MAR-10135536-8.v4 – North Korean Trojan: HOPLIGHT

us-cert.gov/ncas/analysis-reports/ar20-045g

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 distribute 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 Department of Homeland Security (DHS), the Federal Bureau of Inve Department of Defense (DoD). Working with U.S. Government partners, DHS, FBI, and DoD identified Trojan malware variants used by the North malware variant has been identified as HOPLIGHT. The U.S. Government refers to malicious cyber activity by the North Korean government as H information on HIDDEN COBRA activity, visit https[:]//www[.]us-cert.gov/hiddencobra.

DHS, FBI, and DoD are distributing this MAR to enable network defense and reduce exposure to North Korean government malicious cyber activi

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

This report provides analysis of twenty malicious executable files. Sixteen of these files are proxy applications that mask traffic between the malw operators. The proxies have the ability to generate fake TLS handshake sessions using valid public SSL certificates, disguising network connectio actors. One file contains a public SSL certificate and the payload of the file appears to be encoded with a password or key. The remaining file doe public SSL certificates, but attempts outbound connections and drops four files. The dropped files primarily contain IP addresses and SSL certifica For a downloadable copy of IOCs, see MAR-10135536-8.v4.stix.

Submitted Files (20)

05feed9762bc46b47a7dc5c469add9f163c16df4ddaafe81983a628da5714461 (23E27E5482E3F55BF828DAB8855690...)

0608e411348905145a267a9beaf5cd3527f11f95c4afde4c45998f066f418571 (34E56056E5741F33D823859E77235E...)

084b21bc32ee19af98f85aee8204a148032ce7eabef668481b919195dd62b319 (170A55F7C0448F1741E60B01DCEC9C...)

12480585e08855109c5972e85d99cda7701fe992bc1754f1a0736f1eebcb004d (868036E102DF4CE414B0E6700825B3...)

1a01b8a4c505db70f9e199337ce7f497b3dd42f25ad06487e29385580bca3676 (07D2B057D2385A4CDF413E8D342305...)

2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525 (5C3898AC7670DA30CF0B22075F3E8E...)

32ec329301aa4547b4ef4800159940feb950785f1ab68d85a14d363e0ff2bc11 (38FC56965DCCD18F39F8A945F6EBC4...)

4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761 (42682D4A78FE5C2EDA988185A34463...)

4c372df691fc699552f81c3d3937729f1dde2a2393f36c92ccc2bd2a033a0818 (C5DC53A540ABE95E02008A04A0D56D...)

70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3 (61E3571B8D9B2E9CCFADC3DDE10FB6...)

73dcb7639c1f81d3f7c4931d32787bdf07bd98550888c4b29b1058b2d5a7ca33 (3EDCE4D49A2F31B8BA9BAD0B8EF549...)

83228075a604e955d59edc760e4c4ed16eedabfc8f6ac291cf21b4fcbcd1f70a (3021B9EF74c&BDDF59656A035F94FD...)

8a1d57ee05d29a730864299376b830a7e127f089e500e148d96d0868b7c5b520 (5C0C1B4C3B1CFD455AC05ACE994AED...)

b05aae59b3c1d024b19c88448811debef1eada2f51761a5c41e70da3db7615a9 (2FF1688FE866EC2871169197F9D469...)

b9a26a569257fbe02c10d3735587f10ee58e4281dba43474dbdef4ace8ea7101 (2A791769AA73AC757F210F8546125B...)

c66ef8652e15b579b409170658c95d35cfd6231c7ce030b172692f911e7dcff8 (E4ED26D5E2A84CC5E48D285E4EA898...)

d77fdabe17cdba62a8e728cbe6c740e2c2e541072501f77988674e07a05dfb39 (F8D26F2B8DD2AC4889597E1F2FD1F2...)

ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d (BE588CD29B9DC6F8CFC4D0AA5E5C79...)

f8f7720785f7e75bd6407ac2acd63f90ab6c2907d3619162dc41a8ffa40a5d03 (D2DA675A8ADFEF9D0C146154084FFF...)

fe43bc385b30796f5e2d94dfa720903c70e66bc91dfdcfb2f3986a1fea3fe8c5 (F315BE41D9765D69AD60F0B4D29E43...)

Additional Files (7)

44a93ea6e6796530bb3cf99555dfb3b1092ed8fb4336bb198ca15b2a21d32980 (None)

49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359 (rdpproto.dll)

70902623c9cd0cccc8513850072b70732d02c266c7b7e96d2d5b2ed4f5edc289 (udbcgiut.dat)

823d255d3dc8cbc402527072a9220e4c38655de1a3e55a465db28b55d3ac1bf8 (None)

96a296d224f285c67bee93c30f8a309157f0daa35dc5b87e410b78630a09cfc7 (MSDFMAPI.INI)

ba80cb0a08908782f4b6e88aa15e2d306b19bc93e79bd8770bf8be904fd1bd09 (None)

cd5ff67ff773cc60c98c35f9e9d514b597cbd148789547ba152ba67bfc0fec8f (UDPTrcSvc.dll)

IPs (23)

112.175.92.57

113.114.117.122

117.239.241.2

119.18.230.253

128.200.115.228

137.139.135.151

14.140.116.172

181.39.135.126

186.169.2.237

195.158.234.60

197.211.212.59

21.252.107.198

210.137.6.37

217.117.4.110

218.255.24.226

221.138.17.152

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

Ahnlab	Trojan/Win32.Generic
Antiy	Trojan/Win32.Casdet
Avira	TR/NukeSped.uxivj
BitDefender	Trojan.GenericKD.41198265
ClamAV	Win.Trojan.HiddenCobra-7402602-0
Cyren	W32/Trojan.LXQN-3818
ESET	a variant of Win32/NukeSped.AI trojan
Emsisoft	Trojan.GenericKD.41198265 (B)
Ikarus	Trojan.Win32.NukeSped
K7	Trojan (005329311)
McAfee	Trojan-Hoplight
Microsoft Security Essentials	Trojan:Win32/Hoplight
Quick Heal	Trojan.Hoplight.S5793599
Sophos	Troj/Hoplight-C
Symantec	Trojan.Hoplight
TrendMicro	Trojan.55DEE3DA
TrendMicro House Call	Trojan.55DEE3DA
VirusBlokAda	Trojan.Casdet

YARA Rules

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

- rule polarSSL_servernames
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $polarSSL = "fjiejffndxklfsdkfjsaadiepwn"
    $sn1 = "www.google.com"
    $sn2 = "www.naver.com"
  condition:
        (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) -- 0x4550) and ($polarSSL and 1 of ($sn*))
  }

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 32-bit Windows executable. When executed the malware will collect system information about the victim machine inclu
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 family has 2 versions. Both are nearly identical in functionality but use slightly different command codes. So if the opcode for Keepa
0xB6C1, the opcode in version 2 will be 0xB6C2.

There may be some versions of the malware that have limited/additional functionality, but most will have these command codes:

---Begin Version 1 Command Codes---

0xB6A4 GetComputerInfo
  -Gets OS Version
  -Opens and sends back multiple registry keys
    Keys are encrypted in actually binary using RC4 with 16 byte key (af 3d 78 23 4a 79 92 81 9d 7f 20 47 ad e3 f2 b3). Keys are decrypted pri
RegOpenKey/RegQueryValue.

-Calls GetSystemInfo, returns results of a SYSTEM_INFO struct
-Calls GetSystemMetrics and returns results
0xB6AS GetDrivesInfo
-Gets info about different drives/share drives on system as well as memory available/memory used on those drives
0xB6A6 Directorylist
-Gives list of all files in a directory that is specified by the C2
0xB6A7 SendFile
-Sends a file from the victim machine to the C2 that is specified by the C2
0xB6A8 ReceiveFile
-Victim machine receives file from the C2
0xB6A9 CreateProcess
-Calls CreateProcessW to run a process via the command line. C2 specifies the path of the file to be run via command line.
0xB6AA EnableLogging
-Prior to victim and C2 closing out a connection the victim will spawn a new thread that will compile a comprehensive log of system/session info
it opens a file that is named randomly and places it in the temp directory. It puts all the log results into this file.
0xB6AB Deletefile
-Deletes file specified by the C2.
0xB6AC RunCmdPipe
-Runs CreateProcessW to run a process via the command line. The process will be cmd.exe and the arguments will be the windows cmd comm
The results of this command will be sent to a temporary file and then read back to the C2 from that file. Afterwards that file is deleted.
0xB6AD Processlist
-Gets a list of processes
0xB6AE KillProcess
-Kills process based on the PID that the C2 supplies.
0xB6AF TestEncryption
-Tests LFSR encryption, no real functionality
0xB6B0 Uninstall
-Uninstalls the implant from the victim box
0xB6B2 GetConfig
-Gets the current callback config file from memory, returns the list to C2. There are 10 IP options in this config.
0xB6B3 SetConfig
-Gets the current callback config file from memory, allows C2 to change the configurations. This will change the beacon IP to whatever the C2 w
0xB6B4 SetCurrentDirectory
-Changes current working directory to the path supplied by C2
0xB6B5 GetCurrentDirectory
-Gets the current working directory and returns it to the C2
0xB6C1 KeepAlive
-C2s sends this as a keep alive to the victim, victim responds with confirmation that it received the keep alive and keeps session open

---End Version 1 Command Codes---

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.

The malware uses the default certificates/private keys that come with PolarSSL. These are generally used for testing purposes only. Additionally t
server for the TLS handshake require the malware to respond back with a client key. This key is also a default key found within the PolarSSL libra

---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

After the TLS authentication is completed this particular malware does NOT use the session key that is generated via TLS. It uses a custom Linea
(LFSR) encryption scheme to encrypt all communications after the completion of the handshake. A python script to decrypt traffic is given below:

---Begin LFSR Decryption Script---

```
class lfsr:
  def _init_(self):
     self.b = (0, 0, 0, 0)
     self.data = b''
     self.L= 0

  def lfsr_init(self, data):
     self.L = len(data)
     self.data = data
     self.b[0] = 0
     self.b[1] = 0xc2b45678
     self.b[2] = 0x90abcdef
     self.b[3] = 0xfe268455
```

```
    for i in range(int(self.L / 3)):
        self.b[1] ^= self.b[2]
        self.b[2] ^= self.b[3]
        self.b[3] ^= self.b[1]

    for i in range{self.L % 3):
        self.b[1] |= self.b[2]
        self.b[2] |= self.b[3]
        self.b[3] |= self.b[1]

     def lfsr_1(self):
        r = 0
        if (self.b[1] & 0x200) == 0x200:
            r += 1
        if (self.b[2] & 0x800) == 0x800:
            r += 1
        if (self.b[3] & 0x800) == 0x800:
            r += 1
        if r <= 1:
            self.b[0] = 1
        else:
            self.b[0] = 0

    def lfsr_2(self):
        v1 = self.b[1]
        r = (self.b[1] >> 9) & 1
        v3 = r == self.b[0]
        self.b[0] ^= r
        if not v3:
            r = (v1 ^ ((v1 ^ (( v1 ^ (v1 >> 1)) >> 1)) >> 3)) >> 13
            v4 = 2 * (v1 & 0x3ffff)
            self.b[1] = v4
            if (r & 1):
                self.b[1] = v4 ^ 1

    def lfsr_3(self):
        v1 = self.b[2]
        r = (self.b[2] >> 11) & 1
        v3 = r == self.b[0]
        self.b[0] ^= r
        if not v3:
            r = (v1 ^ ((v1 ^ ((v1 ^ (v1 >> 1)) >> 4)) >> 4)) >> 12
            v4 = 2 * (v1 & 0x1fffff)
            self.b[2] = v4
            if (r & 1):
                self.b[2] = v4 ^ 1

    def lfsr 4(self):
        v1 = self.b[3]
        r = (self.b[3] >> 11) & 1
        v3 = r == self.b[0]
        self.b[0] ^= r
        if not v3:
            r = (v1 ^ ((v1 ^ ((v1 ^ (v1 >> 1)) >> 3)) >> 1)) >> 17
            v4 = 2 * (v1 & 0x3fffff)
            self.b[3] = v4
            if (r & 1):
                self.b[3] = v4 ^ 1

    def lfsr_genKeyByte(self):
        self.lfsr_1()
        self.lfsr_2()
        self.lfsr_3()
        self.lfsr_4()
        v2 = self.b[1] ^ self.b[2] ^ self.b[3]
        r = (v2 >> 0x18) ^ (v2 >> 0x10) ^ (v2 >> 0x8) ^ v2
        r &= 0xff
        return r

    def crypt(self):
        r= b''
        for i in range(len(self.data)):
            k = self.lfsr_genKeyByte()
            r += bytes([self.data[i] ^ k])
        return r
```

---End LFSR Decryption Script---

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

Ahnlab	Trojan/Win32.Generic
Antiy	Trojan/Win32.NukeSped
Avira	TR/NukeSped.bqdkh
BitDefender	Trojan.GenericKD.41198269
ClamAV	Win.Trojan.HiddenCobra-7402602-0
Cyren	W32/Trojan.MYIL-1461
ESET	a variant of Win32/NukeSped.AI trojan
Emsisoft	Trojan.GenericKD.41198269 (B)
Ikarus	Trojan.Win32.NukeSped
K7	Trojan (005329311)
McAfee	Trojan-Hoplight
Microsoft Security Essentials	Trojan:Win32/Hoplight
Quick Heal	Trojan.Hoplight.S5774771
Sophos	Troj/Hoplight-C
Symantec	Trojan.Hoplight
TACHYON	Trojan/W32.Hoplight.221184
TrendMicro	Trojan.55DEE3DA
TrendMicro House Call	Trojan.55DEE3DA
VirusBlokAda	BScope.Trojan.Casdet

YARA Rules

- rule crypt_constants_2
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $ = {efcdab90}
    $ = {558426fe}
    $ = {7856b4c2}
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them
  }
- rule lsfr_constants
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $ = {efcdab90}
    $ = {558426fe}
    $ = {7856b4c2}
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them
  }
- rule polarSSL_servernames
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $polarSSL = "fjiejffndxklfsdkfjsaadiepwn"
    $sn1 = "www.google.com"
    $sn2 = "www.naver.com"
  condition:
        (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) -- 0x4550) and ($polarSSL and 1 of ($sn*))
  }

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
IP addresses were attempted during analysis.
197.211.212.59

Tags

command-and-control

Ports

443 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
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

Tags

command-and-control

Ports

443 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
associated with the IP address.

112.175.92.57

Tags

command-and-control

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
mail.everzone.co.kr is associated with the IP address, however, no DNS query is made for the name.

81.94.192.147

Tags

command-and-control

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 associated with the IP address.

70902623c9cd0cccc8513850072b70732d02c266c7b7e96d2d5b2ed4f5edc289

Tags

droppertrojan

Details

Name	udbcgiut.dat
Size	1171 bytes
Type	data
MD5	ae829f55db0198a0a36b227addcdeeff
SHA1	04833210fa57ea70a209520f4f2a99d049e537f2
SHA256	70902623c9cd0cccc8513850072b70732d02c266c7b7e96d2d5b2ed4f5edc289
SHA512	1b4509102ac734ce310b6f8631b1bedd772a38582b4feda9fee09f1edd096006cf5ba528435c844effa97f95984b07bd2c111aa480bb22f
ssdeep	3:ElclFUl8GlFcmzkXIil23X1ll:ElcUXmQkXQ3
Entropy	0.395693

Antivirus

Ahnlab	BinImage/Hoplight
Antiy	Trojan/Generic.Generic
ClamAV	Win.Dropper.Hoplight-7402658-0
Ikarus	Trojan.Win32.Hoplight
McAfee	Trojan-Hoplight.b
Microsoft Security Essentials	Trojan:Win32/Hoplight
TrendMicro	Trojan.22D9D34C
TrendMicro House Call	Trojan.22D9D34C

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 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

Ahnlab	Trojan/Win32.Hoplight
Antiy	Trojan/Win32.Casdet
Avira	TR/NukeSped.qdbcu
BitDefender	Trojan.GenericKD.31879714
ClamAV	Win.Trojan.HiddenCobra-7402602-0
Cyren	W32/Trojan.OTMD-4999
ESET	a variant of Win32/NukeSped.AS trojan
Emsisoft	Trojan.GenericKD.31879714 (B)
Ikarus	Trojan.Win32.NukeSped
K7	Trojan (0051d4f01)
McAfee	Trojan-Hoplight
Microsoft Security Essentials	Trojan:Win32/Hoplight
Quick Heal	Trojan.Hoplight.S5793599
Sophos	Troj/Hoplight-C
Symantec	Trojan.Hoplight

TrendMicro	Trojan.55DEE3DA
TrendMicro House Call	Trojan.55DEE3DA
VirusBlokAda	Trojan.Casdet

YARA Rules

- rule crypt_constants_2
  {
  meta:
  Author="NCCIC trusted 3rd party"
  Incident="10135536"
  Date = "2018/04/19"
  category = "hidden_cobra"
  family = "n/a"
  description = "n/a"
  strings:
  $ = {efcdab90}
  $ = {558426fe}
  $ = {7856b4c2}
  condition:
  (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them
  }
- rule lsfr_constants
  {
  meta:
  Author="NCCIC trusted 3rd party"
  Incident="10135536"
  Date = "2018/04/19"
  category = "hidden_cobra"
  family = "n/a"
  description = "n/a"
  strings:
  $ = {efcdab90}
  $ = {558426fe}
  $ = {7856b4c2}
  condition:
  (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them
  }
- rule polarSSL_servernames
  {
  meta:
  Author="NCCIC trusted 3rd party"
  Incident="10135536"
  Date = "2018/04/19"
  category = "hidden_cobra"
  family = "n/a"
  description = "n/a"
  strings:
  $polarSSL = "fjiejffndxklfsdkfjsaadiepwn"
  $sn1 = "www.google.com"
  $sn2 = "www.naver.com"
  condition:
  (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) -- 0x4550) and ($polarSSL and 1 of ($sn*))
  }

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

Ahnlab	Trojan/Win32.Generic
Antiy	Trojan/Win32.Casdet
Avira	TR/NukeSped.yvkuj
BitDefender	Trojan.GenericKD.31879713
ClamAV	Win.Trojan.HiddenCobra-7402602-0
Cyren	W32/Trojan.TBKF-4720
ESET	a variant of Win32/NukeSped.AI trojan
Emsisoft	Trojan.GenericKD.31879713 (B)
Filseclab	Adware.Amonetize.heur.xjym.mg
Ikarus	Trojan.Win32.NukeSped
K7	Trojan (005329311)
McAfee	Trojan-Hoplight
Microsoft Security Essentials	Trojan:Win32/Nukesped.PA!MTB
Sophos	Troj/Hoplight-C
Symantec	Trojan.Hoplight

TACHYON	Trojan/W32.Hoplight.267776
TrendMicro	Trojan.55DEE3DA
TrendMicro House Call	Trojan.55DEE3DA
VirusBlokAda	BScope.Trojan.Casdet

YARA Rules

- rule crypt_constants_2
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $ = {efcdab90}
    $ = {558426fe}
    $ = {7856b4c2}
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them
  }
- rule lsfr_constants
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $ = {efcdab90}
    $ = {558426fe}
    $ = {7856b4c2}
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them
  }
- rule polarSSL_servernames
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $polarSSL = "fjiejffndxklfsdkfjsaadiepwn"
    $sn1 = "www.google.com"
    $sn2 = "www.naver.com"
  condition:
        (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) -- 0x4550) and ($polarSSL and 1 of ($sn*))
  }

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 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

Tags

command-and-control

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

droppertrojan

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

Ahnlab	Trojan/Win64.Hoplight
Antiy	Trojan/Generic.Generic
Avira	TR/Dropper.ezydy
BitDefender	Trojan.Autoruns.GenericKDS.32698229
ClamAV	Win.Trojan.Hoplight-7402636-0
Cyren	W64/Trojan.PLQG-3049
ESET	a variant of Win64/NukeSped.BV trojan
Emsisoft	Trojan.Autoruns.GenericKDS.32698229 (B)
Ikarus	Trojan.Win64.Nukesped
K7	Riskware (0040eff71)
McAfee	Generic Trojan.ix
Microsoft Security Essentials	Trojan:Win64/Hoplight
NANOAV	Trojan.Win64.Crypted.excqpl
NetGate	Trojan.Win32.Malware
Quick Heal	Trojan.Win64
Sophos	Troj/Hoplight-C
Symantec	Trojan.Gen.MBT

TACHYON	Trojan/W32.Hoplight.453791
TrendMicro	Trojan.D58D9624
TrendMicro House Call	Trojan.D58D9624
VirusBlokAda	Trojan.Win64.Hoplight

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

Ahnlab	Trojan/Win64.Hoplight
Antiy	Trojan/Win32.Casdet
Avira	TR/Crypt.XPACK.xuqld
BitDefender	Trojan.Generic.22790108
ClamAV	Win.Trojan.Hoplight-7402636-0
ESET	a variant of Win64/NukeSped.BV trojan
Emsisoft	Trojan.Generic.22790108 (B)
Ikarus	Trojan.SuspectCRC
K7	Trojan (0054bb211)
McAfee	Hoplight-FDXG!DC268B166FE4
Microsoft Security Essentials	Trojan:Win64/Hoplight
NANOAV	Trojan.Win64.Crypted.excqpl
Quick Heal	Trojan.Win64
Sophos	Troj/Hoplight-C
Symantec	Trojan.Hoplight
TACHYON	Trojan/W32.Hoplight.391680
VirusBlokAda	Trojan.Win64.Agent

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

Tags

command-and-control

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

Tags

command-and-control

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

Tags

command-and-control

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

Tags

command-and-control

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

Tags

command-and-control

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

Tags

command-and-control

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

Tags

command-and-control

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

Tags

command-and-control

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

Tags

command-and-control

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

Tags

command-and-control

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

Ahnlab	Trojan/Win32.Generic
Antiy	Trojan/Win32.AGeneric
Avira	TR/NukeSped.tbxxd
BitDefender	Trojan.GenericKD.41198710
ClamAV	Win.Trojan.HiddenCobra-7402602-0
Cyren	W64/Trojan.NKDY-0871
ESET	a variant of Win64/NukeSped.T trojan
Emsisoft	Trojan.GenericKD.41198710 (B)
Ikarus	Trojan.Win64.Nukesped
K7	Trojan (0054bc321)
McAfee	Generic Trojan.ix
Microsoft Security Essentials	Trojan:Win64/Hoplight
Quick Heal	Trojan.Hoplight.S5795935
Sophos	Troj/Hoplight-C
Symantec	Trojan.Hoplight
TACHYON	Trojan/W32.Hoplight.346624
TrendMicro	Trojan.A7CCF529
TrendMicro House Call	Trojan.A7CCF529
VirusBlokAda	Trojan.Win64.Hoplight
Zillya!	Trojan.NukeSped.Win64.56

YARA Rules

- rule crypt_constants_2
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $ = {efcdab90}
    $ = {558426fe}
    $ = {7856b4c2}
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them
  }
- rule lsfr_constants
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $ = {efcdab90}
    $ = {558426fe}
    $ = {7856b4c2}
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them
  }
- rule polarSSL_servernames
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $polarSSL = "fjiejffndxklfsdkfjsaadiepwn"
    $sn1 = "www.google.com"
    $sn2 = "www.naver.com"
  condition:
        (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) -- 0x4550) and ($polarSSL and 1 of ($sn*))
  }

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
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

Tags

trojan

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

Ahnlab	Trojan/Win64.Hoplight
Antiy	Trojan/Win32.Hoplight
Avira	TR/AD.APTLazerus.ltfzr
BitDefender	Trojan.Agent.DVDE
ClamAV	Win.Trojan.HiddenCobra-7402602-0
Cyren	W64/Trojan.KDWH-2913
ESET	a variant of Win64/NukeSped.BW trojan
Emsisoft	Trojan.Agent.DVDE (B)
Ikarus	Trojan.Agent
K7	Riskware (0040eff71)
McAfee	Generic Trojan.jp
Microsoft Security Essentials	Trojan:Win64/Hoplight
Sophos	Troj/Hoplight-C
Symantec	Trojan.Hoplight
TrendMicro	Trojan.A7CCF529
TrendMicro House Call	Trojan.A7CCF529
VirusBlokAda	Trojan.Win64.Hoplight

YARA Rules

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

- rule lsfr_constants
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $ = {efcdab90}
    $ = {558426fe}
    $ = {7856b4c2}
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them
  }
- rule polarSSL_servernames
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $polarSSL = "fjiejffndxklfsdkfjsaadiepwn"
    $sn1 = "www.google.com"
    $sn2 = "www.naver.com"
  condition:
        (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) -- 0x4550) and ($polarSSL and 1 of ($sn*))
  }

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 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 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 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 VMWare Tools no longer works. It cannot be determined if this is an intentional characteristic of the malware to hinder analysis, or simply a sympt 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

Ahnlab	Trojan/Win32.Hoplight
Antiy	Trojan/Win32.NukeSped
Avira	TR/NukeSped.oppme
BitDefender	Dropped:Trojan.Generic.22954895
Cyren	W32/Trojan.GZYA-1356
ESET	Win32/NukeSped.AI trojan
Emsisoft	Dropped:Trojan.Generic.22954895 (B)
Ikarus	Trojan.Win32.NukeSped
K7	Trojan (005329311)
McAfee	Trojan-Hoplight
Microsoft Security Essentials	Trojan:Win32/Hoplight
NANOAV	Trojan.Win32.NukeSped.fpblwf
NetGate	Trojan.Win32.Malware
Sophos	Troj/Hoplight-C
Symantec	Trojan.Gen.MBT
TACHYON	Trojan/W32.Hoplight.258052
TrendMicro	Trojan.55DEE3DA
TrendMicro House Call	Trojan.55DEE3DA

YARA Rules

- rule crypt_constants_2
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $ = {efcdab90}
    $ = {558426fe}
    $ = {7856b4c2}
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them
  }
- rule lsfr_constants
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $ = {efcdab90}
    $ = {558426fe}
    $ = {7856b4c2}
  condition:
    (uint16(0) == 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.Generic.22954895
ClamAV	Win.Trojan.HiddenCobra-7402602-0
ESET	Win32/NukeSped.AI trojan
Emsisoft	Trojan.Generic.22954895 (B)
Ikarus	Trojan.Win32.NukeSped
K7	Trojan (005329311)
McAfee	Trojan-Hoplight
Microsoft Security Essentials	Trojan:Win32/Hoplight
NANOAV	Trojan.Win32.NukeSped.fcodob
Sophos	Troj/Hoplight-C

Symantec	Trojan.Gen.MBT
Systweak	malware.gen-ra
TACHYON	Trojan/W32.Hoplight.221184.B
TrendMicro	Trojan.CCD7B260
TrendMicro House Call	Trojan.CCD7B260
VirusBlokAda	Trojan.Tiggre
Zillya!	Trojan.NukeSped.Win32.73

YARA Rules

- rule crypt_constants_2
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $ = {efcdab90}
    $ = {558426fe}
    $ = {7856b4c2}
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them
  }
- rule lsfr_constants
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $ = {efcdab90}
    $ = {558426fe}
    $ = {7856b4c2}
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them
  }
- rule polarSSL_servernames
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $polarSSL = "fjiejffndxklfsdkfjsaadiepwn"
    $sn1 = "www.google.com"
    $sn2 = "www.naver.com"
  condition:
        (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) -- 0x4550) and ($polarSSL and 1 of ($sn*))
  }

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 foll
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

Details

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

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

100	028f5531e8593ce6faf30dd5c5131abf1400fc4deb4d322f3f39578f14348be1
100	132fde08d7f788dece120e98bf6c794bafb655959764798ead053b872d097638
100	200608c94d52d33ff86b8f4db28451752eeae7c70062488f380f112e11b4350a
100	2d07a41ae992770085117e9815300bfd0730745883e60b24aaad5e69dfc087ae
100	3d1066ae1cd00d635b2131664a7d0d5483554901ed6aae9d627b697ecb02718e
100	5309e677c79cffae49a65728c61b436d3cdc2a2bab4c81bf0038415f74a56880
100	854871db188e45e5a948fb03d293459aef6def1c9a63acb8cfdaaf7155d5699e
100	ad7facb2586fc6e966c004d7d1d16b024f5805ff7cb47c7a85dabd8b48892ca7
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
purpose of the file has not been determined. This file containing two NULL bytes is benign.

d77fdabe17cdba62a8e728cbe6c740e2c2e541072501f77988674e07a05dfb39

Tags

droppertrojan

Details

Name	F8D26F2B8DD2AC4889597E1F2FD1F248
Name	d77fdabe17cdba62a8e728cbe6c740e2c2e541072501f77988674e07a05dfb39
Size	456241 bytes
Type	data
MD5	f8d26f2b8dd2ac4889597e1f2fd1f248
SHA1	dd132f76a4aff9862923d6a10e54dca26f26b1b4
SHA256	d77fdabe17cdba62a8e728cbe6c740e2c2e541072501f77988674e07a05dfb39
SHA512	34f8d10ebcab6f10c5140e94cf858761e9fa2e075db971b8e49c7334e1d55237f844ed6cf8ce735e984203f58d6b5032813b55e29a59af
ssdeep	12288:MG31DF/ubokxmgF8JsVusikiWxdj3tlQLYe:NII0UV0ou1kiWvm4Ye
Entropy	7.999350

Antivirus

Ahnlab	BinImage/Agent
Antiy	Trojan/Win32.Casdet
Avira	TR/Agent.anrq
BitDefender	Trojan.Agent.DVDS
ClamAV	Win.Dropper.Hoplight-7402659-0
Cyren	Trojan.GTWY-8
Emsisoft	Trojan.Agent.DVDS (B)
Ikarus	Trojan.Agent
McAfee	Trojan-Hoplight.b

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.

b9a26a569257fbe02c10d3735587f10ee58e4281dba43474dbdef4ace8ea7101

Tags

trojan

Details

Name	2A791769AA73AC757F210F8546125B57
Size	110592 bytes

Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	2a791769aa73ac757f210f8546125b57
SHA1	269f1cc44f6b323118612bde998d17e5bfbf555e
SHA256	b9a26a569257fbe02c10d3735587f10ee58e4281dba43474dbdef4ace8ea7101
SHA512	1e88edf97f62282323928a304762864d69e0e5a1b98c7824cf7ee8af92a5a7d17586e30165c6b6ec4b64ea64dd97d6f2b3a3ef880debc
ssdeep	1536:BdQGY/Ni+mo06N1homALeoYbrAUD7Qum5T9Xlxgj5MX7jbthYWL3:DQGYFFzxAgoYbrAOQum5TsgjbHP
Entropy	6.406443

Antivirus

Ahnlab	Trojan/Win32.Akdoor
Antiy	Trojan/Win32.Autophyte
Avira	TR/AD.APTLazerus.zobau
BitDefender	Gen:Variant.Graftor.487501
ClamAV	Win.Trojan.HiddenCobra-7402602-0
Cyren	W32/Trojan.BCDT-8700
ESET	a variant of Win32/NukeSped.AU trojan
Emsisoft	Gen:Variant.Graftor.487501 (B)
Huorong	Trojan/NukeSped.a
Ikarus	Trojan.Win32.NukeSped
K7	Trojan (0052cf421)
McAfee	Trojan-HidCobra
Microsoft Security Essentials	Trojan:Win32/Autophyte.E!dha
NANOAV	Trojan.Win32.NukeSped.fyoobu
Quick Heal	Trojan.Generic
Sophos	Troj/NukeSpe-G
Symantec	Trojan Horse
TrendMicro	BKDR_HO.9D36C86C
TrendMicro House Call	BKDR_HO.9D36C86C
VirusBlokAda	BScope.Trojan.Autophyte
Zillya!	Trojan.NukeSped.Win32.158

YARA Rules

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

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

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-08-11 01:03:45-04:00
Import Hash	e56949fef3294200cb30be8009694a42

PE Sections

MD5	Name	Raw Size	Entropy
3d755df7f28ddb5a661a68637cfdf23e	header	4096	0.647583
8f28409d19efb02746f0cc7f186ac3e3	.text	86016	6.553916
03ec21be9a3702ad9b6a107a387c2be1	.rdata	16384	5.844150
cecd220a4af1182a425b07c4547fd1e6	.data	4096	2.638490

Packers/Compilers/Cryptors

Microsoft Visual C++ v6.0

Relationships

b9a26a5692...	Connected_To	117.239.241.2
b9a26a5692...	Connected_To	195.158.234.60
b9a26a5692...	Connected_To	218.255.24.226

Description

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

When the malware runs it checks a config file to determine where it should beacon back to. If the config file has not been modified the malware w following hard coded IPs:

--Begin IP List--

117.239.241.2
218.255.24.226
195.158.234.60

--End IP List--

Client uses uk.yahoo.com for client hello server name instead of naver.com.

117.239.241.2

Tags

command-and-control

Relationships

117.239.241.2	Connected_From	ba80cb0a08908782f4b6e88aa15e2d306b19bc93e79bd8770bf8be904fd1bd09
117.239.241.2	Connected_From	b9a26a569257fbe02c10d3735587f10ee58e4281dba43474dbdef4ace8ea7101

218.255.24.226

Tags

command-and-control

Relationships

218.255.24.226 Connected_From b9a26a569257fbe02c10d3735587f10ee58e4281dba43474dbdef4ace8ea7101

195.158.234.60

Tags

command-and-control

Relationships

195.158.234.60 Connected_From b9a26a569257fbe02c10d3735587f10ee58e4281dba43474dbdef4ace8ea7101

1a01b8a4c505db70f9e199337ce7f497b3dd42f25ad06487e29385580bca3676

Tags

trojan

Details

Name	07D2B057D2385A4CDF413E8D342305DF
Size	2608223 bytes
Type	PE32+ executable (GUI) x86-64, for MS Windows
MD5	07d2b057d2385a4cdf413e8d342305df
SHA1	1991e7797b2e97179b7604497f7f6c39eba2229b
SHA256	1a01b8a4c505db70f9e199337ce7f497b3dd42f25ad06487e29385580bca3676
SHA512	fa2535b08c43c0dae210c12c4a5445925723d50f8828e0d0b89ec70d08aaa2f1d222eea9fd4be40c46c9024b3ed9bfe33e16724496c1c
ssdeep	49152:2sn+T/ymkSsvc1vb+oNEOaPmztSWNz25hqhbR5C7kcaFZweRrjxQTgZdy:2sck5ojp+Ef25al5CyjwSJQMzy
Entropy	7.981828

Antivirus

Ahnlab	Trojan/Win32.Akdoor
Antiy	Trojan/Win64.NukeSped
Avira	TR/NukeSped.cgnux
BitDefender	Trojan.GenericKD.41793016
Cyren	W64/Trojan.DUQO-0431
ESET	a variant of Win64/NukeSped.AH trojan
Emsisoft	Trojan.GenericKD.41793016 (B)
Ikarus	Trojan.Win64.Nukesped
K7	Trojan (00545d8d1)
McAfee	Trojan-HidCobra.a
Microsoft Security Essentials	Trojan:Win32/Casdet!rfn
NANOAV	Trojan.Win64.NukeSped.gayjsq
Sophos	Troj/NukeSpe-H
Symantec	Trojan.Hoplight
TACHYON	Trojan/W64.Agent.2608223
TrendMicro	TSPY_KI.58F058EF
TrendMicro House Call	TSPY_KI.58F058EF

VirusBlokAda	Trojan.Agent
Zillya!	Trojan.Agent.Win32.1135323

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2018-02-12 15:06:28-05:00
Import Hash	347c977c6137a340c7cc0fcd5b224aef

PE Sections

MD5	Name	Raw Size	Entropy
28fc69ad12a0765af4cc06fbd261cb24	header	1024	2.672166
88425c71e7e293d43db9868e4693b365	.text	89088	6.415516
bb0048e4f3851ea07b365828ddf613f7	.rdata	26624	4.912250
50e3efe1a6ea325c87f8e86e2fbd40b4	.data	5632	2.093641
f56a65eb9562d6c6d607f867d1d0fd09	.pdata	4608	4.725531
6a9a84d523e53e1d43c31b2cc069930c	.rsrc	1536	4.308150
dab5e290c15de9634d93d8f592a44633	.reloc	1536	2.912599

Packers/Compilers/Cryptors

Microsoft Visual C++ 8.0 (DLL)

Description

This artifact is a malicious 64bit Windows dynamic library. When run the malware drops a Themida packed DLL. This DLL runs and drops another Remote admin tool. This RAT is very similar to version 2 in op codes and functionality however it uses real TLS instead of the LFSR encryption. A data with XOR Ox47 SUB Ox28 prior to being TLS encrypted.

73dcb7639c1f81d3f7c4931d32787bdf07bd98550888c4b29b1058b2d5a7ca33

Tags

trojan

Details

Name	3EDCE4D49A2F31B8BA9BAD0B8EF54963
Size	147456 bytes
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	3edce4d49a2f31b8ba9bad0b8ef54963
SHA1	1209582451283c46f29a5185f451aa3c989723c9
SHA256	73dcb7639c1f81d3f7c4931d32787bdf07bd98550888c4b29b1058b2d5a7ca33
SHA512	0d3de1758b44597ccc4dad46a9b42626237da425a41b8833bf7549a3c809bd7432ce938cd8757b362e2268bead45a0b212c96cc8817
ssdeep	3072:bQGYFFzsaXlvJdbx9NAzDZWaNoh05WKRYW7IWwh7:bSFhLlh9N8DZWaNoG5W8VIWC
Entropy	6.605430

Antivirus

Ahnlab	Trojan/Win32.Akdoor
Antiy	Trojan/Win32.Autophyte
Avira	TR/AD.APTLazerus.jtxjg

BitDefender	Gen:Variant.Zusy.290462
ClamAV	Win.Trojan.HiddenCobra-7402602-0
Cyren	W32/Trojan.DXJJ-0934
ESET	a variant of Win32/NukeSped.AU trojan
Emsisoft	Gen:Variant.Zusy.290462 (B)
Ikarus	Trojan.Win32.NukeSped
K7	Trojan (0052cf421)
McAfee	Trojan-HidCobra
Microsoft Security Essentials	Trojan:Win32/Autophyte.E!dha
NetGate	Trojan.Win32.Malware
Sophos	Troj/NukeSpe-I
Symantec	Trojan.Hoplight
TrendMicro	BKDR_HO.9D36C86C
TrendMicro House Call	BKDR_HO.9D36C86C
VirusBlokAda	Trojan.Autophyte
Zillya!	Trojan.NukeSped.Win32.154

YARA Rules

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

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-07-11 14:26:59-04:00
Import Hash	cf3e2269004b18054d77ec54601edfd1

PE Sections

MD5	Name	Raw Size	Entropy
f31fc1b632aa011a29b506385890b3bb	header	4096	0.703326
0b401c68fa1a8f024f25189b31fd8caf	.text	118784	6.634510
78ad5231f5184af8093a2f31ef1f9952	.rdata	16384	6.126224
8c48fdefd1785500380702796882a0b6	.data	4096	3.860135
e6b0be8044e573ca9fc84de173a7ca3d	.reloc	4096	5.404736

Packers/Compilers/Cryptors

Microsoft Visual C++ 6.0 DLL

Description

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

This file is dropped by a different binary into System32 and then run as a service. When the malware runs it checks a config file to determine whe to. If the config file has not been modified the malware will beacon back to the following hard coded IPs:

--Begin IP List--

192.168.1.2

--End IP List--

Client uses uk.yahoo.com for client hello server name instead of naver.com.
084b21bc32ee19af98f85aee8204a148032ce7eabef668481b919195dd62b319

Tags

trojan

Details

Name	170A55F7C0448F1741E60B01DCEC9CFB
Size	197632 bytes
Type	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
MD5	170a55f7c0448f1741e60b01dcec9cfb
SHA1	b6b84783816cca123adbc18e78d3b847f04f1d32
SHA256	084b21bc32ee19af98f85aee8204a148032ce7eabef668481b919195dd62b319
SHA512	a014cf5772ed993951dc62026e3acef174c424e47fd56583a1563c692ac3ed2ae5e1d51d34974ed04db11824dc9c76290297244e28e5
ssdeep	6144:XT1NVhDJSUaZcdHItR3SG88+Tlm5T7BRWj:xx9tuVSe+Tlm5Tt
Entropy	6.262340

Antivirus

Ahnlab	Trojan/Win32.Akdoor
Antiy	Trojan/Win32.Agent
Avira	TR/AD.APTLazerus.dsenk
BitDefender	Trojan.GenericKD.32643407
ClamAV	Win.Trojan.HiddenCobra-7402602-0
Cyren	W64/Trojan3.AOLF
ESET	a variant of Win32/NukeSped.AU trojan
Emsisoft	Trojan.GenericKD.32643407 (B)
Ikarus	Trojan.Win32.NukeSped
K7	Trojan (005233111)
McAfee	Trojan-HidCobra

Microsoft Security Essentials	Trojan:Win32/Casdet!rfn
NANOAV	Trojan.Win64.NukeSped.fzpbxb
Quick Heal	Trojan.Multi
Sophos	Troj/NukeSpe-G
Symantec	Trojan.Hoplight
TrendMicro	TROJ64_.655BEC93
TrendMicro House Call	TROJ64_.655BEC93
VirusBlokAda	Trojan.Agent
Zillya!	Trojan.Agent.Win32.1134660

YARA Rules

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

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-05-03 22:40:47-04:00
Import Hash	0675d7e21ce264449360c0b797c279e7

PE Sections

MD5	Name	Raw Size	Entropy
48a2d611f70a4718084857fa2f732b21	header	1024	2.780205
aaf67ea89d12bea95c148274c71ebac5	.text	44544	6.440744
91171a72af025ca7098ba6c94ecbb2a0	.rdata	25600	3.935800
fc2a61b6f1b29162f93fad1660c4b8af	.data	120320	6.379891
114b795f9c567e0a81a04cec6ae1a0b4	.pdata	2560	4.287495
17c80d03f2f5729407ec55eca7e1f5b2	.rsrc	2048	2.948558

c9243c94e36bc012d7d5eb0a3f588dfb	.reloc	1536	5.079827

Description

This artifact is a malicious 64bit Windows dynamic library. The DLL can be run using the DoStart export. This export calls write file to load the actu "C:\windows\msncone.exe" and then calls Win Exec to execute the implant.

c66ef8652e15b579b409170658c95d35cfd6231c7ce030b172692f911e7dcff8

Tags

trojan

Details

Name	E4ED26D5E2A84CC5E48D285E4EA898C0
Size	157696 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	e4ed26d5e2a84cc5e48d285e4ea898c0
SHA1	c3d28d8e49a24a0c7082053d22597be9b58302b1
SHA256	c66ef8652e15b579b409170658c95d35cfd6231c7ce030b172692f911e7dcff8
SHA512	0c0b8fa4e83036b9dbe88b193e93b412c47eee8c6f4b04f04082288d7dce0f0d687e7581e624145bd357e5ad70584b9ab4d9f5a950afe
ssdeep	3072:MzviXzovLFOLUAqWilvLc1V2n9+zEty7+LEfq0Mg3ewPWTc:Mzv+zovLFOLFqhlvlQz7ZqueweT
Entropy	6.446363

Antivirus

Ahnlab	Trojan/Win32.Crypt
Antiy	Trojan/Win32.NukeSped
Avira	TR/AD.APTLazerus.tmifd
BitDefender	Trojan.GenericKD.32416111
ClamAV	Win.Trojan.HiddenCobra-7402602-0
Cyren	W32/Trojan.GVKT-3327
ESET	a variant of Win32/NukeSped.AU trojan
Emsisoft	Trojan.GenericKD.32416111 (B)
Ikarus	Trojan.Win32.NukeSped
K7	Trojan (0052cf421)
McAfee	Trojan-HidCobra
Microsoft Security Essentials	Trojan:Win32/Nukesped.PA!MTB
NANOAV	Trojan.Win32.NukeSped.fzlqhl
NetGate	Trojan.Win32.Malware
Quick Heal	Trojan.Generic
Sophos	Troj/NukeSpe-E
Symantec	Trojan.Gen.MBT
TrendMicro	TROJ_FR.D1E707E2
TrendMicro House Call	TROJ_FR.D1E707E2
Vir.IT eXplorer	Trojan.Win32.Genus.BRN
VirusBlokAda	BScope.Trojan.Casdet
Zillya!	Trojan.NukeSped.Win32.153

YARA Rules

- rule crypt_constants_2
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $ = {efcdab90}
    $ = {558426fe}
    $ = {7856b4c2}
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them
  }
- rule lsfr_constants
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $ = {efcdab90}
    $ = {558426fe}
    $ = {7856b4c2}
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them
  }
- rule polarSSL_servernames
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $polarSSL = "fjiejffndxklfsdkfjsaadiepwn"
    $sn1 = "www.google.com"
    $sn2 = "www.naver.com"
  condition:
        (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) -- 0x4550) and ($polarSSL and 1 of ($sn*))
  }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-10-23 16:44:37-04:00
Import Hash	861401f76d1251e0d08a8ade1a5ed38c

PE Sections

MD5	Name	Raw Size	Entropy
0aa18a6525a2203ee52f6df5f9622dcb	header	1024	2.637312
33e3584e4c52c24e16fc108224a3f6a3	.text	132608	6.153434
8a43450710359fae49269f1217924cf5	.rdata	16896	6.299497
b0c95d35585e130bea58057c11e9d53b	.data	3584	5.455587
3a4fdc31bb49b29d6f19b94641d14ee8	.rsrc	512	5.112624
f74e21bd34aa3a05131ae77f0b48c2b2	.reloc	3072	5.875833

Packers/Compilers/Cryptors

Microsoft Visual C++ ?.?

Description

This artifact is a malicious PE32 executable that is an add-on tool for other Hoplight implants.

When malware is run it opens a log file C:\WINDOWS\Temp\ndb.dat that is used for the remainder of the program to log all activity.

The malware runs with an IP as an argument. It sends out a beacon to this IP and connects to it using the same FakeTLS/PolarSSL protocol as th
successful connection to a C2, it uses a named pipe called \\\\.\\pipe\\AnonymousPipe to connect to a running implant and sends tasking to the ru
returns the results of these taskings over the named pipe and the malware sends the results back to the C2.
fe43bc385b30796f5e2d94dfa720903c70e66bc91dfdcfb2f3986a1fea3fe8c5

Tags

trojan

Details

Name	F315BE41D9765D69AD60F0B4D29E4300
Size	147456 bytes
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	f315be41d9765d69ad60f0b4d29e4300
SHA1	f60c2bd78436a14e35a7e85feccb319d3cc040eb
SHA256	fe43bc385b30796f5e2d94dfa720903c70e66bc91dfdcfb2f3986a1fea3fe8c5
SHA512	bc8f821b4989076e441fbe5668cee0a388adcc375fac4a553f4c27423cd61c4500739820033b32f4197820ddf34decf1a043c6d34619aa
ssdeep	3072:pQWbIWSG5bzxbT33FiDZWTNArLioB4Gwhes:pR3SGtJ33YDZWTNMLiGah
Entropy	6.477832

Antivirus

Ahnlab	Trojan/Win32.Agent
Antiy	Trojan/Win32.Autophyte
Avira	TR/AD.APTLazerus.ifaaj
BitDefender	Gen:Variant.Graftor.487501
ClamAV	Win.Trojan.HiddenCobra-7402602-0
Cyren	W32/Trojan.CTPG-1488
ESET	a variant of Win32/NukeSped.AU trojan
Emsisoft	Gen:Variant.Graftor.487501 (B)
Ikarus	Trojan.Win32.NukeSped
K7	Trojan (0052cf421)
McAfee	Trojan-HidCobra
Microsoft Security Essentials	Trojan:Win32/Autophyte.E!rfn
NetGate	Trojan.Win32.Malware
Sophos	Troj/NukeSpe-D
Symantec	Trojan Horse
TrendMicro	BKDR_HO.9D36C86C
TrendMicro House Call	BKDR_HO.9D36C86C
VirusBlokAda	BScope.Trojan.Autophyte
Zillya!	Trojan.NukeSped.Win32.161

YARA Rules

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

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-08-21 12:39:06-04:00
Import Hash	00c4520b07e61d244e7e7b942ebae39f

PE Sections

MD5	Name	Raw Size	Entropy
7991745d0f6ed295154f066bb53ccbc2	header	4096	0.767780
cd39ffb10726106d9b85172804784b97	.text	114688	6.620841
3ab93f20dc7859f5510efbf121790dd7	.rdata	16384	5.991690
9fdf9be0cd049c58cb3718927458e69c	.data	4096	3.880827
330d3d9d2c3c1a342547cea468095f2a	.rsrc	4096	1.138029
cefd737bf48bc8375f92c8f7d9755e3a	.reloc	4096	5.221555

Packers/Compilers/Cryptors

Microsoft Visual C++ 6.0 DLL

f8f7720785f7e75bd6407ac2acd63f90ab6c2907d3619162dc41a8ffa40a5d03

Tags

trojan

Details

Name	D2DA675A8ADFEF9D0C146154084FFF62
Size	139264 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	d2da675a8adfef9d0c146154084fff62

SHA1	c55d080ea24e542397bbbfa00edc6402ec1c902c
SHA256	f8f7720785f7e75bd6407ac2acd63f90ab6c2907d3619162dc41a8ffa40a5d03
SHA512	06f531e49154d59f684475da95693df1fccd50b505e6d3ca028c9d84fcfc79ef287704dd0b24b022bfac6ba9ee581d19f440773dd00cfcfe
ssdeep	3072:1QGYFFzYCGUXBk/hbpjYr9Lde0NPV1Y88PxbE:1SFhYaXBkjYJLde0Nd1Hqb
Entropy	6.605300

Antivirus

Ahnlab	Trojan/Win32.Akdoor
Antiy	Trojan/Win32.Autophyte
Avira	TR/AD.APTLazerus.denpe
BitDefender	Gen:Variant.Graftor.487501
ClamAV	Win.Trojan.HiddenCobra-7402602-0
Cyren	W32/Trojan.ATKI-5308
ESET	a variant of Win32/NukeSped.AU trojan
Emsisoft	Gen:Variant.Graftor.487501 (B)
Huorong	Trojan/NukeSped.a
Ikarus	Trojan.Win32.NukeSped
K7	Trojan (0052cf421)
McAfee	Trojan-FPIA!D2DA675A8ADF
Microsoft Security Essentials	Trojan:Win32/Autophyte.E!dha
NANOAV	Trojan.Win32.NukeSped.fyopnf
NetGate	Trojan.Win32.Malware
Quick Heal	Trojan.Generic
Sophos	Troj/NukeSpe-F
Symantec	Trojan Horse
TrendMicro	BKDR_HO.9D36C86C
TrendMicro House Call	BKDR_HO.9D36C86C
VirusBlokAda	BScope.Trojan.Autophyte
Zillya!	Trojan.NukeSped.Win32.146

YARA Rules

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

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

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-07-14 18:40:25-04:00
Import Hash	86e90e40d8e53d1e5b06a22353734ed4

PE Sections

MD5	Name	Raw Size	Entropy
bf34ee8fcf71c0aa14531ae02d74f359	header	4096	0.647238
66e2b83909b4d47d3e3d20ad44df1acc	.text	114688	6.660284
d20ad0b8b42883ae6eb4c89cfbbd893b	.rdata	16384	6.057701
5e1b09084dfc15dda52bdac606eaed3d	.data	4096	3.824972

Packers/Compilers/Cryptors

Microsoft Visual C++ v6.0

Description

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

When the malware runs it checks a config file to determine where it should beacon back to. If the config file has not been modified the malware w following hard coded IPs:

--Begin IP List--

10.10.30.130

--End IP List--

Client uses uk.yahoo.com for client hello server name instead of naver.com.
32ec329301aa4547b4ef4800159940feb950785f1ab68d85a14d363e0ff2bc11

Tags

trojan

Details

Name	38FC56965DCCD18F39F8A945F6EBC439
Size	122880 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	38fc56965dccd18f39f8a945f6ebc439
SHA1	50736517491396015afdf1239017b9abd16a3ce9
SHA256	32ec329301aa4547b4ef4800159940feb950785f1ab68d85a14d363e0ff2bc11
SHA512	70a1568df0e97e8ab020f108e52ec861a0cdae936ac3340f1657565a8ac8a253179b4c451a79cb7c362fe60ff70be2694705110c67369c

ssdeep	1536:kSQWbe9BzK0xGtGVyDBWikDsD3bG0aII2Tm5TPb+5MI7jcg9YL23O:fQWbIWSG61UD3bGUI2Tm5TP2Njcmn+
Entropy	6.236928

Antivirus

Ahnlab	Trojan/Win32.Crypt
Antiy	Trojan/Win32.AGeneric
Avira	TR/AD.APTLazerus.sogzc
BitDefender	Gen:Variant.Graftor.487501
ClamAV	Win.Trojan.HiddenCobra-7402602-0
Cyren	W32/Trojan.ACES-2943
ESET	a variant of Win32/NukeSped.AU trojan
Emsisoft	Gen:Variant.Graftor.487501 (B)
Huorong	Trojan/NukeSped.a
Ikarus	Trojan.Win32.NukeSped
K7	Trojan (0052cf421)
McAfee	Trojan-FPIA!38FC56965DCC
Microsoft Security Essentials	Trojan:Win32/Nukesped.PA!MTB
NANOAV	Trojan.Win32.HiddenCobra.fyqdsh
NetGate	Trojan.Win32.Malware
Sophos	Troj/NukeSpe-F
Symantec	Trojan Horse
TrendMicro	BKDR_HO.9D36C86C
TrendMicro House Call	BKDR_HO.9D36C86C
VirusBlokAda	BScope.Trojan.Autophyte
Zillya!	Trojan.NukeSped.Win32.149

YARA Rules

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

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

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-12-12 12:58:45-05:00
Import Hash	2054fd7bbbbcb62441ba2a21c156d403

PE Sections

MD5	Name	Raw Size	Entropy
39af78f4af9f093c2eb4765202eab41a	header	4096	0.704943
48f0a09061c556cbde93f864f2adb2e3	.text	94208	6.479768
65fe1d182b2f7322719d142a81a901a8	.rdata	16384	5.812175
43cd1b0954c2785708b9e8da200242e9	.data	4096	2.465375
cab878079ca8c3f53ed3e0d0414e3a3a	.rsrc	4096	1.194369

Packers/Compilers/Cryptors

Microsoft Visual C++ v6.0

Description

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

When the malware runs it checks a config file to determine where it should beacon back to. If the config file has not been modified the malware w following hard coded IPs:

--Begin IP List--

218.255.24.226

--End IP List--

Client uses www.bing.com. Microsoft.com, and facebook.com for client hello server name instead of naver.com.
8a1d57ee05d29a730864299376b830a7e127f089e500e148d96d0868b7c5b520

Tags

backdoortrojan

Details

Name	5C0C1B4C3B1CFD455AC05ACE994AED4B
Size	348160 bytes
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	5c0c1b4c3b1cfd455ac05ace994aed4b
SHA1	69cda1f1adeeed455b519f9cf188e7787b5efa07
SHA256	8a1d57ee05d29a730864299376b830a7e127f089e500e148d96d0868b7c5b520

SHA512	084d2223934848594e23dbedab5064f98cd3d07d0783d4a7de66800a2a823daf73b0b044aea0ff9516538e6c478c8d18018c006c713e
ssdeep	6144:aR3SGkuDrOZm5Te5EXzO7h2ZMB6zJJ+KFvmjyFdzDs0dRb83hYnOQSzS7:aVSWrOZm5TeOjVMoJFFv+mdzDs+kYnOS
Entropy	7.540376

Antivirus

Ahnlab	Backdoor/Win32.Akdoor
Antiy	Trojan/Win32.Autophyte
Avira	TR/AD.APTLazerus.itcpp
BitDefender	Gen:Variant.Graftor.487501
ClamAV	Win.Trojan.HiddenCobra-7402602-0
Cyren	W32/Trojan.HLGX-3930
ESET	a variant of Win32/NukeSped.AU trojan
Emsisoft	Gen:Variant.Graftor.487501 (B)
Ikarus	Trojan.Win32.NukeSped
K7	Trojan (0052cf421)
McAfee	Trojan-HidCobra
Microsoft Security Essentials	Trojan:Win32/Autophyte.E!rfn
NetGate	Trojan.Win32.Malware
Sophos	Troj/NukeSpe-I
Symantec	Trojan.Hoplight
TrendMicro	BKDR_HO.9D36C86C
TrendMicro House Call	BKDR_HO.9D36C86C
VirusBlokAda	Trojan.Autophyte
Zillya!	Trojan.NukeSped.Win32.163

YARA Rules

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

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

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-08-12 05:20:38-04:00
Import Hash	3ca68e2a005e05e2c4831de87ae091c0

PE Sections

MD5	Name	Raw Size	Entropy
787ed8122e53d5ea17e3ece6d9fb7342	header	4096	0.782305
83b06d297acb20b05505da2d09905abd	.text	102400	6.523509
b2e739b37837f1c2b941660711daf98f	.rdata	16384	5.951907
cd8aa1387168caeb4604401aedb143eb	.data	4096	2.718596
8840ce03428c311935a20ac968c10ce7	.rsrc	217088	7.888219
2f0ede5fcdada29ec11ad8cd25c53f77	.reloc	4096	4.923777

Packers/Compilers/Cryptors

Microsoft Visual C++ 6.0 DLL

Description

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

This file is dropped by a different binary into System32 and then run as a service. When the malware runs it checks a config file to determine whe to. If the config file has not been modified the malware will beacon back to the following hard coded IPs:

--Begin IP List--

81.94.192.147
112.175.92.57
181.39.135.126
197.211.212.59

--End IP List--

0608e411348905145a267a9beaf5cd3527f11f95c4afde4c45998f066f418571

Tags

trojan

Details

Name	34E56056E5741F33D823859E77235ED9
Size	151552 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	34e56056e5741f33d823859e77235ed9

SHA1	fcc2dcbac7d3cbcf749f6aab2f37cc4b62d0bb64
SHA256	0608e411348905145a267a9beaf5cd3527f11f95c4afde4c45998f066f418571
SHA512	93ac57f0b9bf48e39870b88f918f9b6e33404c1667d5f98d0965736e9e001b18152530f1c3a843b91929d308f63739faf3de62077bbfb15
ssdeep	3072:nQWbIWSGw0CkXbhM1Vsm5TJYwMrzPoXL8GnQj3y3:nR3SGQYM16m5TJDwPo7bUC3
Entropy	6.652398

Antivirus

Ahnlab	Trojan/Win32.Agent
Antiy	Trojan/Win32.Autophyte
Avira	HEUR/AGEN.1023221
BitDefender	Gen:Variant.Graftor.487501
ClamAV	Win.Trojan.HiddenCobra-7402602-0
Cyren	W32/Trojan.PGQL-0621
ESET	a variant of Win32/NukeSped.AU trojan
Emsisoft	Gen:Variant.Graftor.487501 (B)
Huorong	Trojan/NukeSped.a
Ikarus	Trojan.Win32.NukeSped
K7	Trojan (0052cf421)
McAfee	Trojan-FPIA!34E56056E574
Microsoft Security Essentials	Trojan:Win32/Autophyte.E!rfn
NANOAV	Trojan.Win32.NukeSped.fyqduv
Quick Heal	Trojan.Generic
Sophos	Troj/NukeSpe-F
Symantec	Trojan Horse
TrendMicro	TROJ_FR.D0256DD5
TrendMicro House Call	TROJ_FR.D0256DD5
VirusBlokAda	BScope.Trojan.Autophyte
Zillya!	Trojan.NukeSped.Win32.166

YARA Rules

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

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

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-08-12 03:44:57-04:00
Import Hash	e93a06b89e75751a9ac2c094ca7da8b0

PE Sections

MD5	Name	Raw Size	Entropy
a45f9a7c2174752a1472fb634ba9d8c7	header	4096	0.715236
2b9f5ce0725453a209a416ab7a13f3df	.text	98304	6.576807
03605ec3eefe3b70e118cea4b8655229	.rdata	16384	5.866137
5ac0ab0641ec076e15dd1468e11c57cd	.data	4096	2.680020
58ede934084bbe73fa7f9e0d32c4fafb	.rsrc	28672	7.045289

Packers/Compilers/Cryptors

Microsoft Visual C++ v6.0

Relationships

0608e41134... Connected_To 14.140.116.172

Description

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

When the malware runs it checks a config file to determine where it should beacon back to. If the config file has not been modified the malware w following hard coded IPs:

---Begin IP List---

14.140.116.172

---End IP List---

Client uses uk.yahoo.com for client hello server name instead of naver.com.

14.140.116.172

Tags

command-and-control

Relationships

14.140.116.172 Connected_From 0608e411348905145a267a9beaf5cd3527f11f95c4afde4c45998f066f418571

Description

The file 34E56056E5741F33D823859E77235ED9 beacons to this hard coded IP.

b05aae59b3c1d024b19c88448811debef1eada2f51761a5c41e70da3db7615a9

Tags

trojan

Details

Name	2FF1688FE866EC2871169197F9D46936
Size	229500 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	2ff1688fe866ec2871169197f9d46936
SHA1	6dc37ff32ea70cbd0078f1881a351a0a4748d10e
SHA256	b05aae59b3c1d024b19c88448811debef1eada2f51761a5c41e70da3db7615a9
SHA512	91c3a6e84ca728ecc26d63b91a09f3081288c9b9592430035b9ea50ba7cf2d4b4ddba4711933d17013d3d06fcb8d70789a37ddfa5c741
ssdeep	6144:GANjUaXCXwz+vLFOLEq3VNwO9zyPqYNkHms:bNjxXgA9uPqR
Entropy	6.385793

Antivirus

Ahnlab	Trojan/Win32.Agent
Antiy	Trojan/Win32.NukeSped
Avira	TR/AD.APTLazerus.oytdw
BitDefender	Trojan.GenericKD.32416090
ClamAV	Win.Trojan.HiddenCobra-7402602-0
Cyren	W32/Trojan.GCCR-6631
ESET	a variant of Win32/NukeSped.AI trojan
Emsisoft	Trojan.GenericKD.32416090 (B)
Ikarus	Trojan.Win32.NukeSped
K7	Trojan (005329311)
McAfee	Trojan-HidCobra
Microsoft Security Essentials	Trojan:Win32/Nukesped.PA!MTB
NetGate	Trojan.Win32.Malware
Quick Heal	Trojan.Generic
Sophos	Troj/Inject-DZV
Symantec	Trojan.Gen.MBT
TrendMicro	BKDR_HO.9D36C86C
TrendMicro House Call	BKDR_HO.9D36C86C
Zillya!	Trojan.NukeSped.Win32.160

YARA Rules

- rule crypt_constants_2
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $ = {efcdab90}
    $ = {558426fe}
    $ = {7856b4c2}
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them
  }
- rule lsfr_constants
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $ = {efcdab90}
    $ = {558426fe}
    $ = {7856b4c2}
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them
  }
- rule polarSSL_servernames
  {
  meta:
    Author="NCCIC trusted 3rd party"
    Incident="10135536"
    Date = "2018/04/19"
    category = "hidden_cobra"
    family = "n/a"
    description = "n/a"
  strings:
    $polarSSL = "fjiejffndxklfsdkfjsaadiepwn"
    $sn1 = "www.google.com"
    $sn2 = "www.naver.com"
  condition:
        (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) -- 0x4550) and ($polarSSL and 1 of ($sn*))
  }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-06-13 11:12:43-04:00
Import Hash	8948765c0ef7c91beff2e97907c801d0

PE Sections

MD5	Name	Raw Size	Entropy
eb0f947605842ea84fea9d8d8382f056	header	4096	0.684814
f9aa8191af45813b80031064403835f1	.text	192512	6.400854
bbcbbf5f54deaee51d41d404973c30e4	.rdata	16384	6.228868
8ea12cda731d50b93944d8534c11402c	.data	12288	3.927662
06d5d2729a367d565819e6867d8caea7	.rsrc	4096	3.317978

Packers/Compilers/Cryptors

Microsoft Visual C++ v6.0

Description

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

When the malware runs it checks a config file to determine where it should beacon back to. If the config file has not been modified the malware w following hard coded IPs:

---Begin IP List---

210.137.6.37
119.18.230.253
221.138.17.152

---End IP List---

Client uses naver.com for client hello server name.

119.18.230.253

Tags

command-and-control

Description

The file 2FF1688FE866EC2871169197F9D46936 beacons to this hard coded IP.

210.137.6.37

Tags

command-and-control

Description

The file 2FF1688FE866EC2871169197F9D46936 beacons to this hard coded IP.

221.138.17.152

Tags

command-and-control

Description

The file 2FF1688FE866EC2871169197F9D46936 beacons to this hard coded IP.

ba80cb0a08908782f4b6e88aa15e2d306b19bc93e79bd8770bf8be904fd1bd09

Tags

trojan

Details

Size	117591 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	3dbd47cc12c2b7406726154e2e95a403
SHA1	afaa88c46666e5684b89b94ef2c4bc82e4c00845
SHA256	ba80cb0a08908782f4b6e88aa15e2d306b19bc93e79bd8770bf8be904fd1bd09
SHA512	c13e79b4c7e7dd53736e87836930d4aafe5a9c6c467c31c976253ebc0b031424eb2d92a04bbdcb7b610afc5d93f2b752b14663b2e9c0
ssdeep	1536:/sQWbe9BzK0xGtFOpVyDpWpQCnRx/bV3Q3Wgim5TjZU15MX7jbQnKVYJ3n:EQWbIWSGWjBjrbV3jgim5TjqPgjbQgA
Entropy	6.387236

Antivirus

Ahnlab	Trojan/Win32.Generic
ClamAV	Win.Trojan.HiddenCobra-7402602-0
ESET	a variant of Win32/NukeSped.AU trojan
Huorong	Trojan/NukeSped.a
McAfee	Trojan-HidCobra!3DBD47CC12C2
Microsoft Security Essentials	Trojan:Win32/Autophyte.E!dha
Symantec	Trojan.Hoplight
VirusBlokAda	BScope.Trojan.Autophyte

YARA Rules

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

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-09-03 11:02:30-04:00
Import Hash	7d69af70a4430663ca427aa423f7c5ea

PE Sections

MD5	Name	Raw Size	Entropy
8291bca724e71f42f0653dbd18357965	header	4096	0.642884
a883335516b2b5c2ff7377e5532611af	.text	94208	6.462877
63fb256f6eaf5fbd897d36dd4777ef89	.rdata	16384	5.845991
8934903570874d7e20867e8c89be5c64	.data	2903	3.458180

Packers/Compilers/Cryptors

Microsoft Visual C++ v6.0

Relationships

ba80cb0a08...	Connected_To	117.239.241.2
ba80cb0a08...	Connected_To	217.117.4.110

Description

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

When the malware runs it checks a config file to determine where it should beacon back to. If the config file has not been modified the malware w following hardcoded IPs.

--Begin Hardcoded IP--

117.239.241.2
217.117.4.110

--End Hardcoded IP--

217.117.4.110

Tags

command-and-control

Relationships

217.117.4.110 Connected_From ba80cb0a08908782f4b6e88aa15e2d306b19bc93e79bd8770bf8be904fd1bd09

Description

The file ba80cb0a08908782f4b6e88aa15e2d306b19bc93e79bd8770bf8be904fd1bd09 beacons to this hardcoded IP.

44a93ea6e6796530bb3cf99555dfb3b1092ed8fb4336bb198ca15b2a21d32980

Tags

backdoordroppertrojan

Details

Size	557681 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	4e595db3b612e1e9da90a0ef7d740792
SHA1	1483720917e754d05818e64ae07b320ffbdf4d78
SHA256	44a93ea6e6796530bb3cf99555dfb3b1092ed8fb4336bb198ca15b2a21d32980
SHA512	fadd5aea13935cfc592da535c0b4b182d3b2c50cfc5122dd9bb4040a6298e5b0db788d9025b5043e216a242334fd4a08ae69597e0a13(
ssdeep	12288:j6k9os/EpYE+DMX6GHU3ZSrLwQ+ruZdwl4TntpdK9roGOeAQ:j6Qos/EpYEWGHFrL1+iZdwVTtp09rbOi
Entropy	7.850778

Antivirus

Ahnlab	Backdoor/Win32.Agent
Avira	TR/Dropper.Gen
ESET	a variant of Win32/NukeSped.O trojan
Ikarus	Trojan.Win32.NukeSped
Microsoft Security Essentials	Trojan:Win32/Nukesped.PA!MTB

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2018-02-12 15:04:34-05:00
Import Hash	1e6c10653c6b505369db00e880dbfecb

PE Sections

MD5	Name	Raw Size	Entropy
aef5c3923e5820f46533bf0b26cd7c4e	header	4096	0.626079
70a3e4024020c2792542fcb13130235f	.text	73728	6.252791
f29b61b835618a1c4a0c2cf966badbe9	.rdata	12288	4.414075
0b968078c58131b96a48ffc77413a61b	.data	4096	2.653332

Packers/Compilers/Cryptors

Microsoft Visual C++ v6.0

Description

This executable must be run with argument 15975345682 to execute and then drops C:\Windows\system32\dispark.dll (E5D1C42E5CA7A0AC3A
custom packed loader.

E5D1C42E5CA7A0AC3A3B31BD0F290E84 drops 535C879CA109DBECD336E1DE0ECCB696 that runs as a service.
823d255d3dc8cbc402527072a9220e4c38655de1a3e55a465db28b55d3ac1bf8

Tags

trojan

Details

Size	692274 bytes
Type	PE32+ executable (GUI) x86-64, for MS Windows
MD5	894b81b907c23f927a3f38cfd30f32da
SHA1	411a320c389e492bf41eb6c5708809721f28a81f
SHA256	823d255d3dc8cbc402527072a9220e4c38655de1a3e55a465db28b55d3ac1bf8
SHA512	ea550ce5ad8f58fdaf74476cda5255117b4dd3c64ef70ba0f5f08e3c2af62ba45fdafec56ee7d76de3e59894bddf39e26d6c787e2876552
ssdeep	12288:yeR6alRBGA44gibT2QPAdfyGwspLvgwEq8kkAwkeJbJPCYzH:yeR6alP44JbydfyGn84KAwbxJPCYD
Entropy	7.849516

Antivirus

Ahnlab	Trojan/Win32.Akdoor
Antiy	Trojan/Win64.NukeSped
ESET	a variant of Win64/NukeSped.AH trojan
K7	Trojan (00545d8d1)
Zillya!	Trojan.Agent.Win32.1135323

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2018-02-12 15:06:28-05:00
Import Hash	347c977c6137a340c7cc0fcd5b224aef

PE Sections

MD5	Name	Raw Size	Entropy
28fc69ad12a0765af4cc06fbd261cb24	header	1024	2.672166
88425c71e7e293d43db9868e4693b365	.text	89088	6.415516
bb0048e4f3851ea07b365828ddf613f7	.rdata	26624	4.912250
50e3efe1a6ea325c87f8e86e2fbd40b4	.data	5632	2.093641
f56a65eb9562d6c6d607f867d1d0fd09	.pdata	4608	4.725531
6a9a84d523e53e1d43c31b2cc069930c	.rsrc	1536	4.308150
dab5e290c15de9634d93d8f592a44633	.reloc	1536	2.912599

Packers/Compilers/Cryptors

Microsoft Visual C++ 8.0 (DLL)

Description

This executable must be run with argument 15975345682 to execute and then drops C:\Windows\system32\diskpart.dll (7AFF84FB44840E4FD5
custom packed loader.

7AFF84FB44840E4FD53CC9561172E14B drops BD674814315892B937BC91A10783D140 that runs as a service.

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
b9a26a5692...	Connected_To	117.239.241.2
b9a26a5692...	Connected_To	195.158.234.60
b9a26a5692...	Connected_To	218.255.24.226
117.239.241.2	Connected_From	ba80cb0a08908782f4b6e88aa15e2d306b19bc93e79bd8770bf8be904fd1bd09
117.239.241.2	Connected_From	b9a26a569257fbe02c10d3735587f10ee58e4281dba43474dbdef4ace8ea7101
218.255.24.226	Connected_From	b9a26a569257fbe02c10d3735587f10ee58e4281dba43474dbdef4ace8ea7101
195.158.234.60	Connected_From	b9a26a569257fbe02c10d3735587f10ee58e4281dba43474dbdef4ace8ea7101
0608e41134...	Connected_To	14.140.116.172
14.140.116.172	Connected_From	0608e411348905145a267a9beaf5cd3527f11f95c4afde4c45998f066f418571
ba80cb0a08...	Connected_To	117.239.241.2
ba80cb0a08...	Connected_To	217.117.4.110
217.117.4.110	Connected_From	ba80cb0a08908782f4b6e88aa15e2d306b19bc93e79bd8770bf8be904fd1bd09

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 most provide initial indicators for computer and network defense. To request additional analysis, please contact CISA and provide information regarding 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 should 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

February 14, 2020: v3 - Initial Version

February 19, 2020: v4 - Updated file MSDFMAPI.INI

Please share your thoughts.

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