede8ddd48f226	.rsrc	3072	5.511870
4be460324f0f4dc1f6a0983752094cce	.reloc	9728	5.303151

Packers/Compilers/Cryptors

Microsoft Visual C++ ?.?

Relationships

ddea408e17...	Connected_To	81.94.192.147
ddea408e17...	Connected_To	112.175.92.57
ddea408e17...	Connected_To	181.39.135.126
ddea408e17...	Connected_To	197.211.212.59
ddea408e17...	Related_To	70902623c9cd0cccc8513850072b70732d02c266c7b7e96d2d5b2ed4f5edc289
ddea408e17...	Connected_To	81.94.192.10

Description

This artifact is a malicious PE32 executable with similar characteristics of those described in 23E27E5482E3F55BF828DAB885569033 above.

This program attempts to initiate a TLS Handshake to the four IP/Port pairs listed in 'udbcgiut.dat'. If the program is unable to establish a connecti is deleted.

After 'udbcgiut.dat' is deleted, an outbound SSL connection is made to 81.94.192.10. The IP address is hard coded in the malware and are not ra

This artifact also loads several APIs that are commonly associated with Pass-The-Hash (PTH) toolkits, indicating a capability to harvest user cred

---Begin Common PTH APIs---

SamiChangePasswordUser
SamFreeMemory
SamCloseHandle
SamOpenUser
SamLookupNamesInDomain
SamOpenDomain
SamConnect

---End Common PTH APIs---
81.94.192.10

Whois

Domain name:
redstation.net.uk

Registrant:
Redstation Limited

Registrant type:
UK Limited Company, (Company number: 3590745)

Registrant's address:
2 Frater Gate Business Park
Aerodrome Road
Gosport
Hampshire
PO13 0GW
United Kingdom

Data validation:
Nominet was able to match the registrant's name and address against a 3rd party data source on 21-Feb-2017

Registrar:
Easyspace Ltd [Tag = EASYSPACE]
URL: https://www.easyspace.com/domain-names/extensions/uk

Relevant dates:
Registered on: 11-Apr-2005
Expiry date: 11-Apr-2019
Last updated: 12-Apr-2017

Registration status:
Registered until expiry date.

Name servers:
ns1.redstation.com
ns2.redstation.com

Relationships

81.94.192.10 Connected_From ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d

Description

A high port to high port connection attempt is made to this IP address from 'Malware5.dll'. No domain is associated with the IP address.

12480585e08855109c5972e85d99cda7701fe992bc1754f1a0736f1eebcb004d

Tags

trojan

Details

Name	868036E102DF4CE414B0E6700825B319
Size	453791 bytes
Type	PE32+ executable (GUI) x86-64, for MS Windows

MD5	868036e102df4ce414b0e6700825b319
SHA1	7f1e68d78e455aa14de9020abd2293c3b8ec6cf8
SHA256	12480585e08855109c5972e85d99cda7701fe992bc1754f1a0736f1eebcb004d
SHA512	724d83493dbe86cfcee7f655272d2c733baa5470d7da986e956c789aa1b8f518ad94b575e655b4fe5f6f7d426b9aa7d8304fc879b82a38
ssdeep	12288:eb/3G8vg+Rg1cvAHtE0MLa07rt5POui6z:+/3G8vg+pvi9Sa07rt4ui6z
Entropy	7.713852

Antivirus

NANOAV	Trojan.Win64.Crypted.excqpl

Yara Rules

No matches found.

ssdeep Matches

90	890d3928be0f36b1f4dcfffb20ac3747a31451ce010caba768974bfccdc26e7c

PE Metadata

Compile Date	2017-06-06 10:54:03-04:00
Import Hash	947a389c3886c5fa7f3e972fd4d7740c

PE Sections

MD5	Name	Raw Size	Entropy
e772c7a04c7e3d53c58fdb8a88bb0c02	header	1024	2.486400
a6a2750e5b57470403299e0327553042	.text	34816	6.297430
cc5d69374e9b0266a4b1119e5274d392	.rdata	12288	4.715650
ac4ee21fcb2501656efc217d139ec804	.data	5120	1.876950
359af12d4a14ced423d39736dfec613a	.pdata	2560	3.878158
097e0e4be076b795a7316f1746bace8a	.rsrc	3072	5.514584
5849f380266933d6f3c5c4740334b041	.reloc	1024	2.517963

Packers/Compilers/Cryptors

Microsoft Visual C++ 8.0 (DLL)

Relationships

12480585e0...	Related_To	70902623c9cd0cccc8513850072b70732d02c266c7b7e96d2d5b2ed4f5edc289
12480585e0...	Dropped	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359

Description

This artifact is a malicious x64 executable with similar characteristics of those described in 23E27E5482E3F55BF828DAB885569033 above.

In addition to the capabilities described above, this variant will hook the Windows Local Security Authority (lsass.exe). 'lsass.exe' will check the re
'rdpproto' under the key SYSTEM\CurrentControlSet\Control\Lsa Name: Security Packages. If not found, this value is added by 'lsass.exe'.
Next, the malware will drop the embedded file, 'rdpproto.dll' into the %System32% directory.
The file, 'udbcgiut.dat' is then written to C:\Windows. Outbound connection attempts are made to the socket pairs found within this file as describe
49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359

Tags

trojan

Details

Name	rdpproto.dll
Size	391680 bytes

Type	PE32+ executable (DLL) (console) x86-64, for MS Windows
MD5	dc268b166fe4c1d1c8595dccf857c476
SHA1	8264556c8a6e460760dc6bb72ecc6f0f966a16b8
SHA256	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359
SHA512	b47c4caa0b5c17c982fcd040c7171d36ec962fe32e9b8bec567ee14b187507fe90e026aa05eec17d36c49a924eeaed55e66c95a111cfa
ssdeep	6144:jfsTC8amAXJeZP6BPjIDeLkigDxcvAHjVXjhtBGshMLa1Mj7rtlkiP60dwtudIye:jvg+Rg1cvAHtE0MLa07rt5POui6
Entropy	7.893665

Antivirus

Avira	TR/Crypt.XPACK.xuqld
BitDefender	Trojan.Generic.22790108
ESET	a variant of Generik.MYWMFCM trojan
Emsisoft	Trojan.Generic.22790108 (B)
Ikarus	Trojan.SuspectCRC
NANOAV	Trojan.Win64.Crypted.excqpl

Yara Rules

No matches found.

ssdeep Matches

99 890d3928be0f36b1f4dcfffb20ac3747a31451ce010caba768974bfccdc26e7c

PE Metadata

Compile Date	2017-06-06 11:34:06-04:00
Import Hash	360d26520c50825099ec61e97b01a43b

PE Sections

MD5	Name	Raw Size	Entropy
3bb2a7d6aab283c82ab853f536157ce2	header	1024	2.524087
b0bf8ec7b067fd3592c0053702e34504	.text	23552	6.180871
6cc98c5fef3ea1b782262e355b5c5862	.rdata	10752	4.635336
484d4698d46b3b5ad033c1a80ba83acf	.data	4096	2.145716
a07c8f17c18c6789a3e757aec183aea6	.pdata	2048	3.729952
fae0d0885944745d98849422bd799457	.rsrc	348672	7.997488
0c1c23e1fb129b1b1966f70fc75cf20e	.reloc	1536	1.737829

Relationships

49757cf856...	Dropped_By	12480585e08855109c5972e85d99cda7701fe992bc1754f1a0736f1eebcb004d
49757cf856...	Connected_To	21.252.107.198
49757cf856...	Connected_To	70.224.36.194
49757cf856...	Connected_To	113.114.117.122
49757cf856...	Connected_To	47.206.4.145
49757cf856...	Connected_To	84.49.242.125
49757cf856...	Connected_To	26.165.218.44
49757cf856...	Connected_To	137.139.135.151

49757cf856...	Connected_To	97.90.44.200
49757cf856...	Connected_To	128.200.115.228
49757cf856...	Connected_To	186.169.2.237

Description

"rdpproto.dll" is dropped into the %System32% directory by 868036E102DF4CE414B0E6700825B319. When the library is loaded, "rdpproto.dll" will attempt to send SSL Client Hello packets to any of the following embedded IP addresses:

---Begin Embedded IP Addresses---

21.252.107.198
70.224.36.194
113.114.117.122
47.206.4.145
84.49.242.125
26.165.218.44
137.139.135.151
97.90.44.200
128.200.115.228
186.169.2.237

---End Embedded IP Addresses---

This artifact contains the following notable strings:

---Begin Notable Strings---

CompanyName
Adobe System Incorporated
FileDescription
MicrosoftWindows TransFilter/FilterType : 01 WindowsNT Service
FileVersion
6.1 Build 7601
InternalName
TCP/IP Packet Filter Service
LegalCopyright
Copyright 2015 - Adobe System Incorporated
LegalTrademarks
OriginalFileName
TCP/IP - PacketFilter

---End Notable Strings---
21.252.107.198

Ports

23164 TCP

Whois

NetRange: 21.0.0.0 - 21.255.255.255
CIDR: 21.0.0.0/8
NetName: DNIC-SNET-021
NetHandle: NET-21-0-0-0-1
Parent: ()
NetType: Direct Allocation
OriginAS:
Organization: DoD Network Information Center (DNIC)
RegDate: 1991-06-30
Updated: 2009-06-19
Ref: https://whois.arin.net/rest/net/NET-21-0-0-0-1

OrgName: DoD Network Information Center
OrgId: DNIC
Address: 3990 E. Broad Street
City: Columbus
StateProv: OH
PostalCode: 43218
Country: US
RegDate:
Updated: 2011-08-17
Ref: https://whois.arin.net/rest/org/DNIC

Relationships

21.252.107.198	Connected_From	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761

21.252.107.198 Connected_From 49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359

Description

A high port to high port connection attempt is made to this IP address from 'Malware2.dll'. No domain is associated with the IP address.

70.224.36.194

Ports

59681 TCP

Whois

Domain Name: AMERITECH.NET
Registry Domain ID: 81816_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://www.cscglobal.com/global/web/csc/digital-brand-services.html
Updated Date: 2017-06-09T05:27:34Z
Creation Date: 1996-06-14T04:00:00Z
Registry Expiry Date: 2018-06-13T04:00:00Z
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: 8887802723
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.ATTDNS.COM
Name Server: NS2.ATTDNS.COM
Name Server: NS3.ATTDNS.COM
Name Server: NS4.ATTDNS.COM
DNSSEC: unsigned

Domain Name: ameritech.net
Registry Domain ID: 81816_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2017-06-09T05:27:34Z
Creation Date: 1996-06-14T04:00:00Z
Registrar Registration Expiration Date: 2018-06-13T04:00:00Z
Registrar: CSC CORPORATE DOMAINS, INC.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: AT&T SERVICES, INC.
Registrant Street: 801 Chestnut Street
Registrant City: Saint Louis
Registrant State/Province: MO
Registrant Postal Code: 63101
Registrant Country: US
Registrant Phone: +1.3142358168
Registrant Phone Ext:
Registrant Fax: +1.3142358168
Registrant Fax Ext:
Registrant Email: att-domains@att.com
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: AT&T SERVICES, INC.
Admin Street: 801 Chestnut Street
Admin City: Saint Louis
Admin State/Province: MO
Admin Postal Code: 63101
Admin Country: US
Admin Phone: +1.3142358168
Admin Phone Ext:
Admin Fax: +1.3142358168
Admin Fax Ext:
Admin Email: att-domains@att.com
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: AT&T SERVICES, INC.
Tech Street: 801 Chestnut Street
Tech City: Saint Louis
Tech State/Province: MO
Tech Postal Code: 63101
Tech Country: US
Tech Phone: +1.3142358168
Tech Phone Ext:

Tech Fax: +1.3142358168
Tech Fax Ext:
Tech Email: att-domains@att.com
Name Server: ns3.attdns.com
Name Server: ns1.attdns.com
Name Server: ns2.attdns.com
Name Server: ns4.attdns.com
DNSSEC: unsigned
Relationships

70.224.36.194	Connected_From	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
70.224.36.194	Connected_From	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359

Description

A high port to high port connection attempt is made to this IP address from 'Malware2.dll'. No domain is associated with the IP address.

113.114.117.122

Ports

23397 TCP

Whois

inetnum: 113.112.0.0 - 113.119.255.255
netname: CHINANET-GD
descr: CHINANET Guangdong province network
descr: Data Communication Division
descr: China Telecom
country: CN
admin-c: CH93-AP
tech-c: IC83-AP
remarks: service provider
status: ALLOCATED PORTABLE
mnt-by: APNIC-HM
mnt-lower: MAINT-CHINANET-GD
mnt-routes: MAINT-CHINANET-GD
last-modified: 2016-05-04T00:15:17Z
source: APNIC
mnt-irt: IRT-CHINANET-CN

irt: IRT-CHINANET-CN
address: No.31 ,jingrong street,beijing
address: 100032
e-mail: anti-spam@ns.chinanet.cn.net
abuse-mailbox: anti-spam@ns.chinanet.cn.net
admin-c: CH93-AP
tech-c: CH93-AP
auth: # Filtered
mnt-by: MAINT-CHINANET
last-modified: 2010-11-15T00:31:55Z
source: APNIC

person: Chinanet Hostmaster
nic-hdl: CH93-AP
e-mail: anti-spam@ns.chinanet.cn.net
address: No.31 ,jingrong street,beijing
address: 100032
phone: +86-10-58501724
fax-no: +86-10-58501724
country: CN
mnt-by: MAINT-CHINANET
last-modified: 2014-02-27T03:37:38Z
source: APNIC

person: IPMASTER CHINANET-GD
nic-hdl: IC83-AP
e-mail: gdnoc_HLWI@189.cn
address: NO.18,RO. ZHONGSHANER,YUEXIU DISTRIC,GUANGZHOU
phone: +86-20-87189274
fax-no: +86-20-87189274
country: CN
mnt-by: MAINT-CHINANET-GD
remarks: IPMASTER is not for spam complaint,please send spam complaint to abuse_gdnoc@189.cn
abuse-mailbox: antispam_gdnoc@189.cn
last-modified: 2014-09-22T04:41:26Z
source: APNIC
Relationships

113.114.117.122	Connected_From	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
113.114.117.122	Connected_From	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359

Description

A high port to high port connection attempt is made to this IP address from 'Malware2.dll'. No domain is associated with the IP address.

47.206.4.145

Ports

59067 TCP

Whois

Domain Name: FRONTIERNET.NET
Registry Domain ID: 4305589_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.register.com
Registrar URL: http://www.register.com
Updated Date: 2017-09-14T07:53:05Z
Creation Date: 1995-10-14T04:00:00Z
Registry Expiry Date: 2018-10-13T04:00:00Z
Registrar: Register.com, Inc.
Registrar IANA ID: 9
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: AUTH.DLLS.PA.FRONTIERNET.NET
Name Server: AUTH.FRONTIERNET.NET
Name Server: AUTH.LKVL.MN.FRONTIERNET.NET
Name Server: AUTH.ROCH.NY.FRONTIERNET.NET
DNSSEC: unsigned

Domain Name: FRONTIERNET.NET
Registry Domain ID: 4305589_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.register.com
Registrar URL: www.register.com
Updated Date: 2017-09-14T00:53:05.00Z
Creation Date: 1995-10-14T04:00:00.00Z
Registrar Registration Expiration Date: 2018-10-13T04:00:00.00Z
Registrar: REGISTER.COM, INC.
Registrar IANA ID: 9
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: FRONTIERNET HOSTMASTER
Registrant Organization:
Registrant Street: 95 N. FITZHUGH ST.
Registrant City: ROCHESTER
Registrant State/Province: NY
Registrant Postal Code: 14614-1212
Registrant Country: US
Registrant Phone: +1.8664747662
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: HOSTMASTER@FRONTIERNET.NET
Registry Admin ID:
Admin Name: FRONTIERNET HOSTMASTER
Admin Organization:
Admin Street: 95 N. FITZHUGH ST.
Admin City: ROCHESTER
Admin State/Province: NY
Admin Postal Code: 14614-1212
Admin Country: US
Admin Phone: +1.8664747662
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: HOSTMASTER@FRONTIERNET.NET
Registry Tech ID:
Tech Name: FRONTIERNET HOSTMASTER
Tech Organization:
Tech Street: 95 N. FITZHUGH ST.
Tech City: ROCHESTER
Tech State/Province: NY
Tech Postal Code: 14614-1212
Tech Country: US
Tech Phone: +1.8664747662
Tech Phone Ext:

Tech Fax:
Tech Fax Ext:
Tech Email: HOSTMASTER@FRONTIERNET.NET
Name Server: AUTH.DLLS.PA.FRONTIERNET.NET
Name Server: AUTH.FRONTIERNET.NET
Name Server: AUTH.LKVL.MN.FRONTIERNET.NET
Name Server: AUTH.ROCH.NY.FRONTIERNET.NET
DNSSEC: unSigned
Relationships

47.206.4.145	Connected_From	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
47.206.4.145	Connected_From	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359

Description

A high port to high port connection attempt is made to this IP address from 'Malware2.dll'. No domain is associated with the IP address.

84.49.242.125

Ports

17770 TCP

Whois

Domain Name: NEXTGENTEL.COM
Registry Domain ID: 13395561_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.domaininfo.com
Registrar URL: http://www.ports.domains
Updated Date: 2017-11-10T23:44:50Z
Creation Date: 1999-11-17T15:47:51Z
Registry Expiry Date: 2018-11-17T15:47:51Z
Registrar: Ports Group AB
Registrar IANA ID: 73
Registrar Abuse Contact Email: abuse@portsgroup.se
Registrar Abuse Contact Phone: +46.707260017
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: ANYADNS1.NEXTGENTEL.NET
Name Server: ANYADNS2.NEXTGENTEL.NET
DNSSEC: unsigned

Domain Name: nextgentel.com
Registry Domain ID: 13395561_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.domaininfo.com
Registrar URL: ports.domains
Updated Date: 2017-11-10T23:44:50Z
Creation Date: 1999-11-17T15:47:51Z
Registrar Registration Expiration Date: 2018-11-17T15:47:51Z
Registrar: PortsGroup AB
Registrar IANA ID: 73
Registrar Abuse Contact Email: abuse@portsgroup.se
Registrar Abuse Contact Phone: +46.317202000
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Hostmaster
Registrant Organization: NextGenTel AS
Registrant Street: Sandslimarka 31
Registrant City: SANDSLI
Registrant State/Province:
Registrant Postal Code: 5254
Registrant Country: NO
Registrant Phone: +47.55527900
Registrant Fax: +47.55527910
Registrant Email: hostmaster@nextgentel.com
Registry Admin ID:
Admin Name: Hostmaster
Admin Organization: NextGenTel AS
Admin Street: Sandslimarka 31
Admin City: Sandsli
Admin State/Province:
Admin Postal Code: 5254
Admin Country: NO
Admin Phone: +47.55527900
Admin Fax: +47.55527910
Admin Email: hostmaster@nextgentel.com
Registry Tech ID:
Tech Name: Hostmaster v/ Eivind Olsen
Tech Organization: NextGenTel AS
Tech Street: Postboks 3 Sandsli

Tech City: Bergen
Tech State/Province:
Tech Postal Code: 5861
Tech Country: NO
Tech Phone: +47.41649322
Tech Fax: +47.55527910
Tech Email: hostmaster@nextgentel.com
Name Server: ANYADNS1.NEXTGENTEL.NET
Name Server: ANYADNS2.NEXTGENTEL.NET
DNSSEC: unsigned
Relationships

84.49.242.125	Connected_From	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
84.49.242.125	Connected_From	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359

Description

A high port to high port connection attempt is made to this IP address from 'Malware2.dll'. No domain is associated with the IP address.

26.165.218.44

Ports

2248 TCP

Whois

NetRange: 26.0.0.0 - 26.255.255.255
CIDR: 26.0.0.0/8
NetName: DISANET26
NetHandle: NET-26-0-0-0-1
Parent: ()
NetType: Direct Allocation
OriginAS:
Organization: DoD Network Information Center (DNIC)
RegDate: 1995-04-30
Updated: 2009-06-19
Ref: https://whois.arin.net/rest/net/NET-26-0-0-0-1

OrgName: DoD Network Information Center
OrgId: DNIC
Address: 3990 E. Broad Street
City: Columbus
StateProv: OH
PostalCode: 43218
Country: US
RegDate:
Updated: 2011-08-17
Ref: https://whois.arin.net/rest/org/DNIC

OrgTechHandle: MIL-HSTMST-ARIN
OrgTechName: Network DoD
OrgTechPhone: +1-844-347-2457
OrgTechEmail: disa.columbus.ns.mbx.hostmaster-dod-nic@mail.mil
OrgTechRef: https://whois.arin.net/rest/poc/MIL-HSTMST-ARIN

OrgAbuseHandle: REGIS10-ARIN
OrgAbuseName: Registration
OrgAbusePhone: +1-844-347-2457
OrgAbuseEmail: disa.columbus.ns.mbx.arin-registrations@mail.mil
OrgAbuseRef: https://whois.arin.net/rest/poc/REGIS10-ARIN

OrgTechHandle: REGIS10-ARIN
OrgTechName: Registration
OrgTechPhone: +1-844-347-2457
OrgTechEmail: disa.columbus.ns.mbx.arin-registrations@mail.mil
OrgTechRef: https://whois.arin.net/rest/poc/REGIS10-ARIN
Relationships

26.165.218.44	Connected_From	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
26.165.218.44	Connected_From	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359

Description

A high port to high port connection attempt is made to this IP address from 'Malware2.dll'. No domain is associated with the IP address.

137.139.135.151

Ports

64694 TCP

Whois

NetRange: 137.139.0.0 - 137.139.255.255
CIDR: 137.139.0.0/16
NetName: SUC-OLDWEST
NetHandle: NET-137-139-0-0-1
Parent: NET137 (NET-137-0-0-0-0)
NetType: Direct Assignment
OriginAS:
Organization: SUNY College at Old Westbury (SCAOW)
RegDate: 1989-11-29
Updated: 2014-02-18
Ref: https://whois.arin.net/rest/net/NET-137-139-0-0-1

OrgName: SUNY College at Old Westbury
OrgId: SCAOW
Address: 223 Store Hill Road
City: Old Westbury
StateProv: NY
PostalCode: 11568
Country: US
RegDate: 1989-11-29
Updated: 2011-09-24
Ref: https://whois.arin.net/rest/org/SCAOW

OrgTechHandle: SUNYO-ARIN
OrgTechName: SUNYOWNOC
OrgTechPhone: +1-516-876-3379
OrgTechEmail: sunyownoc@oldwestbury.edu
OrgTechRef: https://whois.arin.net/rest/poc/SUNYO-ARIN

OrgAbuseHandle: SUNYO-ARIN
OrgAbuseName: SUNYOWNOC
OrgAbusePhone: +1-516-876-3379
OrgAbuseEmail: sunyownoc@oldwestbury.edu
OrgAbuseRef: https://whois.arin.net/rest/poc/SUNYO-ARIN

RAbuseHandle: SUNYO-ARIN
RAbuseName: SUNYOWNOC
RAbusePhone: +1-516-876-3379
RAbuseEmail: sunyownoc@oldwestbury.edu
RAbuseRef: https://whois.arin.net/rest/poc/SUNYO-ARIN

RTechHandle: SUNYO-ARIN
RTechName: SUNYOWNOC
RTechPhone: +1-516-876-3379
RTechEmail: sunyownoc@oldwestbury.edu
RTechRef: https://whois.arin.net/rest/poc/SUNYO-ARIN

RNOCHandle: SUNYO-ARIN
RNOCName: SUNYOWNOC
RNOCPhone: +1-516-876-3379
RNOCEmail: sunyownoc@oldwestbury.edu
RNOCRef: https://whois.arin.net/rest/poc/SUNYO-ARIN

Relationships

137.139.135.151	Connected_From	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
137.139.135.151	Connected_From	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359

Description

A high port to high port connection attempt is made to this IP address from 'Malware2.dll'. No domain is associated with the IP address.

97.90.44.200

Ports

37120 TCP

Whois

Domain Name: CHARTER.COM
Registry Domain ID: 340223_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2017-07-03T04:22:18Z
Creation Date: 1994-07-30T04:00:00Z
Registry Expiry Date: 2019-07-29T04:00:00Z

Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS1.CHARTER.COM
Name Server: NS2.CHARTER.COM
Name Server: NS3.CHARTER.COM
Name Server: NS4.CHARTER.COM
DNSSEC: unsigned

Domain Name: charter.com
Registry Domain ID: 340223_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2017-12-18T04:00:14-0800
Creation Date: 1994-07-29T21:00:00-0700
Registrar Registration Expiration Date: 2019-07-28T21:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Registry Registrant ID:
Registrant Name: Domain Admin
Registrant Organization: Charter Communications Operating, LLC
Registrant Street: 12405 Powerscourt Drive,
Registrant City: Saint Louis
Registrant State/Province: MO
Registrant Postal Code: 63131
Registrant Country: US
Registrant Phone: +1.3149650555
Registrant Phone Ext:
Registrant Fax: +1.9064010617
Registrant Fax Ext:
Registrant Email: hostmaster@charter.com
Registry Admin ID:
Admin Name: Domain Admin
Admin Organization: Charter Communications Operating, LLC
Admin Street: 12405 Powerscourt Drive,
Admin City: Saint Louis
Admin State/Province: MO
Admin Postal Code: 63131
Admin Country: US
Admin Phone: +1.3149650555
Admin Phone Ext:
Admin Fax: +1.9064010617
Admin Fax Ext:
Admin Email: hostmaster@charter.com
Registry Tech ID:
Tech Name: Charter Communications Internet Security and Abuse
Tech Organization: Charter Communications Operating, LLC
Tech Street: 12405 Powerscourt Drive,
Tech City: Saint Louis
Tech State/Province: MO
Tech Postal Code: 63131
Tech Country: US
Tech Phone: +1.3142883111
Tech Phone Ext:
Tech Fax: +1.3149090609
Tech Fax Ext:
Tech Email: abuse@charter.net
Name Server: ns4.charter.com
Name Server: ns3.charter.com
Name Server: ns1.charter.com
Name Server: ns2.charter.com
DNSSEC: unsigned

Relationships

97.90.44.200	Connected_From	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
97.90.44.200	Connected_From	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359

Description

A high port to high port connection attempt is made to this IP address from 'Malware2.dll'. No domain is associated with the IP address.

128.200.115.228

Ports

52884 TCP

Whois

Domain Name: UCI.EDU

Registrant:
University of California, Irvine
6366 Ayala Science Library
Irvine, CA 92697-1175
UNITED STATES

Administrative Contact:
Con Wieland
University of California, Irvine
Office of Information Technology
6366 Ayala Science Library
Irvine, CA 92697-1175
UNITED STATES
(949) 824-2222
oit-nsp@uci.edu

Technical Contact:
Con Wieland
University of California, Irvine
Office of Information Technology
6366 Ayala Science Library
Irvine, CA 92697-1175
UNITED STATES
(949) 824-2222
oit-nsp@uci.edu

Name Servers:
NS4.SERVICE.UCI.EDU 128.200.59.190
NS5.SERVICE.UCI.EDU 52.26.131.47

Domain record activated: 30-Sep-1985
Domain record last updated: 07-Jul-2016
Domain expires: 31-Jul-2018

Relationships

128.200.115.228	Connected_From	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
128.200.115.228	Connected_From	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359

Description

A high port to high port connection attempt is made to this IP address from 'Malware2.dll'. No domain is associated with the IP address.

186.169.2.237

Ports

65292 TCP

Whois

inetnum: 186.168/15
status: allocated
aut-num: N/A
owner: COLOMBIA TELECOMUNICACIONES S.A. ESP
ownerid: CO-CTSE-LACNIC
responsible: Administradores Internet
address: Transversal 60, 114, A 55
address: N - BOGOTA - Cu
country: CO
phone: +57 1 5339833 []
owner-c: CTE7
tech-c: CTE7
abuse-c: CTE7
inetrev: 186.169/16
nserver: DNS5.TELECOM.COM.CO
nsstat: 20171220 AA
nslastaa: 20171220
nserver: DNS.TELECOM.COM.CO
nsstat: 20171220 AA

nslastaa: 20171220
created: 20110404
changed: 20141111

nic-hdl: CTE7
person: Grupo de Administradores Internet
e-mail: admin.internet@TELECOM.COM.CO
address: Transversal, 60, 114 A, 55
address: 571111 - BOGOTA DC - CU
country: CO
phone: +57 1 7050000 [71360]
created: 20140220
changed: 20140220

Relationships

186.169.2.237	Connected_From	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
186.169.2.237	Connected_From	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359

Description

A high port to high port connection attempt is made to this IP address from 'Malware2.dll'. No domain is associated with the IP address.

4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761

Tags

trojan

Details

Name	42682D4A78FE5C2EDA988185A344637D
Name	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
Size	346624 bytes
Type	PE32+ executable (DLL) (console) x86-64, for MS Windows
MD5	42682d4a78fe5c2eda988185a344637d
SHA1	4975de2be0a1f7202037f5a504d738fe512191b7
SHA256	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
SHA512	213e4a0afbfac0bd884ab262ac87aee7d9a175cff56ba11aa4c75a4feb6a96c5e4e2c26adbe765f637c783df7552a56e4781a3b17be5fda
ssdeep	6144:nCgsFAkxS1rrtZQXTip12P04nTnvze6lxjWV346vze6lpjWV34Evze6lSjWV34a7:nCgsukxS1vtZ+5nvze6lxjWV346vze6N
Entropy	6.102810

Antivirus

ESET	a variant of Win64/NukeSped.T trojan

Yara Rules

hidden_cobra_consolidated.yara	rule crypt_constants_2 { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/04/19 "hidden_cobra" family = "n/a" description = "n/a" strings: $ = {efcdab90} $ = {558426fe} $ = {7856b4c2} cor 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }
hidden_cobra_consolidated.yara	rule lsfr_constants { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/04/19" cat "hidden_cobra" family = "n/a" description = "n/a" strings: $ = {efcdab90} $ = {558426fe} $ = {7856b4c2} cor 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }
hidden_cobra_consolidated.yara	rule polarSSL_servernames { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/ "hidden_cobra" family = "n/a" description = "n/a" strings: $polarSSL = "fjiejffndxklfsdkfjsaadiepwn" $sn1 = " $sn2 = "www.naver.com" condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) -- 0x4550) and ($polarS

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-06-06 11:24:44-04:00
Import Hash	e395fbfa0104d0173b3c4fdd3debdceb

Company Name	Kamsky Co,.Ltd
File Description	Vote_Controller
Internal Name	MDL_170329_x86_V06Lv3
Legal Copyright	Copyright \u24d2 2017
Original Filename	Vote_Controller
Product Name	Kamsky ColdFear
Product Version	17, 0, 0, 0

PE Sections

MD5	Name	Raw Size	Entropy
40d66d1a2f846d7c3bf291c604c9fca3	header	1024	2.628651
d061ffec6721133c433386c96520bc55	.text	284160	5.999734
cbbc6550dcbdcaf012bdbf758a377779	.rdata	38912	5.789426
c83bcaab05056d5b84fc609f41eed210	.data	7680	3.105496
b9fc36206883aa1902566b5d01c27473	.pdata	8704	5.319307
1c1d46056b4cb4627a5f92112b7e09f7	.rsrc	4096	5.608168
3baedaa3d6b6d6dc9fb0ec4f5c3b007c	.reloc	2048	2.331154

Relationships

4a74a9fd40...	Connected_To	21.252.107.198
4a74a9fd40...	Connected_To	70.224.36.194
4a74a9fd40...	Connected_To	113.114.117.122
4a74a9fd40...	Connected_To	47.206.4.145
4a74a9fd40...	Connected_To	84.49.242.125
4a74a9fd40...	Connected_To	26.165.218.44
4a74a9fd40...	Connected_To	137.139.135.151
4a74a9fd40...	Connected_To	97.90.44.200
4a74a9fd40...	Connected_To	128.200.115.228
4a74a9fd40...	Connected_To	186.169.2.237

Description

This artifact is a malicious 64bit Windows dynamic library called 'Vote_Controller.dll'. The file shares similar functionality with 'rdpproto.dll' above, a
to the same ten IP addresses.

42682D4A78FE5C2EDA988185A344637D also contains the same public SSL certificate as many of the artifacts above.

The file contains the following notable strings:

---Begin Notable Strings---

CompanyName
Kamsky Co, .Ltd
FileDescription
Vote_Controller
FileVersion
49, 0, 0, 0
InternalName
MDL_170329_x86_V06Lv3
LegalCopyright
Copyright
2017
LegalTrademarks
OriginalFileName

Vote_Controller
PrivateBuild
ProductName
Kamsky ColdFear
ProductVersion
17, 0, 0, 0

---End Notable Strings---
83228075a604e955d59edc760e4c4ed16eedabfc8f6ac291cf21b4fcbcd1f70a

Details

Name	3021B9EF74c&BDDF59656A035F94FD08
Name	83228075a604e955d59edc760e4c4ed16eedabfc8f6ac291cf21b4fcbcd1f70a
Size	245760 bytes
Type	PE32+ executable (DLL) (console) x86-64, for MS Windows
MD5	3021b9ef74c7bddf59656a035f94fd08
SHA1	05ad5f346d0282e43360965373eb2a8d39735137
SHA256	83228075a604e955d59edc760e4c4ed16eedabfc8f6ac291cf21b4fcbcd1f70a
SHA512	f8fcc5ed34b7bf144fc708d01d9685f0cb2e678c173d014987d6ecbf4a7c3ed539452819237173a2ab14609a913cf46c3bd618cffe7b599(
ssdeep	6144:4+ZmN/ix9bd+Rvze6lxjWV346vze6lpjWV34Evze6lSjWV34avze6lkjWV34z5FT:4+ZmN/ix9b8Rvze6lxjWV346vze6lpjn
Entropy	5.933390

Antivirus

No matches found.

Yara Rules

hidden_cobra_consolidated.yara	rule crypt_constants_2 { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/04/19 "hidden_cobra" family = "n/a" description = "n/a" strings: $ = {efcdab90} $ = {558426fe} $ = {7856b4c2} cor 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }
hidden_cobra_consolidated.yara	rule lsfr_constants { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/04/19" cat "hidden_cobra" family = "n/a" description = "n/a" strings: $ = {efcdab90} $ = {558426fe} $ = {7856b4c2} cor 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }
hidden_cobra_consolidated.yara	rule polarSSL_servernames { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/ "hidden_cobra" family = "n/a" description = "n/a" strings: $polarSSL = "fjiejffndxklfsdkfjsaadiepwn" $sn1 = " $sn2 = "www.naver.com" condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) -- 0x4550) and ($polar

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-05-16 02:44:21-04:00
Import Hash	ca767ccbffbed559cbe77c923e3af1f8
Company Name	Kamsky Co,.Ltd
File Description	Vote_Controller
Internal Name	MDL_170329_x86_V06Lv3
Legal Copyright	Copyright \u24d2 2017
Original Filename	Vote_Controller
Product Name	Kamsky ColdFear
Product Version	17, 0, 0, 0

PE Sections

MD5	Name	Raw Size	Entropy
83ec15e3cf335f784144db4208b328c9	header	1024	2.790421

036c57e89ea3a6afa819c242c5816b70	.text	206848	5.688491
4812d2f39e9a8ae569370d423ba31344	.rdata	26112	6.000116
cb41e8f63b7c22c401a0634cb4fe1909	.data	2048	4.748331
3cc7651747904bfe94ed18f44354a706	.pdata	5120	4.962073
9e92c54604ea67e76210c3c914e9608c	.rsrc	4096	5.606351
71dcfb1ec7257ee58dcc20cafb0be691	.reloc	512	0.673424

Relationships

83228075a6... Connected_To 112.175.92.57

Description

This artifact is 64bit Windows dynamic library file which shares many of the same characteristics and name (Vote_Controller.dll) as 42682D4A78FE5C2EDA988185A344637D above.

When this library is loaded it will look for the file 'udbcgiut.dat' in C:\WINDOWS. If 'udbcgiut.dat' is not found, the file will attempt connections to th addresses described under 'rdpproto.dll' above.

One notable difference with this variant is that it uses the Windows Management Instrumentation (WMI) process to recompile the Managed Objec the WMI repository. At runtime, the malware will enumerate the drivers located in the registry at HKLM\Software\WBEM\WDM.
These files are then recompiled by invoking wmiprvse.exe through svchost.exe: "C:\Windows\system32\wbem\wmiprvse.exe -Embedding".
MOF files are written in a SQL-like language and are run (compiled) by the operating system when a predetermined event takes place. Recent ma been observed modifying the MOF files within the system registry to run specific commands and create persistency on the system.

Of note, the paravirtual SCSI driver for VMWare Tools is also located in HKLM\Software\WBEM\WDM within a virtual image. When this driver is re malware, VMWare Tools no longer works. It cannot be determined if this is an intentional characteristic of the malware to hinder analysis, or simpl method used to establish persistence.
70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3

Tags

trojan

Details

Name	61E3571B8D9B2E9CCFADC3DDE10FB6E1
Size	258052 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	61e3571b8d9b2e9ccfadc3dde10fb6e1
SHA1	55daa1fca210ebf66b1a1d2db1aa3373b06da680
SHA256	70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3
SHA512	235f7b920f54c4d316386cbf6cc14db1929029e8053270e730be15acc8e9f333231d2d984681bea26013a1d1cf4670528ba0989337be1
ssdeep	6144:d71TKN7LBHvS+bujAfrsxwkm1Ka5l7gTtJUGx:dxKHPuj8WR0K6VgTtZx
Entropy	7.829590

Antivirus

BitDefender	Dropped:Trojan.GenericKD.30867638
ESET	a variant of Win32/NukeSped.AI trojan
Emsisoft	Dropped:Trojan.GenericKD.30867638 (B)

Yara Rules

hidden_cobra_consolidated.yara	rule crypt_constants_2 { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/04/19 "hidden_cobra" family = "n/a" description = "n/a" strings: $ = {efcdab90} $ = {558426fe} $ = {7856b4c2} cor 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }
hidden_cobra_consolidated.yara	rule lsfr_constants { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/04/19" cat "hidden_cobra" family = "n/a" description = "n/a" strings: $ = {efcdab90} $ = {558426fe} $ = {7856b4c2} cor 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2016-08-23 00:19:59-04:00
Import Hash	8e253f83371d82907ff72f57257e3810

PE Sections

MD5	Name	Raw Size	Entropy
84f39a6860555231d60a55c72d07bc5e	header	4096	0.586304
649c24790b60bda1cf2a85516bfc7fa0	.text	24576	5.983290
fbd6ca444ef8c0667aed75820cc99dce	.rdata	4096	3.520964
0ecb4bcb0a1ef1bf8ea4157fabdd7357	.data	4096	3.988157

Packers/Compilers/Cryptors

Installer VISE Custom

Relationships

70034b33f5...	Dropped	cd5ff67ff773cc60c98c35f9e9d514b597cbd148789547ba152ba67bfc0fec8f
70034b33f5...	Dropped	70902623c9cd0cccc8513850072b70732d02c266c7b7e96d2d5b2ed4f5edc289
70034b33f5...	Dropped	96a296d224f285c67bee93c30f8a309157f0daa35dc5b87e410b78630a09cfc7
70034b33f5...	Connected_To	81.94.192.147
70034b33f5...	Connected_To	112.175.92.57
70034b33f5...	Connected_To	181.39.135.126
70034b33f5...	Connected_To	197.211.212.59
70034b33f5...	Related_To	70902623c9cd0cccc8513850072b70732d02c266c7b7e96d2d5b2ed4f5edc289

Description

This artifact is a malicious PE32 executable. When executed, the artifact sets up the service, 'Network UDP Trace Management Service'.
To set up the service, the program drops a dynamic library, 'UDPTrcSvc.dll' into the %System32% directory.
Next, the following registry keys are added:

---Begin Registry Keys---

HKLM\SYSTEM\CurrentControlSet\services\UDPTrcSvc Name: Type Value: 20
HKLM\SYSTEM\CurrentControlSet\services\UDPTrcSvc Name: Start Value: 02
HKLM\SYSTEM\CurrentControlSet\services\UDPTrcSvc Name: ImagePath Value: "%SystemRoot%\System32\svchost.exe -k mdnetuse"
HKLM\SYSTEM\CurrentControlSet\services\UDPTrcSvc Name: DisplayName Value: "Network UDP Trace Management Service"
HKLM\SYSTEM\CurrentControlSet\services\UDPTrcSvc Name: ObjectName Value: "LocalSystem"
HKLM\SYSTEM\CurrentControlSet\services\UDPTrcSvc\Parameters Name: ServiceDll Value: "%SystemRoot%\System32\svchost.exe -k mdnetu
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost\mdnetuse

---End Registry Keys---

The service is started by invoking svchost.exe.

After writing 'UDPTrcSvd.dll' to disk, the program drops two additional files. Similar to 5C3898AC7670DA30CF0B22075F3E8ED6 above, the prog
'udbcgiut.dat' to the victim's profile at %AppData/Local/Temp%. A second file is written to the victim's profile in the %AppData/Local/VirtualStore/V
identified as 'MSDFMAPI.INI'. 'MSDFMAPI.INI' is also written to C:\WINDOWS. More information on the content of these files is below.

61E3571B8D9B2E9CCFADC3DDE10FB6E1 attempts the same outbound connections as 5C3898AC7670DA30CF0B22075F3E8ED6, however t
any of the public SSL certificates referenced above.
cd5ff67ff773cc60c98c35f9e9d514b597cbd148789547ba152ba67bfc0fec8f

Tags

backdoortrojan

Details

Name	UDPTrcSvc.dll

Size	221184 bytes
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	0893e206274cb98189d51a284c2a8c83
SHA1	d1f4cf4250e7ba186c1d0c6d8876f5a644f457a4
SHA256	cd5ff67ff773cc60c98c35f9e9d514b597cbd148789547ba152ba67bfc0fec8f
SHA512	8042356ff8dc69fa84f2de10a4c34685c3ffa798d5520382d4fbcdcb43ae17e403a208be9891cca6cf2bc297f767229a57f746ca834f6b79(
ssdeep	3072:WsyjTzEvLFOL8AqCiueLt1VFu9+zcSywy0mcj90nSJ5NatCmtWwNQLK:W/zEvLFOLdq9uebdSwHN9n5wtkwNwK
Entropy	6.359677

Antivirus

Ahnlab	Backdoor/Win32.Akdoor
Antiy	Trojan/Win32.AGeneric
Avira	TR/NukeSped.davct
BitDefender	Trojan.GenericKD.30867638
ESET	Win32/NukeSped.AI trojan
Emsisoft	Trojan.GenericKD.30867638 (B)
Ikarus	Trojan.Win32.NukeSped
K7	Trojan (005329311)
NANOAV	Trojan.Win32.NukeSped.fcodob
Systweak	malware.gen-ra
TrendMicro	TROJ_FR.8F37E76D
TrendMicro House Call	TROJ_FR.8F37E76D
VirusBlokAda	Trojan.Tiggre
Zillya!	Trojan.NukeSped.Win32.73

Yara Rules

hidden_cobra_consolidated.yara	rule crypt_constants_2 { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/04/19 "hidden_cobra" family = "n/a" description = "n/a" strings: $ = {efcdab90} $ = {558426fe} $ = {7856b4c2} cor 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }
hidden_cobra_consolidated.yara	rule lsfr_constants { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/04/19" cat "hidden_cobra" family = "n/a" description = "n/a" strings: $ = {efcdab90} $ = {558426fe} $ = {7856b4c2} cor 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }
hidden_cobra_consolidated.yara	rule polarSSL_servernames { meta: Author="NCCIC trusted 3rd party" Incident="10135536" Date = "2018/ "hidden_cobra" family = "n/a" description = "n/a" strings: $polarSSL = "fjiejffndxklfsdkfjsaadiepwn" $sn1 = " $sn2 = "www.naver.com" condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) -- 0x4550) and ($polarS

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2016-08-23 00:23:04-04:00
Import Hash	30d3466536de2b423897a3c8992ef999

PE Sections

MD5	Name	Raw Size	Entropy
d37b95aa17fa132415b37ec777f439ff	header	4096	0.709908
badbc93c35554aec904ab0c34f05fbe0	.text	180224	6.295472

64f7a9cafdad34003aba4547bba0e25b	.rdata	16384	6.372911
c792eb0c57577f4f3649775cbf32b253	.data	12288	3.996008
8791f715ae89ffe2c7d832c1be821edc	.reloc	8192	5.154376

Relationships

cd5ff67ff7... Dropped_By 70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3

Description

This artifact is a malicious 32bit Windows dynamic library. 'UDPTrcSvc.dll' is identified as the 'Network UDP Trace Management Service'. The follo
provided:

---Begin Service Description---

Network UDP Trace Management Service Hosts TourSvc Tracing. If this service is stopped, notifications of network trace will no longer function a
access to service functions. If this service is disabled, notifications of and monitoring to network state will no longer function.

---End Service Description---

The service is invoked with the command, 'C:\Windows\System32\svchost.exe -k mdnetuse'.
When the service is run a modification to the system firewall is attempted, 'cmd.exe /c netsh firewall add portopening TCP 0 "adp"'.

Unlike many of the files listed above that use a public certificate from naver.com, 'UDPTrcSvc.dll' uses a public SSL certificate from google.com.
96a296d224f285c67bee93c30f8a309157f0daa35dc5b87e410b78630a09cfc7

Tags

trojan

Details

Name	MSDFMAPI.INI
Size	2 bytes
Type	data
MD5	c4103f122d27677c9db144cae1394a66
SHA1	1489f923c4dca729178b3e3233458550d8dddf29
SHA256	96a296d224f285c67bee93c30f8a309157f0daa35dc5b87e410b78630a09cfc7
SHA512	5ea71dc6d0b4f57bf39aadd07c208c35f06cd2bac5fde210397f70de11d439c62ec1cdf3183758865fd387fcea0bada2f6c37a4a17851dd
ssdeep	3::
Entropy	0.000000

Antivirus

NetGate Trojan.Win32.Malware

Yara Rules

No matches found.

ssdeep Matches

100 c35020473aed1b4642cd726cad727b63fff2824ad68cedd7ffb73c7cbd890479

Relationships

96a296d224...	Dropped_By	70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3
96a296d224...	Dropped_By	2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525

Description

'MSDFMAPI.INI' is written to C:\WINDOWS and to %UserProfile\AppData\Local\VirtualStore\Windows%. During analysis, two NULL characters w
The purpose of the file has not been determined.

d77fdabe17cdba62a8e728cbe6c740e2c2e541072501f77988674e07a05dfb39

Details

Name	F8D26F2B8DD2AC4889597E1F2FD1F248
Name	d77fdabe17cdba62a8e728cbe6c740e2c2e541072501f77988674e07a05dfb39
Size	456241 bytes
Type	data
MD5	f8d26f2b8dd2ac4889597e1f2fd1f248
SHA1	dd132f76a4aff9862923d6a10e54dca26f26b1b4
SHA256	d77fdabe17cdba62a8e728cbe6c740e2c2e541072501f77988674e07a05dfb39
SHA512	34f8d10ebcab6f10c5140e94cf858761e9fa2e075db971b8e49c7334e1d55237f844ed6cf8ce735e984203f58d6b5032813b55e29a59af4
ssdeep	12288:MG31DF/ubokxmgF8JsVusikiWxdj3tlQLYe:NII0UV0ou1kiWvm4Ye
Entropy	7.999350

Antivirus

No matches found.

Yara Rules

No matches found.

ssdeep Matches

No matches found.

Description

This artifact contains a similar public SSL certificate from naver.com, similar to many of the files above. The payload of the file appears to be encc key. No context was provided with the file's submission.

Relationship Summary

2151c1977b...	Connected_To	81.94.192.147
2151c1977b...	Connected_To	112.175.92.57
2151c1977b...	Related_To	181.39.135.126
2151c1977b...	Related_To	197.211.212.59
2151c1977b...	Related_To	70902623c9cd0cccc8513850072b70732d02c266c7b7e96d2d5b2ed4f5edc289
2151c1977b...	Dropped	96a296d224f285c67bee93c30f8a309157f0daa35dc5b87e410b78630a09cfc7
197.211.212.59	Related_To	2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525
197.211.212.59	Connected_From	ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d
197.211.212.59	Connected_From	70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3
181.39.135.126	Related_To	2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525
181.39.135.126	Connected_From	ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d
181.39.135.126	Connected_From	70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3
112.175.92.57	Connected_From	2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525
112.175.92.57	Connected_From	ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d
112.175.92.57	Connected_From	70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3
112.175.92.57	Connected_From	83228075a604e955d59edc760e4c4ed16eedabfc8f6ac291cf21b4fcbcd1f70a
81.94.192.147	Connected_From	2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525
81.94.192.147	Connected_From	ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d
81.94.192.147	Connected_From	70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3
70902623c9...	Dropped_By	70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3
70902623c9...	Related_To	ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d

70902623c9...	Related_To	2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525
70902623c9...	Related_To	70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3
70902623c9...	Related_To	12480585e08855109c5972e85d99cda7701fe992bc1754f1a0736f1eebcb004d
ddea408e17...	Connected_To	81.94.192.147
ddea408e17...	Connected_To	112.175.92.57
ddea408e17...	Connected_To	181.39.135.126
ddea408e17...	Connected_To	197.211.212.59
ddea408e17...	Related_To	70902623c9cd0cccc8513850072b70732d02c266c7b7e96d2d5b2ed4f5edc289
ddea408e17...	Connected_To	81.94.192.10
81.94.192.10	Connected_From	ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d
12480585e0...	Related_To	70902623c9cd0cccc8513850072b70732d02c266c7b7e96d2d5b2ed4f5edc289
12480585e0...	Dropped	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359
49757cf856...	Dropped_By	12480585e08855109c5972e85d99cda7701fe992bc1754f1a0736f1eebcb004d
49757cf856...	Connected_To	21.252.107.198
49757cf856...	Connected_To	70.224.36.194
49757cf856...	Connected_To	113.114.117.122
49757cf856...	Connected_To	47.206.4.145
49757cf856...	Connected_To	84.49.242.125
49757cf856...	Connected_To	26.165.218.44
49757cf856...	Connected_To	137.139.135.151
49757cf856...	Connected_To	97.90.44.200
49757cf856...	Connected_To	128.200.115.228
49757cf856...	Connected_To	186.169.2.237
21.252.107.198	Connected_From	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
21.252.107.198	Connected_From	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359
70.224.36.194	Connected_From	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
70.224.36.194	Connected_From	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359
113.114.117.122	Connected_From	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
113.114.117.122	Connected_From	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359
47.206.4.145	Connected_From	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
47.206.4.145	Connected_From	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359
84.49.242.125	Connected_From	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
84.49.242.125	Connected_From	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359
26.165.218.44	Connected_From	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
26.165.218.44	Connected_From	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359
137.139.135.151	Connected_From	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
137.139.135.151	Connected_From	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359
97.90.44.200	Connected_From	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
97.90.44.200	Connected_From	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359
128.200.115.228	Connected_From	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761

128.200.115.228	Connected_From	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359
186.169.2.237	Connected_From	4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761
186.169.2.237	Connected_From	49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359
4a74a9fd40...	Connected_To	21.252.107.198
4a74a9fd40...	Connected_To	70.224.36.194
4a74a9fd40...	Connected_To	113.114.117.122
4a74a9fd40...	Connected_To	47.206.4.145
4a74a9fd40...	Connected_To	84.49.242.125
4a74a9fd40...	Connected_To	26.165.218.44
4a74a9fd40...	Connected_To	137.139.135.151
4a74a9fd40...	Connected_To	97.90.44.200
4a74a9fd40...	Connected_To	128.200.115.228
4a74a9fd40...	Connected_To	186.169.2.237
83228075a6...	Connected_To	112.175.92.57
70034b33f5...	Dropped	cd5ff67ff773cc60c98c35f9e9d514b597cbd148789547ba152ba67bfc0fec8f
70034b33f5...	Dropped	70902623c9cd0cccc8513850072b70732d02c266c7b7e96d2d5b2ed4f5edc289
70034b33f5...	Dropped	96a296d224f285c67bee93c30f8a309157f0daa35dc5b87e410b78630a09cfc7
70034b33f5...	Connected_To	81.94.192.147
70034b33f5...	Connected_To	112.175.92.57
70034b33f5...	Connected_To	181.39.135.126
70034b33f5...	Connected_To	197.211.212.59
70034b33f5...	Related_To	70902623c9cd0cccc8513850072b70732d02c266c7b7e96d2d5b2ed4f5edc289
cd5ff67ff7...	Dropped_By	70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3
96a296d224...	Dropped_By	70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3
96a296d224...	Dropped_By	2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525

Recommendations

CISA would like to remind users and administrators to consider using the following best practices to strengthen the security posture of their organ 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 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 Incide 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 most will provide initial indicators for computer and network defense. To request additional analysis, please contact US-CERT and provide information r desired analysis.

What is a MAR? A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manua To request additional analysis, please contact 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 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/US-CERT's homepage at www.us-cert.gov.

Revisions

April 10, 2019: Initial version

Please share your thoughts.

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