MAR-10301706-2.v1 - North Korean Remote Access Tool: VIVACIOUSGIFT

us-cert.cisa.gov/ncas/analysis-reports/ar20-239b

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained 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 foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol (TLP), see http://www.us-cert.gov/tlp.

Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts between the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the Department of Defense (DoD). Working with U.S. Government partners, DHS, FBI, and DoD identified Remote Access Tool (RAT) malware variants used by the North Korean government. This malware variant has been identified as VIVACIOUSGIFT. The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA. For more information on HIDDEN COBRA activity, visit https[:]//www[.]us-cert.gov/hiddencobra.

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

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

This report looks at the malware samples known as VIVACIOUSGIFT that is used by advanced persistent threat (APT) cyber actors as a network proxy tool. The proxy requires an encrypted command line argument for its source and destination Internet Protocol (IP) addresses and has command and control (C2) functionality to retrieve and set the destination IP. The command line argument can also contain a source proxy IP, port, and password. The source proxy is used as an additional proxy when communicating with the source IP. The library libcurl version 7.94.1 is used when communicating with the source proxy.
For a downloadable copy of IOCs, see MAR-10301706-2.v1.stix.

Submitted Files (6)

70b494b0a8fdf054926829dcb3235fc7bd0346b6a19faf2a57891c71043b3b38 (70b494b0a8fdf054926829dcb3235f...)

8cad61422d032119219f465331308c5a61e21c9a3a431b88e1f8b25129b7e2a1 (8cad61422d032119219f465331308c...)

9a776b895e93926e2a758c09e341accb9333edc1243d216a5e53f47c6043c852 (9a776b895e93926e2a758c09e341ac...)

a917c1cc198cf36c0f2f6c24652e5c2e94e28d963b128d54f00144d216b2d118 (a917c1cc198cf36c0f2f6c24652e5c...)

aca598e2c619424077ef8043cb4284729045d296ce95414c83ed70985c892c83 (aca598e2c619424077ef8043cb4284...)

f3ca8f15ca582dd486bd78fd57c2f4d7b958163542561606bebd250c827022de (f3ca8f15ca582dd486bd78fd57c2f4...)

Findings

a917c1cc198cf36c0f2f6c24652e5c2e94e28d963b128d54f00144d216b2d118

Tags

HIDDEN-COBRAproxytrojan

Details

Name	a917c1cc198cf36c0f2f6c24652e5c2e94e28d963b128d54f00144d216b2d118
Size	408576 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	40e698f961eb796728a57ddf81f52b9a

SHA1	50b4f9a8fa6803f0aabb6fd9374244af40c2ba4c
SHA256	a917c1cc198cf36c0f2f6c24652e5c2e94e28d963b128d54f00144d216b2d118
SHA512	2ee35d902f2a4022488bdc75cf7531f75de7e8bb4ca8645a9448f33051e835f0cea62e0157ac292187cd9406901f80570b8e17be52fee4a
ssdeep	12288:E30MB7N+man4IrT0qhPyRg8o//ND6lAMYqcl:i0YNwrT0qhPFtHN2lLYq
Entropy	6.651902

Antivirus

Ahnlab	Trojan/Win32.Banker
Antiy	Trojan[Banker]/Win32.Agent
Avira	TR/SpyBanker.Agent.AM
BitDefender	Trojan.GenericKD.4446633
ClamAV	Win.Trojan.Agent-6971031-0
Comodo	TrojWare.Win32.Ransom.Teerac.C
Cyren	W32/Banker.FTBC-3937
ESET	Win32/Spy.Banker.ADRO trojan
Emsisoft	Trojan.GenericKD.4446633 (B)
Ikarus	Trojan-Spy.Banker
K7	Riskware (0040eff71)
Lavasoft	Trojan.GenericKD.4446633
McAfee	Generic.abb
Microsoft Security Essentials	TrojanSpy:Win32/Banker
NANOAV	Trojan.Win32.Agent.enikaf
Quick Heal	TrojanSpy.Banker
Sophos	Mal/Generic-L
Symantec	Trojan Horse
TrendMicro	BKDR_KL.89AB2FB2
TrendMicro House Call	BKDR_KL.89AB2FB2
Vir.IT eXplorer	Trojan.Win32.Banker.FUW
VirusBlokAda	TrojanBanker.Agent
Zillya!	Trojan.Agent.Win32.763316

YARA Rules

```
rule CISA_3P_10301706_02 : HiddenCobra TWOPENCE backdoor dropper proxy spyware trojan
{
  meta:
    Author = "CISA Trusted Third Party"
    Incident = "10301706.r2.v1"
    Date = "2020-08-11"
    Actor = "Hidden Cobra"
    Category = "Backdoor Dropper Proxy Spyware Trojan"
    Family = "TWOPENCE"
    Description = "Detects strings in TWOPENCE proxy tool"
    MD5_1 = "40e698f961eb796728a57ddf81f52b9a"
    SHA256_1 = "a917c1cc198cf36c0f2f6c24652e5c2e94e28d963b128d54f00144d216b2d118"
    MD5_2 = "dfd09e91b7f86a984f8687ed6033af9d"
    SHA256_2 = "aca598e2c619424077ef8043cb4284729045d296ce95414c83ed70985c892c83"
    MD5_3 = "bda82f0d9e2cb7996d2eefdd1e5b41c4"
    SHA256_3 = "f3ca8f15ca582dd486bd78fd57c2f4d7b958163542561606bebd250c827022de"
    MD5_4 = "97aaf130cfa251e5207ea74b2558293d"
    SHA256_4 = "9a776b895e93926e2a758c09e341accb9333edc1243d216a5e53f47c6043c852"
    MD5_5 = "889e320cf66520485e1a0475107d7419"
    SHA256_5 = "8cad61422d032119219f465331308c5a61e21c9a3a431b88e1f8b25129b7e2a1"
  strings:
    $cmd1 = "ssylka"
    $cmd2 = "ustanavlivat"
    $cmd3 = "poluchit"
    $cmd4 = "pereslat"
    $cmd5 = "derzhat"
    $cmd6 = "vykhodit"
    $cmd7 = "Nachalo"
    $cmd8 = "kliyent2podklyuchit"
    $frmt1 = "Host: %s%s%s:%hu"
    $frmt2 = "%s%s%s%s%s%s%s%s%s%s"
  condition:
    (4 of ($cmd*)) and (1 of ($frmt*))
}
```

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2016-07-08 19:11:36-04:00
Import Hash	3415ed7e09a44243bcabe4422aeef7dc

PE Sections

MD5	Name	Raw Size	Entropy
0e135280ecde05507a86c5681ee38986	header	1024	2.480337
dfcc176fede07939cc4deb950858b6ce	.text	333824	6.579572
d72f6b9398a7f267dfe5f1bd44778d62	.rdata	51712	6.391152
1e41f003bafe97cb5bfb59b3ad7d7531	.data	6656	3.459925
a8d51b81460671e8fb3df438f0f7fc28	.reloc	15360	5.531184

Packers/Compilers/Cryptors

Microsoft Visual C++ ?.?

Description

This file is a 32-bit Windows executable. The proxy requires a single command line argument. The argument can consist of a maximum of four encrypted strings delineated with the pipe character ("|"). When the four strings are parsed and decrypted, the strings represent the following: source IP and port, destination IP and port, source proxy IP and port, and source proxy password. The IP and port strings have the following format: <IP:port>. If the destination IP is missing from the command line argument, the proxy will wait to get the destination IP from the actor.

The source proxy IP and port, as well as the source proxy password, are used as an additional proxy when communicating with the source IP. When communicating with the source proxy, the proxy will use libcurl with the options CURLOPT_HTTPPROXYTUNNEL and CURLOPT_NOBODY.

The following is an example of an encrypted command line argument that is missing the destination IP:

--Begin encrypted command line argument--
<encrypted_string>| |<encrypted_string>|<encrypted_string>
--End encrypted command line argument--

--Begin decrypted command line argument--
<IP>:<port>| |<IP>:<port>|<password>
--End decrypted command line argument--

The encrypted strings inside the command line argument can be individually decrypted with the Python script provided in Figure 1.

Below is the flow of events that happens when the proxy starts and is issued the commands "ustanavlivat" and "pereslat". In the following example, the command line argument does not contain a source proxy. The command line argument can contain a source proxy IP, port, and password. If they exist, the proxy will route all traffic to the source IP through the source proxy. When communicating with the source proxy, the proxy uses the library libcurl with options CURLOPT_HTTPPROXYTUNNEL and CURLOPT_NOBODY. The data that is sent and received is encrypted using a custom encryption routine.

First, it connects to source IP and sends initialization message "Nachalo". It sends a custom hash of "Dazdrav$958478Zohsf9q@%5555ahshdnZXniohs". In return it receives two bytes of data. It sends the length (4 bytes) of string "kliyent2podklyuchit" and then sends the string "kliyent2podklyuchit". It sends the length (4 bytes) of string "Nachalo" and then sends the "Nachalo".

Next, it receives C2 command "ustanavlivat" to set the destination IP address. It receives and decrypts the length of the string "ustanavlivat" and then receives and decrypts the string "ustanavlivat".

Then, it receives C2 command "pereslat" to start the proxy functionality. It receives and decrypts the length of the string "pereslat" and then receives and decrypts the string "pereslat".

Next, it connects to source IP and sends start proxy functionality message "ssylka". It sends a custom hash of "Dazdrav$958478Zohsf9q@%5555ahshdnZXniohs". In response it receives data. Then it sends the length (4 bytes) of string "kliyent2podklyuchit" and then sends the string "kliyent2podklyuchit". Then it sends the length (4 bytes) of string "ssylka" and then sends the string "ssylka".

Finally, it connects to destination IP and starts proxy functionality between source and destination IP.

The proxy uses a custom encryption routine to encode the data sent. The Python script provided in Figure 2 can decode the data.
Screenshots

```
def decode(encoded):
  key = "cEzQfoPw"
  dest = ""
  i = 0

  while(True):
    chara = ord(encoded[i])
    charb = ord(encoded[i+1])
    v6 = (chara - 0x37) if (chara>0x39) else (chara - 0x30)
    v7 = 0x10 * v6
    v9 = (charb - 0x37) if (charb>0x39) else (charb - 0x30)
    char = (i/2) ^ ord(key[(i/2)%8]) ^ (v7|v9)
    dest += str(chr(char))
    if(i==len(encoded)-2): break
    i+=2
  return dest
```

Figure 1 - The Python script to individually decrypt the encrypted strings inside the command line argument.

```
key = [0x74, 0x64, 0x40, 0x40, 0x00, 0x47, 0xB0, 0x62, 0x0E, 0x69, 0xF3, 0x22,
 0x8D, 0x65, 0x40, 0xBF, 0x39, 0x24, 0xA6, 0xC3, 0xBB, 0x8E, 0x68, 0xEB, 0xB5]

def decode(length, data):
  ret = ""
  for i in range(length):
    v3 = data[i]
    v4 = 0x14
    while v4>0:
      v3 = v3 + key[v4+4]
      if v3 > 255: v3 -= 256
      v3 = (v3 ^ key[v4+4]) + key[v4+3]
      if v3 > 255: v3 -= 256
      v3 = (v3 ^ key[v4+3]) + key[v4+2]
      if v3 > 255: v3 -= 256
      v3 = (v3 ^ key[v4+2]) + key[v4+1]
      if v3 > 255: v3 -= 256
      v3 = (v3 ^ key[v4+1]) + key[v4]
      if v3 > 255: v3 -= 256
      v4 -= 5
      v3 = v3 ^ key[v4+5]
    ret += str(chr(v3))
  return ret
```

Figure 2 - The Python script to decode the encoded data sent by the proxy custom encryption routine.

aca598e2c619424077ef8043cb4284729045d296ce95414c83ed70985c892c83

Tags

HIDDEN-COBRAdropperproxyspywaretrojan

Details

Name	aca598e2c619424077ef8043cb4284729045d296ce95414c83ed70985c892c83
Size	232960 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	dfd09e91b7f86a984f8687ed6033af9d
SHA1	b8fe7884d2dc4983fb0fbca192694ce2f4685e23
SHA256	aca598e2c619424077ef8043cb4284729045d296ce95414c83ed70985c892c83
SHA512	641dd95c101ae7566defb1a24279badb8c7aa94331442e0f470866b6a1e44c8790a71e83cc1cb188d7530c08bf0e5d227d35caa9a2cf7e
ssdeep	3072:XU5r72JE+FYWR0jZLShk4cPT/QzSaQ0sCFneZTznIhZJJcrJ1GHeV9:XU5uJpYnZL05STQNddFnAnGZIrV
Entropy	6.524225

Antivirus

Ahnlab	Trojan/Win32.Alreay
Antiy	Trojan[Banker]/Win32.Alreay
ClamAV	Win.Trojan.Agent-6971031-0
Comodo	TrojWare.Win32.TrojanDropper.Agent.PRQ
Cyren	W32/Alreay.SQQX-6406
ESET	a variant of Win32/Spy.Banker.ADRO trojan
K7	Spyware (005198041)
McAfee	GenericRXFQ-MX!DFD09E91B7F8
Microsoft Security Essentials	TrojanSpy:Win32/Banker!dha
Symantec	Trojan Horse
TrendMicro	TSPY_BA.C25E7684
TrendMicro House Call	TSPY_BA.C25E7684
Zillya!	Trojan.Alreay.Win32.42

YARA Rules

```
rule CISA_3P_10301706_02 : HiddenCobra TWOPENCE backdoor dropper proxy spyware trojan
{
  meta:
    Author = "CISA Trusted Third Party"
    Incident = "10301706.r2.v1"
    Date = "2020-08-11"
    Actor = "Hidden Cobra"
    Category = "Backdoor Dropper Proxy Spyware Trojan"
    Family = "TWOPENCE"
    Description = "Detects strings in TWOPENCE proxy tool"
    MD5_1 = "40e698f961eb796728a57ddf81f52b9a"
    SHA256_1 = "a917c1cc198cf36c0f2f6c24652e5c2e94e28d963b128d54f00144d216b2d118"
    MD5_2 = "dfd09e91b7f86a984f8687ed6033af9d"
    SHA256_2 = "aca598e2c619424077ef8043cb4284729045d296ce95414c83ed70985c892c83"
    MD5_3 = "bda82f0d9e2cb7996d2eefdd1e5b41c4"
    SHA256_3 = "f3ca8f15ca582dd486bd78fd57c2f4d7b958163542561606bebd250c827022de"
    MD5_4 = "97aaf130cfa251e5207ea74b2558293d"
    SHA256_4 = "9a776b895e93926e2a758c09e341accb9333edc1243d216a5e53f47c6043c852"
    MD5_5 = "889e320cf66520485e1a0475107d7419"
    SHA256_5 = "8cad61422d032119219f465331308c5a61e21c9a3a431b88e1f8b25129b7e2a1"
  strings:
    $cmd1 = "ssylka"
    $cmd2 = "ustanavlivat"
    $cmd3 = "poluchit"
    $cmd4 = "pereslat"
    $cmd5 = "derzhat"
    $cmd6 = "vykhodit"
    $cmd7 = "Nachalo"
    $cmd8 = "kliyent2podklyuchit"
    $frmt1 = "Host: %s%s%s:%hu"
    $frmt2 = "%s%s%s%s%s%s%s%s%s%s"
  condition:
    (4 of ($cmd*)) and (1 of ($frmt*))
}
```

ssdeep Matches

99 9a776b895e93926e2a758c09e341accb9333edc1243d216a5e53f47c6043c852

PE Metadata

Compile Date	2016-09-18 23:24:39-04:00
Import Hash	6b8fa355d78d649f199232a25e22d630

PE Sections

MD5	Name	Raw Size	Entropy
41a5273e6d92dfe9de72f76c18f6475f	header	1024	2.398805
e6412e7fb561ead2b3eddef9bafd3518	.text	198656	6.554337
a9890fd54b24cf53425649a92fe290ad	.rdata	18432	5.115959
884e0d48d1830995eeade874d295ced0	.data	5632	3.201975
0e79f25ba5ec9ae1502fe80ec7b08f79	.reloc	9216	5.674607

Packers/Compilers/Cryptors

Microsoft Visual C++ ?.?

Description

This file is a 32-bit Windows executable. It has similar functionality as a917c1cc198cf36c0f2f6c24652e5c2e94e28d963b128d54f00144d216b2d118.

f3ca8f15ca582dd486bd78fd57c2f4d7b958163542561606bebd250c827022de

Tags

HIDDEN-COBRAproxytrojan

Details

Name	f3ca8f15ca582dd486bd78fd57c2f4d7b958163542561606bebd250c827022de
Size	265216 bytes
Type	PE32+ executable (GUI) x86-64, for MS Windows
MD5	bda82f0d9e2cb7996d2eefdd1e5b41c4
SHA1	9ff715209d99d2e74e64f9db894c114a8d13229a
SHA256	f3ca8f15ca582dd486bd78fd57c2f4d7b958163542561606bebd250c827022de
SHA512	6774cc49f5200d1a427b5a2af77d27eaac671f405e01f3ded2d152e5e08d1217d2b3b9d8508d2924aee5f0925abc32f83645756cf248222
ssdeep	6144:+TW3SZ4GvcPPWi9JhJTxPm26ebMk5Q35m8LERov:invQThJsexib
Entropy	6.304640

Antivirus

Ahnlab	Trojan/Win32.Alreay
Antiy	Trojan[Banker]/Win32.Alreay
Avira	TR/AD.APTLazerus.dsenf
BitDefender	Gen:Variant.Razy.368693
ClamAV	Win.Trojan.Agent-6971031-0
Comodo	Malware
Cyren	W64/Alreay.C
ESET	a variant of Win64/NukeSped.BB trojan
Emsisoft	Gen:Variant.Razy.368693 (B)
Ikarus	Trojan.Win64.Nukesped
K7	Trojan (00538e2b1)
Lavasoft	Gen:Variant.Razy.368693
McAfee	PWS-Banker.gen.gj
Symantec	Trojan.Gen.6
Systweak	trojan.banker
TrendMicro	BKDR64_.8979788A
TrendMicro House Call	BKDR64_.8979788A
VirusBlokAda	TrojanBanker.Alreay
Zillya!	Trojan.GenericKD.Win32.133035

YARA Rules

```
rule CISA_3P_10301706_02 : HiddenCobra TWOPENCE backdoor dropper proxy spyware trojan
{
  meta:
    Author = "CISA Trusted Third Party"
    Incident = "10301706.r2.v1"
    Date = "2020-08-11"
    Actor = "Hidden Cobra"
    Category = "Backdoor Dropper Proxy Spyware Trojan"
    Family = "TWOPENCE"
    Description = "Detects strings in TWOPENCE proxy tool"
    MD5_1 = "40e698f961eb796728a57ddf81f52b9a"
    SHA256_1 = "a917c1cc198cf36c0f2f6c24652e5c2e94e28d963b128d54f00144d216b2d118"
    MD5_2 = "dfd09e91b7f86a984f8687ed6033af9d"
    SHA256_2 = "aca598e2c619424077ef8043cb4284729045d296ce95414c83ed70985c892c83"
    MD5_3 = "bda82f0d9e2cb7996d2eefdd1e5b41c4"
    SHA256_3 = "f3ca8f15ca582dd486bd78fd57c2f4d7b958163542561606bebd250c827022de"
    MD5_4 = "97aaf130cfa251e5207ea74b2558293d"
    SHA256_4 = "9a776b895e93926e2a758c09e341accb9333edc1243d216a5e53f47c6043c852"
    MD5_5 = "889e320cf66520485e1a0475107d7419"
    SHA256_5 = "8cad61422d032119219f465331308c5a61e21c9a3a431b88e1f8b25129b7e2a1"
  strings:
    $cmd1 = "ssylka"
    $cmd2 = "ustanavlivat"
    $cmd3 = "poluchit"
    $cmd4 = "pereslat"
    $cmd5 = "derzhat"
    $cmd6 = "vykhodit"
    $cmd7 = "Nachalo"
    $cmd8 = "kliyent2podklyuchit"
    $frmt1 = "Host: %s%s%s:%hu"
    $frmt2 = "%s%s%s%s%s%s%s%s%s%s"
  condition:
    (4 of ($cmd*)) and (1 of ($frmt*))
}
```

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2016-05-01 23:24:39-04:00
Import Hash	b2b084698f33fd93bc9e72f0c2af26b5

PE Sections

MD5	Name	Raw Size	Entropy
379ffb6e4aeb96c753dbe1f16dae01db	header	1024	2.516799
33c1647f8f3a870e4c8f9b48b5ec2c82	.text	212480	6.373885
5bb6bf3a50e4982066d5746d99945853	.rdata	31232	5.302106
a62c434f5beb6282b437c5e0dc40c616	.data	7168	2.877953
6ba7963edd09a132976d6830462fc17f	.pdata	11776	5.348074
06ce263d0dc81197b88ff3f576787648	.reloc	1536	2.915027

Packers/Compilers/Cryptors

Microsoft Visual C++ 8.0 (DLL)

Description

This file is a 64-bit Windows executable. It has similar functionality as a917c1cc198cf36c0f2f6c24652e5c2e94e28d963b128d54f00144d216b2d118.

9a776b895e93926e2a758c09e341accb9333edc1243d216a5e53f47c6043c852

Tags

HIDDEN-COBRAproxyspywaretrojan

Details

Name	9a776b895e93926e2a758c09e341accb9333edc1243d216a5e53f47c6043c852
Size	232960 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	97aaf130cfa251e5207ea74b2558293d
SHA1	c7e7dd96fefca77bb1097aeeefef126d597126bd
SHA256	9a776b895e93926e2a758c09e341accb9333edc1243d216a5e53f47c6043c852
SHA512	d8b750263ac8b295a934ef60a694108257c489055c6aee24bae000d70d0bdde70934e8c2a157d38c15469bc5fb2a6cfcb733ddd4729ba
ssdeep	3072:6U5r72JE+FYWR0jZLShk4cPT/QzSaQ0sCFneZTznIhZJJcrJ1GHeV9:6U5uJpYnZL05STQNddFnAnGZIrV
Entropy	6.524151

Antivirus

Ahnlab	Trojan/Win32.Alreay
Antiy	Trojan[Banker]/Win32.Alreay
BitDefender	Trojan.Generic.22528938
ClamAV	Win.Trojan.Agent-6971031-0
Comodo	Malware
Cyren	W32/Alreay.SQQX-6406
ESET	a variant of Win32/Spy.Banker.ADRO trojan
Emsisoft	Trojan.Generic.22528938 (B)
Ikarus	Trojan-Spy.Agent
K7	Spyware (005198041)
Lavasoft	Trojan.Generic.22528938
McAfee	GenericRXFQ-MX!97AAF130CFA2
Microsoft Security Essentials	Trojan:Win32/Alreay
NANOAV	Trojan.Win32.Alreay.ettzed
NetGate	Trojan.Win32.Malware
Sophos	Troj/Banker-GUU
Symantec	Trojan.Gen.2
TrendMicro	Trojan.79245AFC
TrendMicro House Call	Trojan.79245AFC
VirusBlokAda	TrojanBanker.Alreay
Zillya!	Trojan.Alreay.Win32.42

YARA Rules

```
rule CISA_3P_10301706_02 : HiddenCobra TWOPENCE backdoor dropper proxy spyware trojan
{
  meta:
    Author = "CISA Trusted Third Party"
    Incident = "10301706.r2.v1"
    Date = "2020-08-11"
    Actor = "Hidden Cobra"
    Category = "Backdoor Dropper Proxy Spyware Trojan"
    Family = "TWOPENCE"
    Description = "Detects strings in TWOPENCE proxy tool"
    MD5_1 = "40e698f961eb796728a57ddf81f52b9a"
    SHA256_1 = "a917c1cc198cf36c0f2f6c24652e5c2e94e28d963b128d54f00144d216b2d118"
    MD5_2 = "dfd09e91b7f86a984f8687ed6033af9d"
    SHA256_2 = "aca598e2c619424077ef8043cb4284729045d296ce95414c83ed70985c892c83"
    MD5_3 = "bda82f0d9e2cb7996d2eefdd1e5b41c4"
    SHA256_3 = "f3ca8f15ca582dd486bd78fd57c2f4d7b958163542561606bebd250c827022de"
    MD5_4 = "97aaf130cfa251e5207ea74b2558293d"
    SHA256_4 = "9a776b895e93926e2a758c09e341accb9333edc1243d216a5e53f47c6043c852"
    MD5_5 = "889e320cf66520485e1a0475107d7419"
    SHA256_5 = "8cad61422d032119219f465331308c5a61e21c9a3a431b88e1f8b25129b7e2a1"
  strings:
    $cmd1 = "ssylka"
    $cmd2 = "ustanavlivat"
    $cmd3 = "poluchit"
    $cmd4 = "pereslat"
    $cmd5 = "derzhat"
    $cmd6 = "vykhodit"
    $cmd7 = "Nachalo"
    $cmd8 = "kliyent2podklyuchit"
    $frmt1 = "Host: %s%s%s:%hu"
    $frmt2 = "%s%s%s%s%s%s%s%s%s%s"
  condition:
    (4 of ($cmd*)) and (1 of ($frmt*))
}
```

ssdeep Matches

99 aca598e2c619424077ef8043cb4284729045d296ce95414c83ed70985c892c83

PE Metadata

Compile Date	2017-02-20 06:09:30-05:00
Import Hash	6b8fa355d78d649f199232a25e22d630

PE Sections

MD5	Name	Raw Size	Entropy
bb573973d723ebac15a2dd783a56921f	header	1024	2.372576
e6412e7fb561ead2b3eddef9bafd3518	.text	198656	6.554337
a9890fd54b24cf53425649a92fe290ad	.rdata	18432	5.115959
884e0d48d1830995eeade874d295ced0	.data	5632	3.201975
0e79f25ba5ec9ae1502fe80ec7b08f79	.reloc	9216	5.674607

Packers/Compilers/Cryptors

Microsoft Visual C++ ?.?

Description

This file is a 32-bit Windows executable. It has similar functionality as a917c1cc198cf36c0f2f6c24652e5c2e94e28d963b128d54f00144d216b2d118.

70b494b0a8fdf054926829dcb3235fc7bd0346b6a19faf2a57891c71043b3b38

Tags

HIDDEN-COBRAbackdoorproxytrojan

Details

Name	70b494b0a8fdf054926829dcb3235fc7bd0346b6a19faf2a57891c71043b3b38
Size	1637888 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	3c9e71400b72cc0213c9c3e4ab4df9df
SHA1	bdb632b27ddb200693c1b0b80819a7463d4e7a98
SHA256	70b494b0a8fdf054926829dcb3235fc7bd0346b6a19faf2a57891c71043b3b38
SHA512	c7a02fadb9fbbe0cf05dddd6a78cbf48b9030638420b421b4ff83816ae1cabbe54656b4e1c8e4020cacab93388934b6c79d3d21fe560ed4
ssdeep	24576:5gDgaE2r55ENJSOZ8jsAMZMF2kPupVevS6ieT17cZ/hJMIYO0:+D9vrrs8OZxZl+wvTTahqO
Entropy	7.956784

Antivirus

Ahnlab	Trojan/Win32.Agent
Antiy	Trojan/Win32.AGeneric
Avira	TR/Crypt.TPM.Gen
BitDefender	Gen:Variant.Symmi.79278
Comodo	Malware
ESET	Win32/Spy.Banker.AECT trojan
Emsisoft	Gen:Variant.Symmi.79278 (B)
K7	Trojan (0040f4ef1)
Lavasoft	Gen:Variant.Symmi.79278
McAfee	Generic Trojan.ej
Microsoft Security Essentials	TrojanSpy:Win32/Banker
NANOAV	Trojan.Win32.TPM.etiucd
Quick Heal	Trojan.Generic
Sophos	Troj/Agent-AXNK
Symantec	Trojan.Gen.2
TrendMicro	BKDR_KL.22A80489
TrendMicro House Call	BKDR_KL.22A80489
VirusBlokAda	Backdoor.Agent
Zillya!	Backdoor.Agent.Win32.64626

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2017-02-20 06:09:30-05:00
Import Hash	baa93d47220682c04d92f7797d9224ce

PE Sections

MD5	Name	Raw Size	Entropy
a32e7b28831808e208355ae637e006f0	header	4096	0.814733
ca42a315c5287101ffdf2d7843b74d34		119296	7.972251
d41d8cd98f00b204e9800998ecf8427e	.rsrc	0	0.000000
9e66a842d63673e7febfc6646ea43c43	.idata	512	1.308723
5668c4714f706c7f669afb1e7f9c6ba7		512	0.260771
de90eb0d146d89f2c2dd76ecf17ea09e	dworqjxn	1512960	7.955321
4857cc05e1ea968cfc978d53f2f34126	omrcmqfn	512	3.378388

Description

This file is a 32-bit Windows executable. It has similar functionality as a917c1cc198cf36c0f2f6c24652e5c2e94e28d963b128d54f00144d216b2d118.

8cad61422d032119219f465331308c5a61e21c9a3a431b88e1f8b25129b7e2a1

Tags

HIDDEN-COBRAproxyspywaretrojan

Details

Name	8cad61422d032119219f465331308c5a61e21c9a3a431b88e1f8b25129b7e2a1
Size	480768 bytes
Type	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
MD5	889e320cf66520485e1a0475107d7419
SHA1	f5fc9d893ae99f97e43adcef49801782daced2d7
SHA256	8cad61422d032119219f465331308c5a61e21c9a3a431b88e1f8b25129b7e2a1
SHA512	8da0ab0b3072b3966c5e32c22e7ac5654ff3923b3cf28cc895ae10d520a27bb70360e4d94e54422033aa7c7527d10774ab6d8b8569bab
ssdeep	6144:sdqAqUok+00rm9TOi9Vc7/VtXvWLnJlh+efvoRKmjbL/xY4fTKKWSFle3IDgDi2C:xABogwttXuLnJlkkiKU/xtKYydF9iIU
Entropy	6.465490

Antivirus

Ahnlab	Trojan/Win32.Alreay
Antiy	Trojan/Win32.BTSGeneric
Avira	TR/Spy.Banker.xbkax
BitDefender	Trojan.Generic.20466258
ClamAV	Win.Trojan.Agent-6971031-0
Comodo	Malware
ESET	a variant of Win64/Spy.Banker.AX trojan
Emsisoft	Trojan.Generic.20466258 (B)
Ikarus	Trojan-Spy.Win64.Agent
K7	Spyware (00504e561)
Lavasoft	Trojan.Generic.20466258
McAfee	Trojan-FLEP!889E320CF665
Microsoft Security Essentials	TrojanSpy:Win64/Cyruslish.A
NANOAV	Trojan.Win64.Alreay.elwnmb
Sophos	Troj/Banker-GSY

Symantec	Trojan.Gen.2
TrendMicro	BKDR64_.D1FB2862
TrendMicro House Call	BKDR64_.D1FB2862
VirusBlokAda	TrojanBanker.Alreay
Zillya!	Trojan.Banker.Win64.148

YARA Rules

```
rule CISA_3P_10301706_02 : HiddenCobra TWOPENCE backdoor dropper proxy spyware trojan
{
  meta:
    Author = "CISA Trusted Third Party"
    Incident = "10301706.r2.v1"
    Date = "2020-08-11"
    Actor = "Hidden Cobra"
    Category = "Backdoor Dropper Proxy Spyware Trojan"
    Family = "TWOPENCE"
    Description = "Detects strings in TWOPENCE proxy tool"
    MD5_1 = "40e698f961eb796728a57ddf81f52b9a"
    SHA256_1 = "a917c1cc198cf36c0f2f6c24652e5c2e94e28d963b128d54f00144d216b2d118"
    MD5_2 = "dfd09e91b7f86a984f8687ed6033af9d"
    SHA256_2 = "aca598e2c619424077ef8043cb4284729045d296ce95414c83ed70985c892c83"
    MD5_3 = "bda82f0d9e2cb7996d2eefdd1e5b41c4"
    SHA256_3 = "f3ca8f15ca582dd486bd78fd57c2f4d7b958163542561606bebd250c827022de"
    MD5_4 = "97aaf130cfa251e5207ea74b2558293d"
    SHA256_4 = "9a776b895e93926e2a758c09e341accb9333edc1243d216a5e53f47c6043c852"
    MD5_5 = "889e320cf66520485e1a0475107d7419"
    SHA256_5 = "8cad61422d032119219f465331308c5a61e21c9a3a431b88e1f8b25129b7e2a1"
  strings:
    $cmd1 = "ssylka"
    $cmd2 = "ustanavlivat"
    $cmd3 = "poluchit"
    $cmd4 = "pereslat"
    $cmd5 = "derzhat"
    $cmd6 = "vykhodit"
    $cmd7 = "Nachalo"
    $cmd8 = "kliyent2podklyuchit"
    $frmt1 = "Host: %s%s%s:%hu"
    $frmt2 = "%s%s%s%s%s%s%s%s%s%s"
  condition:
    (4 of ($cmd*)) and (1 of ($frmt*))
}
```

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2016-08-26 00:11:49-04:00
Import Hash	1cd9192feb9402723bdada868b8c98de

PE Sections

MD5	Name	Raw Size	Entropy
2fb3e4c0734998f9629ba86c4e7c6e99	header	1024	2.603055
9319545c7ac53b81b3d56a722dad8ef1	.text	364032	6.423307
e406c9d4f3bdbdbab8191bb701e4ff57	.rdata	81920	6.056842
6198d24ba115f17c5597e2773cb51a75	.data	8704	3.090138
f7b6096db3b9ad55c3bad4c47de6d5b4	.pdata	22016	5.758547

ddf5f86578d6de91c211211bdd72f63f	.reloc	3072	3.181451

Description

This file is a 32-bit Windows executable. It has similar functionality as a917c1cc198cf36c0f2f6c24652e5c2e94e28d963b128d54f00144d216b2d118.

Mitigation

The following Snort rules were provided by a CISA trusted third party:

// The following Snort rule can be used to detect proxy handshake
alert tcp any any -> any any (msg:"Proxy handshake detected"; content:"|a7 00 a7 00 fb 00 b0 00 8e 00 c5 00 b0 00 48 00 17 00 c5 00 8b 00 6a 00 8e 00 ec 00 f3 00 fe 00 d9 00 f3 00 a7 00 6a 00 ec 00 a7 00 b0 00 17 00 fc 00 48 00 48 00 09 00 09 00 09 00 48 00 8e 00 ce|"; rev:1; sid:1;)

// The following Snort rule can be used to detect encrypted proxy string kliyent2podklyuchit
alert tcp any any -> any any (msg:"Proxy string detected"; content:"|d1 14 23 b3 c7 b2 ac fe 70 0d 1c d1 14 b3 d7 f9 38 23 ac|"; rev:1; sid:1;)

// The following Snort rule can be used to detect encrypted proxy string poluchit
alert tcp any any -> any any (msg:"Proxy string detected"; content:"|70 0d 14 d7 f9 38 23 ac|"; rev:1; sid:1;)

// The following Snort rule can be used to detect encrypted proxy string pereslat
alert tcp any any -> any any (msg:"Proxy string detected"; content:"|70 c7 be c7 c9 14 ab ac|"; rev:1; sid:1;)

Recommendations

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

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB 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) Special Publication 800-83, **"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 the following URL: https://www.cisa.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 instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

What is a MAR? A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manual reverse engineering. To request additional analysis, please contact 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 be directed to the CISA at 1-888-282-0870 or CISA Service Desk.

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 phishing-related scams. Reporting forms can be found on CISA's homepage at www.cisa.gov.