

# MAR-10288834-1.v1 – North Korean Remote Access Tool: COPPERHEDGE

 [us-cert.gov/ncas/analysis-reports/ar20-133a](https://us-cert.gov/ncas/analysis-reports/ar20-133a)

## Notification

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

## Summary

### Description

This Malware Analysis Report (MAR) is the result of analytic efforts between the Department of Homeland Security (DHS), the Federal Bureau of the Department of Defense (DoD). Working with U.S. Government partners, DHS, FBI, and DoD identified Remote Access Tool (RAT) malware variant Korean government. This malware variant has been identified as COPPERHEDGE. The U.S. Government refers to malicious cyber activity by the 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 further network exploitation. DHS, FBI, and DoD are distributing this MAR to enable network defense and reduce exposure to North Korean government activity.

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

The Manuscript family of malware is used by advanced persistent threat (APT) cyber actors in the targeting of cryptocurrency exchanges and related is a full-featured Remote Access Tool (RAT) capable of running arbitrary commands, performing system reconnaissance, and exfiltrating data. Six have been identified based on network and code features. The variants are categorized based on common code and a common class structure. A symptom the implants identifying a class name of "WinHTTP\_Protocol" and later "WebPacket".

For a downloadable copy of IOCs, see [MAR-10288834-1.v1.stix](#).

The breakdown for the variants is displayed below:

### Variant A

D8AF45210BF931BC5B03215ED30FB731E067E91F25EDA02A404BD55169E3E3C37985AF0A87780D27DC52C4F73C38DE44E5AD477CB78B2E8E89708168FBC4A882

### Variant B

E98991CDD9DDD30ADF490673C67A4F8241993F26810DA09B52D8748C6160A2924838F85499E3C68415010D4F19E83E2C9E3F2302290138ABE79C380754F97324E76B3FD3E906AC23218B1FBD66FD29C3945EE209A29E9462BBC46B07D1645DE21FAAA939087C3479441D9F9C83A80AC7EC9B929E626CB34A7417BE9FF0316FF73FF4EBAE6C255D4AE6B747A77F2821F2B619825C7789C7EE5338DA5ECB375395C2F150DBE9A8EFB72DC46416CA29ACDBAE6FD4A2AF16B27F153EAABD4772A2A11678327C5F36074CF5F18D1A92C2D9FEA9BFAE6C245EAAD01640FD75AF4D6C11C0EE19D7545F98FCD15725A3D9F0DBD0F35B2091E1C5B9CF4744F16E81A030C59E4BD9676BB3460BE68BA4559A824940A393BDE7613850EDA9196259E453B9F3EEE38C632C62CA95B5C66F8D39A18E23B9175845560AF84B6A2F69B7F9B6EC1CF6E1A146543D2903146698DA5698B2A214201720C0BE756C6E8D2A2F27DCFAFF

### Variant C

37BB27F4EB40B8947E184AFDDBA019001C12F97588E7F596AB6BC07F7C152602E6FC788B5FF7436DA4450191A003966A68E2A1913C83F1D3AEC78C65F3BA85CA284BC471647F951C79E3E333B2B19AA37F84CC39B55441A82E2A5F7319131FAC A1CDB784100906D0AC895297C5A0959AB21A9FB39C687BAF176324EE84095472

### Variant D

B4BF6322C67A23553D5A9AF6FCD9510EB613FFAC963A21E32A9CED83132A09BA

### Variant E

134B082B418129FFA390FBEE1568BD9510C54BFDD0E6B1F36BC7B8F867E56283

### Variant F

0A763DA26A67CB2B09A3AE6E1AC07828065EB980E452CE7D3354347976038E7E1884DDC53EF66488CA8FC641B438895FCAADA77C15210118465377C63223B3BC C24C322F4535DEF3F8D1579C39F2F9E323787D15B96E2EE457C38925EFFE2D39

Submitted Files (22)

0a763da26a67cb2b09a3ae6e1ac07828065eb980e452ce7d3354347976038e7e (171B9135540F89BF727B690B9E587A...)

134b082b418129ffa390fbee1568bd9510c54bfdd0e6b1f36bc7b8f867e56283 (633BD738AE63B6CE9C2A48CBDDDD154...)

1678327c5f36074cf5f18d1a92c2d9fea9bfae6c245eaad01640fd75af4d6c11 (86D3C1B354CE696E454C42D8DC6DF1...)

1884ddc53ef66488ca8fc641b438895fcaada77c15210118465377c63223b3bc (22F8D2A0C8D9B54A553FCA1B2393B2...)  
1faaa939087c3479441d9f9c83a80ac7ec9b929e626cb34a7417be9ff0316ff7 (667CF9E8EC1DAC7812F92BD77AF702...)  
284bc471647f951c79e3e333b2b19aa37f84cc39b55441a82e2a5f7319131fac (DB590EA77A92AE6435E2EC954D065E...)  
37bb27f4eb40b8947e184afddb019001c12f97588e7f596ab6bc077fc152602 (A8B6EC51ED88C0329FD3329CB615BB...)  
3ff4ebae6c255d4ae6b747a77f2821f2b619825c7789c7ee5338da5ecb375395 (A7C804B62AE93D708478949F498342...)  
4838f85499e3c68415010d4f19e83e2c9e3f2302290138abe79c380754f97324 (EB6275A24D047E3BE05C2B4E5F5070...)  
7985af0a87780d27dc52c4f73c38de44e5ad477cb78b2e8e89708168fbc4a882 (C6801F90AAA11CE81C9B66450E0029...)  
9e4bd9676bb3460be68ba4559a824940a393bde7613850eda9196259e453b9f3 (668D5B5761755C9D061DA74CB21A8B...)  
a1cdb784100906d0ac895297c5a0959ab21a9fb39c687baf176324ee84095472 (0856655351ACFFA1EE459EEEF1647...)  
b4bf6322c67a23553d5a9af6fcd9510eb613ffac963a21e32a9ced83132a09ba (34C2AC6DAA44116713F882694B6B41...)  
c0ee19d7545f98fcd15725a3d9f0dbd0f35b2091e1c5b9cf4744f16e81a030c5 (5182E7A2037717F2F9BBF6BA298C48...)  
c24c322f4535def3f8d1579c39f2f9e323787d15b96e2ee457c38925effe2d39 (FDD55A38A45DE8AF6F8C34A33BAE11...)  
c2f150dbe9a8efb72dc46416ca29acdcae6fd4a2af16b27f153eaabd4772a2a1 (86685EC8C3C717AA2A9702E2C9DEC3...)  
d8af45210bf931bc5b03215ed30fb731e067e91f25eda02a404bd55169e3e3c3 (12C786C490366727CF7279FC141921...)  
e6fc788b5ff7436da4450191a003966a68e2a1913c83f1d3aec78c65f3ba85ca (117FA0B8B8B965680C7B630C6E2BF0...)  
e76b3fd3e906ac23218b1fbd66fd29c3945ee209a29e9462bbc46b07d1645de2 (AA7F506B0C30D76557C82DBA45116C...)  
e98991cdd9dd30adf490673c67a4f8241993f26810da09b52d8748c6160a292 (912F87392A889070DBB1097A82CCD9...)  
eee38c632c62ca95b5c66f8d39a18e23b9175845560af84b6a2f69b7f9b6ec1c (35E38D023B253C0CD9BD3E16AFC362...)  
f6e1a146543d2903146698da5698b2a214201720c0be756c6e8d2a2f27dcfaff (72FE869AA394EF0A62BB8324857770...)

Domains (42)

028xmz.com

168wangpi.com

33cow.com

3x-tv.com

51shousheng.com

530hr.com

919xy.com

92myhw.com

97nb.net

aedlifepower.com

aisou123.com

aloe-china.com

anlway.com

ap8898.com

apshenyihl.com

as-brant.ru

aurumgroup.co.id

bogorcenter.com

cabba-cacao.com

castorbyg.dk

creativefishstudio.com

danagloverinteriors.com

duratransgroup.com  
 eventum.cwsdev3.biz  
 eygingenieros.com  
 growthincone.com  
 inverstingpurpose.com  
 locphuland.com  
 markcoprintandcopy.com  
 marmarademo.com  
 matthias-dlugi.de  
 new.titanik.fr  
 nuokejs.com  
 pakteb.com  
 qdbazaar.com  
 rhythm86.com  
 rxrenew.us  
 sensationalsecrets.com  
 stokeinvestor.com  
 streamf.ru  
 theinspectionconsultant.com  
 vinhsake.com

## Findings

**d8af45210bf931bc5b03215ed30fb731e067e91f25eda02a404bd55169e3e3c3**

Tags

backdoortrojan

Details

<b>Name</b>	12C786C490366727CF7279FC141921D8
<b>Size</b>	166400 bytes
<b>Type</b>	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
<b>MD5</b>	12c786c490366727cf7279fc141921d8
<b>SHA1</b>	a2e966edee45b30bb6bb5c978e55833eec169098
<b>SHA256</b>	d8af45210bf931bc5b03215ed30fb731e067e91f25eda02a404bd55169e3e3c3
<b>SHA512</b>	3abe4cd0d287fdf38715feac4096a16ed8c9ed113897e8e8e26d22adb4346df3c8a14a2c6660fbc2e01beb98e5cc770616866e5e319cfd
<b>ssdeep</b>	3072:G2K5QbCpgMFIQ0O4t5E13j0S0wBiCRcnHaApUiCDyY:G2bSQ0NS3jq6Apm
<b>Entropy</b>	6.529499

Antivirus

<b>Ahnlab</b>	Trojan/Win32.Manuscript
<b>Antiy</b>	Trojan/Win32.Manuscript
<b>Avira</b>	TR/AD.APTLazerus.gqbgj
<b>BitDefender</b>	Gen:Variant.Grafter.452205
<b>ClamAV</b>	Win.Trojan.Agent-6459669-0
<b>Cyren</b>	W32/Nukesped.EBPS-8656

<b>ESET</b>	a variant of Win32/NukeSped.AG trojan
<b>Emsisoft</b>	Gen:Variant.Graftor.452205 (B)
<b>Ikarus</b>	Trojan-Spy.Agent
<b>K7</b>	Trojan ( 005202c91 )
<b>McAfee</b>	HiddenCobra!12C786C49036
<b>Microsoft Security Essentials</b>	Trojan:Win32/Autophyte.M!dha
<b>NANOAV</b>	Trojan.Win32.Manuscript.eyeld
<b>NetGate</b>	Trojan.Win32.Malware
<b>Sophos</b>	Troj/Agent-AYKU
<b>Symantec</b>	Backdoor.Cruprox
<b>Systweak</b>	malware.gen-ra
<b>TrendMicro</b>	TROJ_NUKESPED.B
<b>TrendMicro House Call</b>	TROJ_NUKESPED.B
<b>Vir.IT eXplorer</b>	Trojan.Win32.Genus.BGU
<b>VirusBlokAda</b>	BScope.Trojan.Manuscript
<b>Zillya!</b>	Trojan.Manuscript.Win32.10

#### YARA Rules

- rule CISA\_3P\_10135536\_24 : success\_fail\_codes
 {
 meta:
 Author = "CISA Trusted Third Party"
 Incident = "10135536-A"
 Date = "2017-11-14"
 Actor = "Hidden Cobra"
 Category = "n/a"
 Family = "FALLCHILL"
 Description = ""
 strings:
 \$s0 = { 68 7a 34 12 00 }
 \$s1 = { ba 7a 34 12 00 }
 \$f0 = { 68 5c 34 12 00 }
 \$f1 = { ba 5c 34 12 00 }
 condition:
 (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and ((\$s0 and \$f0) or (\$s1 and \$f1))
 }
- rule CISA\_3P\_10135536\_24 : success\_fail\_codes
 {
 meta:
 Author = "CISA Trusted Third Party"
 Incident = "10135536-A"
 Date = "2017-11-14"
 Actor = "Hidden Cobra"
 Category = "n/a"
 Family = "FALLCHILL"
 Description = ""
 strings:
 \$s0 = { 68 7a 34 12 00 }
 \$s1 = { ba 7a 34 12 00 }
 \$f0 = { 68 5c 34 12 00 }
 \$f1 = { ba 5c 34 12 00 }
 condition:
 (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and ((\$s0 and \$f0) or (\$s1 and \$f1))
 }

ssdeep Matches

No matches found.

PE Metadata

**Compile Date** 2018-02-24 01:52:42-05:00

**Import Hash** 04f1d2f5c7c06a209c29beeff2fce817

PE Sections

MD5	Name	Raw Size	Entropy
c37a64a60af18ec7b8360e84d5b85d0d	header	1024	2.917803
3056f69baa8301ae1f6aef85bf88d0b8	.text	121344	6.526051
3c4cc09c827a1bb000669e8922d7d6d9	.rdata	29184	5.443973
4cda142760a96a9e47daeafc0ea5ed7c	.data	5120	5.302725
8b7fa4533b5f57eebfd85a72154aeafe	.gfids	512	2.058608
f040daaf746c66507cba208212c65d00	.rsrc	2560	2.715102
0d82adf85bb2476ed8bd2bb6c297e301	.reloc	6656	6.477462

Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

Relationships

```
d8af45210b... Connected_To 530hr.com
d8af45210b... Connected_To 028xmz.com
d8af45210b... Connected_To 168wangpi.com
```

Description

This file is a 32-bit Dynamic Link Library (DLL) and has been identified as Variant A. Variant A uses RC4 encryption to obfuscate import loading w "0x78292E4C5DA3B5D067F081B736E5D593". A hard-coded string of "\*dJU!\*JE&!M@UNQ@" is embedded in the malware beacons. This varia Hypertext Transfer Protocol (HTTP) header strings using a custom character manipulation where the certain ranges of characters are modified by subtracting a constant value 9.

Variant A will generate HTTP POST requests with the following format:

```
--Begin HTTP POST request--
POST /<uri> HTTP/1.1
Connection: keep-alive
Cache-Control: max-age=0
Accept: /*/*
Content-Type: multipart/form-data; boundary=----FormBoundary<randomCharacters>
Accept-Encoding: gzip,deflate,sdch
Accept-Language: ko-KR
User-Agent: <obtained from ObtainUserAgentString otherwise: Mozilla/5.0 (Windows NT 6.1; WOW64) Chrome/28.0.1500.95 Safari/537.36>
Host: <domain>
Content-Length: <length>

-----FormBoundary<randomCharacters>
Content-Disposition: form-data; name="board_id"
<sessionID>
-----FormBoundary<randomCharacters>
Content-Disposition: form-data; name="user_id"
<*dJU!*JE&!M@UNQ@ if beacon request otherwise empty>
-----FormBoundary<randomCharacters>
Content-Disposition: form-data; name="file1"; filename="<randomly picked>"
Content-Type: application/octet-stream
<datagram>
--End HTTP POST request--
```

Variant A uses a custom algorithm to encrypt data from datagrams. An implementation of the algorithm is provided below:

```
--Begin custom algorithm--
modVal = 0x6be
addVal = 0x95d9
keyVal = 0x25
def encrypt(data):
    global keyVal
    r = ""
    for c in data:
        r += chr((ord(c) ^ keyVal) & 0xff)
        keyVal = (((ord(c) + keyVal) % modVal) + addVal) & 0xffffffff
```

return r  
--End custom algorithm--  
Screenshots

Ordinal	Description
0x123459	Replv 0x12345C
0x12345A	Reply 0x12347A
0x12345B	GetConfig
0x12345F	Reply with 'not'
0x123460	GetFile
0x123461	DrivesInfo
0x123462	DeleteFile
0x123465	FindFile
0x123467	OverwriteNullDeleteOnReboot
0x123469	DeleteFileOnReboot
0x12346B	CreateProcess
0x12346C	ZipGetFile
0x12346D	RunCommandLine
0x123470	DirectoryList
0x123471	ZipFile
0x123472	SecureDeleteFile
0x123473	ProcessList
0x123474	ProcessKill
0x123475	Uninstall
0x123478	SetConfig
0x12347C	Disconnect
0x12347E	SystemInfo
0x123480	LoadDll
0x123486	PutFile
0x123488	TestConnect
0x123489	Timestomp
0x12348A	CreateProcessAsUser

Figure 1 - Variant A contains the commands displayed in the table.

### 530hr.com

Tags

command-and-control

URLs

530hr.com/data/common.php

Relationships

530hr.com Connected\_From d8af45210bf931bc5b03215ed30fb731e067e91f25eda02a404bd55169e3e3c3

530hr.com Connected\_From 7985af0a87780d27dc52c4f73c38de44e5ad477cb78b2e8e89708168fbc4a882

Description

12C786C490366727CF7279FC141921D8 and C6801F90AAA11CE81C9B66450E002972 attempt to connect to the domain.

### 028xmz.com

Tags

command-and-control

URLs

028xmz.com/include/common.php

Relationships

028xmz.com Connected\_From d8af45210bf931bc5b03215ed30fb731e067e91f25eda02a404bd55169e3e3c3

028xmz.com Connected\_From 7985af0a87780d27dc52c4f73c38de44e5ad477cb78b2e8e89708168fbc4a882

Description

12C786C490366727CF7279FC141921D8 and C6801F90AAA11CE81C9B66450E002972 attempt to connect to the domain.

### 168wangpi.com

Tags

command-and-control

#### URLs

168wangpi.com/include/charset.php

#### Relationships

168wangpi.com Connected\_From d8af45210bf931bc5b03215ed30fb731e067e91f25eda02a404bd55169e3e3c3

168wangpi.com Connected\_From 7985af0a87780d27dc52c4f73c38de44e5ad477cb78b2e8e89708168fbc4a882

#### Description

12C786C490366727CF7279FC141921D8 and C6801F90AAA11CE81C9B66450E002972 attempt to connect to the domain.

**7985af0a87780d27dc52c4f73c38de44e5ad477cb78b2e8e89708168fbc4a882**

#### Tags

backdoorbottrojan

#### Details

<b>Name</b>	C6801F90AAA11CE81C9B66450E002972
<b>Size</b>	176640 bytes
<b>Type</b>	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
<b>MD5</b>	c6801f90aaa11ce81c9b66450e002972
<b>SHA1</b>	4e30ebb98bb9f984c05eb0c0a365ff95305e8c55
<b>SHA256</b>	7985af0a87780d27dc52c4f73c38de44e5ad477cb78b2e8e89708168fbc4a882
<b>SHA512</b>	2568ed6468f6d6b4ec6a930e003b04a2fd9e3379ac9fa320f6130f789ff8471ef2ca596ef2699bc45fd0997a5972243627199eb94e42028
<b>ssdeep</b>	3072:FhjE3GVSDW52icOf+CDqRHiEGK+M/0ivZSRMlxs6D79vrXqx7C5:DE3o52Q+VRHiEGK+M/1hSmZ67
<b>Entropy</b>	6.244198

#### Antivirus

<b>Ahnlab</b>	Trojan/Win32.Manuscript
<b>Antiy</b>	Trojan/Win32.Manuscript
<b>Avira</b>	TR/Autophyte.fadtc
<b>BitDefender</b>	Trojan.GenericKD.40166196
<b>ESET</b>	a variant of Win64/NukeSped.AL trojan
<b>Emsisoft</b>	Trojan.GenericKD.40166196 (B)
<b>Ikarus</b>	Trojan-Spy.Agent
<b>K7</b>	Riskware ( 0040eff71 )
<b>McAfee</b>	HiddenCobra!C6801F90AAA1
<b>Microsoft Security Essentials</b>	Trojan:Win32/Autophyte.Mldha
<b>NANOAV</b>	Trojan.Win64.Manuscript.eyolaj
<b>NetGate</b>	Trojan.Win32.Malware
<b>Sophos</b>	Troj/Agent-AYKV
<b>Symantec</b>	Backdoor.Cruprox
<b>Systweak</b>	trojan-backdoor.bot
<b>TrendMicro</b>	TROJ64_.8C3165BD
<b>TrendMicro House Call</b>	TROJ64_.8C3165BD
<b>Vir.IT eXplorer</b>	Trojan.Win32.Genus.BGU
<b>VirusBlokAda</b>	Trojan.Manuscript
<b>Zillya!</b>	Trojan.NukeSped.Win64.13

YARA Rules

- rule CISA\_3P\_10135536\_24 : success\_fail\_codes  
{  
  meta:  
    Author = "CISA Trusted Third Party"  
    Incident = "10135536-A"  
    Date = "2017-11-14"  
    Actor = "Hidden Cobra"  
    Category = "n/a"  
    Family = "FALLCHILL"  
    Description = ""  
  strings:  
    \$s0 = { 68 7a 34 12 00 }  
    \$s1 = { ba 7a 34 12 00 }  
    \$f0 = { 68 5c 34 12 00 }  
    \$f1 = { ba 5c 34 12 00 }  
  condition:  
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and ((\$s0 and \$f0) or (\$s1 and \$f1))  
}
- rule CISA\_3P\_10135536\_24 : success\_fail\_codes  
{  
  meta:  
    Author = "CISA Trusted Third Party"  
    Incident = "10135536-A"  
    Date = "2017-11-14"  
    Actor = "Hidden Cobra"  
    Category = "n/a"  
    Family = "FALLCHILL"  
    Description = ""  
  strings:  
    \$s0 = { 68 7a 34 12 00 }  
    \$s1 = { ba 7a 34 12 00 }  
    \$f0 = { 68 5c 34 12 00 }  
    \$f1 = { ba 5c 34 12 00 }  
  condition:  
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and ((\$s0 and \$f0) or (\$s1 and \$f1))  
}

ssdeep Matches

No matches found.

PE Metadata

**Compile Date** 2018-02-24 01:52:37-05:00  
**Import Hash** a789d7d213a81de1ef22719353b5a15a

PE Sections

MD5	Name	Raw Size	Entropy
5869d6b6233e336c6aad801596ad0467	header	1024	3.153109
33470b7e064ef6a3d0da14b6ce12cf0f	.text	111104	6.424442
39564530ada80c0adb6a0d5b0c53cb96	.rdata	46592	5.184555
bbf22987d7c4bfec2c3fdf371454d2b6	.data	6144	4.989277
74b4e027ae891b3728ab6efa84bd2614	.pdata	6656	5.232089
346bac74e00a330d731022626b43a9c3	.gfids	512	1.773634
9f5bcd42d44606048eb3e04477c78ac7	.rsrc	2560	2.714498
a8898561836ddcc26054cd0933d39599	.reloc	2048	4.853460

Relationships

- 7985af0a87... Connected\_To 530hr.com
- 7985af0a87... Connected\_To 028xmz.com
- 7985af0a87... Connected\_To 168wangpi.com

Description



This file is a 64-bit DLL and has been identified as Variant A. Refer to 12C786C490366727CF7279FC141921D8 for analysis.

**e98991cdd9ddd30adf490673c67a4f8241993f26810da09b52d8748c6160a292**

Tags

backdoortrojan

Details

<b>Name</b>	912F87392A889070DBB1097A82CCD93F
<b>Size</b>	128512 bytes
<b>Type</b>	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
<b>MD5</b>	912f87392a889070dbb1097a82ccd93f
<b>SHA1</b>	58c5b86691dc922945c8204b465e76fc15c498fb
<b>SHA256</b>	e98991cdd9ddd30adf490673c67a4f8241993f26810da09b52d8748c6160a292
<b>SHA512</b>	968d7ff1a39b95428d139d0c7febd76ebcd37612c133ac238fb2a2accf853a2ceb5827f2344c09dafcd7e5936ddbc4da401bcb328d4831!
<b>ssdeep</b>	1536:Jg6dIYHXVp0AMkysbkQfRkChJITToZdRYKgZXTrP5Dr4vDQeAsWq8McdLEA8CHR:FdnXVplsXRjITToNYKgZjiDwLEA8CH
<b>Entropy</b>	6.559526

Antivirus

<b>Ahnlab</b>	Trojan/Win32.Lumal
<b>Avira</b>	TR/AD.APTLazerus.yvywt
<b>BitDefender</b>	Trojan.GenericKD.30910621
<b>ClamAV</b>	Win.Trojan.Autophyte-6582725-0
<b>ESET</b>	Win32/NukeSped.El trojan
<b>Emsisoft</b>	Trojan.GenericKD.30910621 (B)
<b>Ikarus</b>	Trojan.Win32.Autophyte
<b>Microsoft Security Essentials</b>	Trojan:Win32/Autophyte.F!dha
<b>NANOAV</b>	Trojan.Win32.Manuscript.fdnkqz
<b>NetGate</b>	Trojan.Win32.Malware
<b>Quick Heal</b>	Trojan.Manuscript
<b>Sophos</b>	Troj/Mdrop-IEI
<b>Symantec</b>	Trojan Horse
<b>Systweak</b>	malware.gen-ra
<b>TrendMicro</b>	BKDR_NU.91A5ED8F
<b>TrendMicro House Call</b>	BKDR_NU.91A5ED8F
<b>Vir.IT eXplorer</b>	Backdoor.Win32.NukeSped.S
<b>VirusBlokAda</b>	BScope.Trojan.Manuscript
<b>Zillya!</b>	Trojan.Manuscript.Win32.15

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

<b>Compile Date</b>	2018-05-30 23:29:44-04:00
<b>Import Hash</b>	95dff862e0b00db0b05bcf957ad9e12e

PE Sections

MD5	Name	Raw Size	Entropy
f72cbf29269ccff8e8ad284f34fbc0b1	header	1024	2.894160
50ec6e3135350d312c343fb6f8663146	.text	89600	6.597021
f276082813b38691ceeb9a5d6cc631b3	.rdata	28160	5.353008
d8727a0a5051d7418591aae3a42a3f01	.data	3072	4.460652
7d67fff10fcba2d1075511a8598e6906	.gfids	512	1.761800
89b7e19270b2a5563c301b84b28e423f	.rsrc	512	4.714485
14cf8bfde5b679909af8942ae7ca3ca6	.reloc	5632	6.597866

Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

Relationships

e98991cdd9...	Connected_To	marmarademo.com
e98991cdd9...	Connected_To	33cow.com
e98991cdd9...	Connected_To	97nb.net

Description

This file is a 32-bit DLL and has been identified as Variant B. Variant B generates an HTTP POST request similar to Variant A. However, in Variant B encrypted. The implant maintains separate RC4 key streams for each side of the conversation. The RC4 key used is "0x271A16AB6D7A900EF3f RC4 key streams will reset after the implant receives a "SystemInfo" command. Variant B performs the same RC4 key as variant A for Application (API) obfuscation.

Screenshots

Ordinal	Description
0x1827	SystemInfo
0x1828	DrivesInfo
0x1829	SetConfig
0x182A	GetConfig
0x182B	KeepAlive
0x182C	PutFile
0x182D	GetFile
0x182E	CreateProcess
0x182F	RunCommandLine
0x1830	ZipGetFile
0x1831	ProcessList
0x1832	ProcessKill
0x1833	Hibernate
0x1834	Disconnect
0x1835	TestConnect

Figure 2 - Variant B contains the commands displayed in the table.

marmarademo.com

Tags

command-and-control

URLs

marmarademo.com/include/extend.php

Relationships

marmarademo.com Connected\_From e98991cdd9ddd30adf490673c67a4f8241993f26810da09b52d8748c6160a292

Description

912F87392A889070DBB1097A82CCD93F attempts to connect to the domain.

**33cow.com**

Tags

command-and-control

URLs

33cow.com/include/control.php

Relationships

33cow.com Connected\_From e98991cdd9ddd30adf490673c67a4f8241993f26810da09b52d8748c6160a292

Description

912F87392A889070DBB1097A82CCD93F attempts to connect to the domain.

**97nb.net**

Tags

command-and-control

URLs

97nb.net/include/arc.sglstview.php

Relationships

97nb.net Connected\_From e98991cdd9ddd30adf490673c67a4f8241993f26810da09b52d8748c6160a292

Description

912F87392A889070DBB1097A82CCD93F attempts to connect to the domain.

**4838f85499e3c68415010d4f19e83e2c9e3f2302290138abe79c380754f97324**

Tags

backdoortrojan

Details

<b>Name</b>	EB6275A24D047E3BE05C2B4E5F50703D
<b>Size</b>	128512 bytes
<b>Type</b>	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
<b>MD5</b>	eb6275a24d047e3be05c2b4e5f50703d
<b>SHA1</b>	62faf15eddb64dce9a2b1ba242254271facffd9f
<b>SHA256</b>	4838f85499e3c68415010d4f19e83e2c9e3f2302290138abe79c380754f97324
<b>SHA512</b>	f2715f867a1729d3ff77a5ee561da0df0f736517d0f0197e726e2a5867d21c16f0558afd8e6b38d9a166d0715b51d95407943865e577fb0
<b>ssdeep</b>	3072:wlv9TmP7TvnhplTznm4qg5aHDwU+A8Yr:ljV9ap7TPPlmbay8Y
<b>Entropy</b>	6.561793

Antivirus

<b>Ahnlab</b>	Trojan/Win32.Lumal
<b>Antiy</b>	Trojan/Win32.TSGeneric
<b>Avira</b>	TR/AD.LazerusAPT.bowts
<b>BitDefender</b>	Trojan.GenericKD.40293468
<b>ClamAV</b>	Win.Trojan.Autophyte-6582725-0
<b>ESET</b>	Win32/NukeSped.EN trojan
<b>Emsisoft</b>	Trojan.GenericKD.40293468 (B)

<b>Ikarus</b>	Trojan.Win32.Autophyte
<b>K7</b>	Riskware ( 0040eff71 )
<b>McAfee</b>	Generic BackDoor.gx
<b>Microsoft Security Essentials</b>	Trojan:Win32/Autophyte.F!dha
<b>NANOAV</b>	Trojan.Win32.Manuscript.fekufg
<b>Sophos</b>	Troj/Bdoor-BHF
<b>Symantec</b>	Trojan.Gen.6
<b>TrendMicro</b>	BKDR_NUKESPED.H
<b>TrendMicro House Call</b>	BKDR_NUKESPED.H
<b>Vir.IT eXplorer</b>	Backdoor.Win32.NukeSped.S
<b>VirusBlokAda</b>	BScope.Trojan.Manuscript
<b>Zillya!</b>	Trojan.Manuscript.Win32.14

#### YARA Rules

No matches found.

#### ssdeep Matches

No matches found.

#### PE Metadata

**Compile Date** 2018-06-03 21:31:48-04:00

**Import Hash** 95dff862e0b00db0b05bcf957ad9e12e

#### PE Sections

MD5	Name	Raw Size	Entropy
588b2a99aa2dbacf19c05e5e363a0056	header	1024	2.899780
0726d6e7fdcc41dca2a7fd81df61e0a5	.text	89600	6.597775
c81a53a721abdd9f27386c7590d39c8b	.rdata	28160	5.358969
d8727a0a5051d7418591aae3a42a3f01	.data	3072	4.460652
7fd4f016c8992181e34904887d12f90f	.gfids	512	1.785783
89b7e19270b2a5563c301b84b28e423f	.rsrc	512	4.714485
13444aa676e19fb0c746d2cd954477d5	.reloc	5632	6.600614

#### Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

#### Relationships

4838f85499... Connected\_To anlway.com

4838f85499... Connected\_To apshenyihl.com

4838f85499... Connected\_To ap8898.com

#### Description

This file is a 32-bit DLL and has been identified as Variant B. Refer to 912F87392A889070DBB1097A82CCD93F for analysis.

#### anlway.com

#### Tags

command-and-control

#### URLs

anlway.com/include/arc.search.class.php

Relationships

anlway.com Connected\_From 4838f85499e3c68415010d4f19e83e2c9e3f2302290138abe79c380754f97324

Description

EB6275A24D047E3BE05C2B4E5F50703D attempts to connect to the domain.

**apshenyihl.com**

Tags

command-and-control

URLs

apshenyihl.com/include/arc.speclist.class.php

Relationships

apshenyihl.com Connected\_From 4838f85499e3c68415010d4f19e83e2c9e3f2302290138abe79c380754f97324

Description

EB6275A24D047E3BE05C2B4E5F50703D attempts to connect to the domain.

**ap8898.com**

Tags

command-and-control

URLs

ap8898.com/include/arc.search.class.php

Relationships

ap8898.com Connected\_From 4838f85499e3c68415010d4f19e83e2c9e3f2302290138abe79c380754f97324

Description

EB6275A24D047E3BE05C2B4E5F50703D attempts to connect to the domain.

**e76b3fd3e906ac23218b1fbd66fd29c3945ee209a29e9462bbc46b07d1645de2**

Tags

backdoorbottrojan

Details

<b>Name</b>	AA7F506B0C30D76557C82DBA45116CCC
<b>Size</b>	128512 bytes
<b>Type</b>	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
<b>MD5</b>	aa7f506b0c30d76557c82dba45116ccc
<b>SHA1</b>	b12d174088629f4e3e0009661ca589fc9f17f66a
<b>SHA256</b>	e76b3fd3e906ac23218b1fbd66fd29c3945ee209a29e9462bbc46b07d1645de2
<b>SHA512</b>	38e119207cf99b6b51f41f79f05a9796b5db68c96243596f25287a82454fc31fc7398fee78940308f2a141907e736f52c4a95efbd00c3d95
<b>ssdeep</b>	3072:MIlnlpLjPVxPITDYll6gJow9DwUkA8pED8:hmnlpLjNjql7KR8qD
<b>Entropy</b>	6.562090

Antivirus

<b>Ahnlab</b>	Trojan/Win32.Lumal
<b>Antiy</b>	Trojan/Win32.Manuscript
<b>Avira</b>	TR/AD.LazerusAPT.kgbeu
<b>BitDefender</b>	Trojan.GenericKD.31008542
<b>ClamAV</b>	Win.Trojan.Autophyte-6582725-0
<b>ESET</b>	a variant of Win32/NukeSped.EN trojan

<b>Emsisoft</b>	Trojan.GenericKD.31008542 (B)
<b>Ikarus</b>	Trojan.Win32.Autophyte
<b>K7</b>	Riskware ( 0040eff71 )
<b>McAfee</b>	RDN/Generic.diz
<b>Microsoft Security Essentials</b>	Trojan:Win32/Autophyte.F!dha
<b>NANOAV</b>	Trojan.Win32.Manuscript.femlit
<b>NetGate</b>	Trojan.Win32.Malware
<b>Symantec</b>	Trojan.Gen.2
<b>Systweak</b>	trojan-backdoor.bot
<b>TrendMicro</b>	Backdoo.C7D30B55
<b>TrendMicro House Call</b>	Backdoo.C7D30B55
<b>VirusBlokAda</b>	BScope.Trojan.Manuscript
<b>Zillya!</b>	Trojan.Manuscript.Win32.13

#### YARA Rules

No matches found.

#### ssdeep Matches

No matches found.

#### PE Metadata

**Compile Date** 2018-06-17 21:16:04-04:00

**Import Hash** 95dff862e0b00db0b05bcf957ad9e12e

#### PE Sections

MD5	Name	Raw Size	Entropy
345f78e492d087ea0094b7b1a6f47748	header	1024	2.895517
4a636a6ed82a4e4197590534c75a6594	.text	89600	6.598985
e212140f652f7d7ff7d1656d4a9760b7	.rdata	28160	5.356656
d8727a0a5051d7418591aae3a42a3f01	.data	3072	4.460652
4a3c3b184454a27b36332e5a5d8d221c	.gfids	512	1.769477
89b7e19270b2a5563c301b84b28e423f	.rsrc	512	4.714485
bec045baa0e06b05d5e27a3ce159e66b	.reloc	5632	6.591434

#### Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

#### Relationships

e76b3fd3e9... Connected\_To aloe-china.com

e76b3fd3e9... Connected\_To 92myhw.com

e76b3fd3e9... Connected\_To aisou123.com

#### Description

This file is a 32-bit DLL and has been identified as Variant B. Refer to 912F87392A889070DBB1097A82CCD93F for analysis.

#### aloe-china.com

#### Tags

command-and-control

URLs

aloe-china.com/include/bottom.php

Relationships

aloe-china.com Connected\_From e76b3fd3e906ac23218b1fbd66fd29c3945ee209a29e9462bbc46b07d1645de2

Description

AA7F506B0C30D76557C82DBA45116CCC attempts to connect to the domain.

**92myhw.com**

Tags

command-and-control

URLs

92myhw.com/include/inc/inc\_common.php

Relationships

92myhw.com Connected\_From e76b3fd3e906ac23218b1fbd66fd29c3945ee209a29e9462bbc46b07d1645de2

Description

AA7F506B0C30D76557C82DBA45116CCC attempts to connect to the domain.

**aisou123.com**

Tags

command-and-control

URLs

aisou123.com/include/dialog/common.php

Relationships

aisou123.com Connected\_From e76b3fd3e906ac23218b1fbd66fd29c3945ee209a29e9462bbc46b07d1645de2

Description

AA7F506B0C30D76557C82DBA45116CCC attempts to connect to the domain.

**1faaa939087c3479441d9f9c83a80ac7ec9b929e626cb34a7417be9ff0316ff7**

Tags

backdoortrojan

Details

<b>Name</b>	667CF9E8EC1DAC7812F92BD77AF702A1
<b>Size</b>	128512 bytes
<b>Type</b>	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
<b>MD5</b>	667cf9e8ec1dac7812f92bd77af702a1
<b>SHA1</b>	880fb67893d8ce559857ca783a701b5ca675eb40
<b>SHA256</b>	1faaa939087c3479441d9f9c83a80ac7ec9b929e626cb34a7417be9ff0316ff7
<b>SHA512</b>	83551fc0a12546380e0975f02fb2aff65ceab76885e9a1d47d7726b2e48d0c8cb0871c2036778c9beaa6d9ad455501941eff51db00bec
<b>ssdeep</b>	3072:tljV94Vp7TTPnhalTDY2l6gJ66dDwUGA8Qr:qjV9mp7TvQq27Kf8Q
<b>Entropy</b>	6.561257

Antivirus

<b>Ahnlab</b>	Trojan/Win32.Lumal
<b>Antiy</b>	Trojan/Win32.TSGeneric
<b>Avira</b>	TR/AD.LazerusAPT.nbtos
<b>BitDefender</b>	Trojan.GenericKD.40344666

<b>ClamAV</b>	Win.Trojan.Autophyte-6582725-0
<b>ESET</b>	a variant of Win32/NukeSped.EN trojan
<b>Emsisoft</b>	Trojan.GenericKD.40344666 (B)
<b>Ikarus</b>	Trojan.Win32.NukeSped
<b>K7</b>	Riskware ( 0040eff71 )
<b>McAfee</b>	Generic Trojan.fk
<b>Microsoft Security Essentials</b>	Trojan:Win32/Autophyte.F!dha
<b>NANOAV</b>	Trojan.Win32.Manuscript.fekufg
<b>NetGate</b>	Trojan.Win32.Malware
<b>Symantec</b>	Trojan.Gen.2
<b>TACHYON</b>	Trojan/W32.Backdoor.128512
<b>TrendMicro</b>	BKDR_NU.28D976A2
<b>TrendMicro House Call</b>	BKDR_NU.28D976A2
<b>Vir.IT eXplorer</b>	Backdoor.Win32.NukeSped.S
<b>VirusBlokAda</b>	BScope.Trojan.Manuscript
<b>Zillya!</b>	Trojan.GenericKD.Win32.143947

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

**Compile Date** 2018-07-23 20:17:47-04:00

**Import Hash** 95dff862e0b00db0b05bcf957ad9e12e

PE Sections

MD5	Name	Raw Size	Entropy
30089c82e2388a4d7f83605bcd432c1e	header	1024	2.897568
21c783005e4e290d2d7e225fd0a17cbf	.text	89600	6.598159
1e3e3c4c6bee90a10fc476303ce8b1ae	.rdata	28160	5.354056
d8727a0a5051d7418591aae3a42a3f01	.data	3072	4.460652
7fd4f016c8992181e34904887d12f90f	.gfids	512	1.785783
89b7e19270b2a5563c301b84b28e423f	.rsrc	512	4.714485
6eb49c61e08a4c2613747f6b09b79fcb	.reloc	5632	6.606865

Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

Relationships

1faaa93908... Connected\_To markcoprintandcopy.com

1faaa93908... Connected\_To aedlifepower.com

1faaa93908... Connected\_To 919xy.com

Description

This file is a 32-bit DLL and has been identified as Variant B. Refer to 912F87392A889070DBB1097A82CCD93F for analysis.



## markcoprintandcopy.com

### URLs

markcoprintandcopy.com/data/helper.php

### Relationships

markcoprintandcopy.com Connected\_From 1faaa939087c3479441d9f9c83a80ac7ec9b929e626cb34a7417be9ff0316ff7

### Description

667CF9E8EC1DAC7812F92BD77AF702A1 attempts to connect to the domain.

## aedlifepower.com

### Tags

command-and-control

### URLs

aedlifepower.com/include/image.php

### Relationships

aedlifepower.com Connected\_From 1faaa939087c3479441d9f9c83a80ac7ec9b929e626cb34a7417be9ff0316ff7

### Description

667CF9E8EC1DAC7812F92BD77AF702A1 attempts to connect to the domain.

## 919xy.com

### Tags

command-and-control

### URLs

919xy.com/contactus/about.php

### Relationships

919xy.com Connected\_From 1faaa939087c3479441d9f9c83a80ac7ec9b929e626cb34a7417be9ff0316ff7

### Description

667CF9E8EC1DAC7812F92BD77AF702A1 attempts to connect to the domain.

## 3ff4ebae6c255d4ae6b747a77f2821f2b619825c7789c7ee5338da5ecb375395

### Tags

trojan

### Details

<b>Name</b>	A7C804B62AE93D708478949F498342F9
<b>Size</b>	128512 bytes
<b>Type</b>	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
<b>MD5</b>	a7c804b62ae93d708478949f498342f9
<b>SHA1</b>	09db826a7b6dbb16e2d7b3046e0da9fe7342f00f
<b>SHA256</b>	3ff4ebae6c255d4ae6b747a77f2821f2b619825c7789c7ee5338da5ecb375395
<b>SHA512</b>	c186485779ef22e6b65b3ba43a4290026d7b97b0d98ab8fe35f811c911be80402ea8bdf89e9c7169b3e7168d1e6a55eaa3fb8fd2165e5
<b>ssdeep</b>	1536:JkkY5dY/p7aY3xkuvxaSfhkSn5ITToZkBYKgZXRp5zr4t8DQeAsWq8McdC5vA8G:Ck0Y/p7TvFhITToGYKgZj7DwC5vA8E
<b>Entropy</b>	6.557876

### Antivirus

<b>Ahnlab</b>	Trojan/Win32.Lumal
<b>Antiy</b>	Trojan/Win32.Manuscript
<b>Avira</b>	TR/AD.LazerusAPT.vwvsu
<b>BitDefender</b>	Trojan.GenericKD.40376367

<b>ClamAV</b>	Win.Trojan.Autophyte-6582725-0
<b>ESET</b>	a variant of Win32/NukeSped.EN trojan
<b>Emsisoft</b>	Trojan.GenericKD.40376367 (B)
<b>Ikarus</b>	Trojan.Win32.NukeSped
<b>K7</b>	Trojan ( 00539ca21 )
<b>Microsoft Security Essentials</b>	Trojan:Win32/Autophyte.F!dha
<b>NANOAV</b>	Trojan.Win32.NukeSped.fgiarj
<b>Symantec</b>	Trojan.Gen.2
<b>TACHYON</b>	Trojan/W32.Agent.128512.AAF
<b>TrendMicro</b>	Backdoo.C7D30B55
<b>TrendMicro House Call</b>	Backdoo.C7D30B55
<b>VirusBlokAda</b>	BScope.Trojan.Manuscript

#### YARA Rules

No matches found.

#### ssdeep Matches

No matches found.

#### PE Metadata

**Compile Date** 2018-08-02 21:34:02-04:00

**Import Hash** 95dff862e0b00db0b05bcf957ad9e12e

#### PE Sections

MD5	Name	Raw Size	Entropy
39810a1d06213e840b94fbb1b3858b7c	header	1024	2.896592
197d2613ce721b378472dfa545446db5	.text	89600	6.595346
b875ef9ee01d6efadfad0d1b788851d1	.rdata	28160	5.352208
d8727a0a5051d7418591aae3a42a3f01	.data	3072	4.460652
302771a063d00e731afc38a29a0eda64	.gfids	512	1.779168
89b7e19270b2a5563c301b84b28e423f	.rsrc	512	4.714485
324d867372c3590e64d7eb61f4cd1de5	.reloc	5632	6.594775

#### Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

#### Relationships

3ff4ebae6c... Connected\_To pakteb.com

3ff4ebae6c... Connected\_To nuokejs.com

3ff4ebae6c... Connected\_To qdbazaar.com

#### Description

This file is a 32-bit DLL and has been identified as Variant B. Refer to 912F87392A889070DBB1097A82CCD93F for analysis.

#### pakteb.com

#### Tags

command-and-control

#### URLs

pakteb.com/include/left.php

Relationships

pakteb.com Connected\_From 3ff4ebae6c255d4ae6b747a77f2821f2b619825c7789c7ee5338da5ecb375395

---

pakteb.com Connected\_From c2f150dbe9a8efb72dc46416ca29acdbae6fd4a2af16b27f153eaabd4772a2a1

Description

A7C804B62AE93D708478949F498342F9 and 86685EC8C3C717AA2A9702E2C9DEC379 attempt to connect to the domain.

**nuokejs.com**

Tags

command-and-control

URLs

nuokejs.com/contactus/about.php

Relationships

nuokejs.com Connected\_From 3ff4ebae6c255d4ae6b747a77f2821f2b619825c7789c7ee5338da5ecb375395

---

nuokejs.com Connected\_From c2f150dbe9a8efb72dc46416ca29acdbae6fd4a2af16b27f153eaabd4772a2a1

Description

A7C804B62AE93D708478949F498342F9 and 86685EC8C3C717AA2A9702E2C9DEC379 attempt to connect to the domain.

**qdbazaar.com**

Tags

command-and-control

URLs

qdbazaar.com/include/footer.php

Relationships

qdbazaar.com Connected\_From 3ff4ebae6c255d4ae6b747a77f2821f2b619825c7789c7ee5338da5ecb375395

---

qdbazaar.com Connected\_From c2f150dbe9a8efb72dc46416ca29acdbae6fd4a2af16b27f153eaabd4772a2a1

Description

A7C804B62AE93D708478949F498342F9 and 86685EC8C3C717AA2A9702E2C9DEC379 attempt to connect to the domain.

**c2f150dbe9a8efb72dc46416ca29acdbae6fd4a2af16b27f153eaabd4772a2a1**

Tags

backdoortrojan

Details

<b>Name</b>	86685EC8C3C717AA2A9702E2C9DEC379
<b>Size</b>	156672 bytes
<b>Type</b>	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
<b>MD5</b>	86685ec8c3c717aa2a9702e2c9dec379
<b>SHA1</b>	29ddf9baad018518060814a03d424f4e08a0e914
<b>SHA256</b>	c2f150dbe9a8efb72dc46416ca29acdbae6fd4a2af16b27f153eaabd4772a2a1
<b>SHA512</b>	5bfee5737aaa7b5c42f49d2963ca3fdb0212eb4b298366e6e15ce7b6a9c09b3a1d4971683414318e5b7463eb9fa0a508179b72a72ceb
<b>ssdeep</b>	3072:/ucPnT+MMMMRwVK77YWOj885LhaEuTiAQLvkkABYn9N:/ZnTwn77YWOjbl4hfq
<b>Entropy</b>	6.192260

Antivirus

<b>Ahnlab</b>	Trojan/Win64.Manuscript
<b>Avira</b>	TR/AD.APTLazerus.vzbiu
<b>BitDefender</b>	Trojan.GenericKD.31159551

<b>ClamAV</b>	Win.Trojan.Autophyte-6582725-0
<b>ESET</b>	a variant of Win64/NukeSped.BD trojan
<b>Emsisoft</b>	Trojan.GenericKD.31159551 (B)
<b>Ikarus</b>	Trojan.Win32.Autophyte
<b>K7</b>	Trojan ( 0053a60a1 )
<b>Microsoft Security Essentials</b>	Trojan:Win32/Autophyte.F!dha
<b>NANOAV</b>	Trojan.Win64.NukeSped.fglqhp
<b>Symantec</b>	Trojan Horse
<b>TACHYON</b>	Backdoor/W64.Agent.156672
<b>TrendMicro</b>	BKDR64_.37857E4E
<b>TrendMicro House Call</b>	BKDR64_.37857E4E
<b>VirusBlokAda</b>	Trojan.Manuscript
<b>Zillya!</b>	Trojan.GenericKD.Win32.145349

#### YARA Rules

No matches found.

#### ssdeep Matches

No matches found.

#### PE Metadata

**Compile Date** 2018-08-02 21:34:37-04:00

**Import Hash** 2013af6912650171ab98cb2d8b0b1a2e

#### PE Sections

MD5	Name	Raw Size	Entropy
41a5e8385e9725d9bbf9f9b6a0734475	header	1024	3.078331
7db58e09d4ea1e65d3c0b3bb94fcd1ba	.text	98304	6.401910
b446c87210ab967d6db88c8aa1095ccb	.rdata	44032	5.142828
a748046679e968fa96c68aa53107f08a	.data	4096	3.641240
a1cdf2e22fff16573b4f461759d5e02d	.pdata	6144	4.913515
48a18c337d9c605b138a3f2e8fa572d1	.guids	512	1.638651
106eb1a5ed9fc911defec918b5086d48	.rsrc	512	4.720823
452a8928c69f9af56227179f5b5b98f0	.reloc	2048	4.794478

#### Relationships

c2f150dbe9... Connected\_To pakteb.com

c2f150dbe9... Connected\_To nuokejs.com

c2f150dbe9... Connected\_To qdbazaar.com

#### Description

This file is a 64-bit DLL and has been identified as Variant B. Refer to 912F87392A889070DBB1097A82CCD93F for analysis.

**1678327c5f36074cf5f18d1a92c2d9fea9bfae6c245eaa01640fd75af4d6c11**

#### Tags

trojan

#### Details

<b>Name</b>	86D3C1B354CE696E454C42D8DC6DF1B7
<b>Size</b>	129024 bytes
<b>Type</b>	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
<b>MD5</b>	86d3c1b354ce696e454c42d8dc6df1b7
<b>SHA1</b>	4d17c0fb13b532ba5a680c1701026d29fb1931e7
<b>SHA256</b>	1678327c5f36074cf5f18d1a92c2d9fea9bfae6c245eaad01640fd75af4d6c11
<b>SHA512</b>	cdb1338674ea9407bbffe3569fbd021df4ebefe1bc8fad2415506005d2c6bd7d6f134c89aa6c0bc5a539783fd293329d3d442cf313c8d0c
<b>ssdeep</b>	1536:Qkj1G7eW0vV7qZx1kJMzKzO12lsSKwVDF1ZTgKTTkbv+DQeAsWq8McdsLA8+nr:QkW/0JqezblsSfx1VguFDwsLA8+n
<b>Entropy</b>	6.568189

#### Antivirus

<b>Ahnlab</b>	Trojan/Win32.Manuscript
<b>BitDefender</b>	Gen:Variant.Ursu.337564
<b>ClamAV</b>	Win.Trojan.Autophyte-6582725-0
<b>ESET</b>	a variant of Win32/NukeSped.EN trojan
<b>Emsisoft</b>	Gen:Variant.Ursu.337564 (B)
<b>Microsoft Security Essentials</b>	Trojan:Win32/Autophyte.F!dha
<b>Sophos</b>	Troj/NukSped-A
<b>TACHYON</b>	Trojan-Spy/W32.Manuscript.129024
<b>TrendMicro</b>	Backdoo.C7D30B55
<b>TrendMicro House Call</b>	Backdoo.C7D30B55
<b>VirusBlokAda</b>	BScope.Trojan.Manuscript

#### YARA Rules

No matches found.

#### ssdeep Matches

No matches found.

#### PE Metadata

<b>Compile Date</b>	2018-09-02 20:34:51-04:00
<b>Import Hash</b>	95dff862e0b00db0b05bcf957ad9e12e

#### PE Sections

MD5	Name	Raw Size	Entropy
362b9b00897b7cbef771430b593496d0	header	1024	2.958886
7121ea1bf412df273b88513bd7efb39d	.text	90112	6.601268
cad02e58fb94dfc67ee1fae275b98902	.rdata	28160	5.375842
d8727a0a5051d7418591aae3a42a3f01	.data	3072	4.460652
17c535c5be4192a355ca9e8d19f10138	.gids	512	1.766088
89b7e19270b2a5563c301b84b28e423f	.rsrc	512	4.714485
db55d6484373493760026c3180cebf59	.reloc	5632	6.602821

#### Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

Relationships

1678327c5f... Connected\_To aurumgroup.co.id

---

1678327c5f... Connected\_To 51shousheng.com

---

1678327c5f... Connected\_To new.titanik.fr

Description

This file is a 32-bit DLL and has been identified as Variant B. Refer to 912F87392A889070DBB1097A82CCD93F for analysis.

**aurumgroup.co.id**

Tags

command-and-control

URLs

aurumgroup.co.id/wp-includes/rest.php

Relationships

aurumgroup.co.id Connected\_From 1678327c5f36074cf5f18d1a92c2d9fea9bfae6c245eaad01640fd75af4d6c11

---

aurumgroup.co.id Connected\_From c0ee19d7545f98fcd15725a3d9f0dbd0f35b2091e1c5b9cf4744f16e81a030c5

Description

86D3C1B354CE696E454C42D8DC6DF1B7 and 5182E7A2037717F2F9BBF6BA298C48FB attempt to connect to the domain.

**51shousheng.com**

Tags

command-and-control

URLs

51shousheng.com/include/partview.php

Relationships

51shousheng.com Connected\_From 1678327c5f36074cf5f18d1a92c2d9fea9bfae6c245eaad01640fd75af4d6c11

---

51shousheng.com Connected\_From c0ee19d7545f98fcd15725a3d9f0dbd0f35b2091e1c5b9cf4744f16e81a030c5

Description

86D3C1B354CE696E454C42D8DC6DF1B7 and 5182E7A2037717F2F9BBF6BA298C48FB attempt to connect to the domain.

**new.titanik.fr**

Tags

command-and-control

URLs

new.titanik.fr/wp-includes/common.php

Relationships

new.titanik.fr Connected\_From 1678327c5f36074cf5f18d1a92c2d9fea9bfae6c245eaad01640fd75af4d6c11

---

new.titanik.fr Connected\_From c0ee19d7545f98fcd15725a3d9f0dbd0f35b2091e1c5b9cf4744f16e81a030c5

Description

86D3C1B354CE696E454C42D8DC6DF1B7 and 5182E7A2037717F2F9BBF6BA298C48FB attempt to connect to the domain.

**c0ee19d7545f98fcd15725a3d9f0dbd0f35b2091e1c5b9cf4744f16e81a030c5**

Tags

trojan

Details

**Name** 5182E7A2037717F2F9BBF6BA298C48FB

---

**Size** 157696 bytes

---

**Type** PE32+ executable (DLL) (GUI) x86-64, for MS Windows

---

<b>MD5</b>	5182e7a2037717f2f9bbf6ba298c48fb
<b>SHA1</b>	47b5d2c3f741a896a26993dbbf4a5deec6f9ac53
<b>SHA256</b>	c0ee19d7545f98fcd15725a3d9f0dbd0f35b2091e1c5b9cf4744f16e81a030c5
<b>SHA512</b>	016a80dbd78e5614e38388b3e107cb9c9f29a971dfb90cceb8e91ce0af448359ac8ad3a898e623b142f4b7bd2638ffcd7869575d50e44c
<b>ssdeep</b>	3072:HXyO7ibruDVtCuwxxy7Gwi6OnSaytibCCLUvg2/1Yn:HCO7ibruDVtCuly7GwiBSaYSZ9x
<b>Entropy</b>	6.194475

#### Antivirus

<b>Ahnlab</b>	Trojan/Win64.Manuscript
<b>BitDefender</b>	Gen:Variant.Ser.Ursu.13069
<b>ClamAV</b>	Win.Trojan.Autophyte-6582725-0
<b>ESET</b>	a variant of Win64/NukeSped.BD trojan
<b>Emsisoft</b>	Gen:Variant.Ser.Ursu.13069 (B)
<b>Microsoft Security Essentials</b>	Trojan:Win32/Autophyte.F!dha
<b>Sophos</b>	Troj/NukSped-A
<b>TACHYON</b>	Trojan-Spy/W64.Manuscript.157696
<b>TrendMicro</b>	Backdo0.7185D059
<b>TrendMicro House Call</b>	Backdo0.7185D059

#### YARA Rules

No matches found.

#### ssdeep Matches

No matches found.

#### PE Metadata

<b>Compile Date</b>	2018-09-02 20:35:10-04:00
<b>Import Hash</b>	2013af6912650171ab98cb2d8b0b1a2e

#### PE Sections

MD5	Name	Raw Size	Entropy
61ae8f48806dd3b4eddbc2f093941fa0	header	1024	3.151619
0d0ecb30d5fc4d1be82fbfb1449842c9	.text	99328	6.398421
29946785fcc534b4bb5c9591efc97c5d	.rdata	44032	5.155298
97eb24ae73f627856d986c0aaf5f1bd6	.data	4096	3.639072
d09091ebf6183a54ca5da171553c1484	.pdata	6144	4.949925
3f74a25aca1400441dae0c4256b2d870	.gfids	512	1.622338
2d9583cf3eaec364bc8e0e0ad5dadf74	.rsrc	512	4.720823
921b6d44e23652a86f3462e3eb523499	.reloc	2048	4.794591

#### Relationships

c0ee19d754...	Connected_To	aurumgroup.co.id
c0ee19d754...	Connected_To	51shousheng.com
c0ee19d754...	Connected_To	new.titanik.fr

#### Description

This file is a 64-bit DLL and has been identified as Variant B. Refer to 912F87392A889070DBB1097A82CCD93F for analysis.

9e4bd9676bb3460be68ba4559a824940a393bde7613850eda9196259e453b9f3

Tags

trojan

Details

<b>Name</b>	668D5B5761755C9D061DA74CB21A8B75
<b>Size</b>	2212864 bytes
<b>Type</b>	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
<b>MD5</b>	668d5b5761755c9d061da74cb21a8b75
<b>SHA1</b>	49da356fd99d4b7c8cb4e77f89877ee41f8948ca
<b>SHA256</b>	9e4bd9676bb3460be68ba4559a824940a393bde7613850eda9196259e453b9f3
<b>SHA512</b>	8ec530a1a3fba89589f6041fc5466befa2247f3829ae46bff91f341a0957abb2515168e1ac6eaf02d04fc8bcd37a237c9071b2fa295a9963
<b>ssdeep</b>	49152:h6nuk9DG/IEYtBgKPd3S7k1X2NDxDNWnnuTniH6:h6ukYEYtJV3S7aEDrWnnuTu
<b>Entropy</b>	7.958398

Antivirus

<b>Ahnlab</b>	Trojan/Win64.Agent
<b>Antiy</b>	Trojan/Win32.Manuscript
<b>Avira</b>	TR/Agent.qhgqy
<b>BitDefender</b>	Trojan.GenericKD.31269235
<b>ESET</b>	Win64/NukeSped.BT trojan
<b>Emsisoft</b>	Trojan.GenericKD.31269235 (B)
<b>Ikarus</b>	Trojan.Win64.Themida
<b>K7</b>	Trojan ( 0054ac401 )
<b>McAfee</b>	Generic Trojan.gw
<b>NANOAV</b>	Trojan.Win64.Manuscript.fouxwk
<b>Quick Heal</b>	Trojan.Manuscript
<b>Symantec</b>	Trojan Horse
<b>TACHYON</b>	Trojan/W64.Manuscript.2212864
<b>TrendMicro</b>	Trojan.20BD6557
<b>TrendMicro House Call</b>	Trojan.20BD6557
<b>VirusBlokAda</b>	Trojan.Manuscript
<b>Zillya!</b>	Trojan.Manuscript.Win32.19

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

<b>Compile Date</b>	2018-09-16 20:16:44-04:00
<b>Import Hash</b>	baa93d47220682c04d92f7797d9224ce

PE Sections

MD5	Name	Raw Size	Entropy
-----	------	----------	---------



e7fd8dca1ed04d4a10fb802bf3c8d5ef	header	4096	0.987963
de0782befb39ad89b25486af66e57da0		80896	7.892611
7b576835c006db4e4bd934eedf39c4ec	.rsrc	512	4.525348
52add692ea0be6f14721c05b9a5dab58	.idata	512	1.297004
936850d3b5e99c2a119b2a334196f7ac		512	0.227252
994b9b89968924be47b7897c566017cb	dwukfuez	2119680	7.961143
63fc048012cf91b3840d92a6b6bbe245	fgwvbapa	512	4.416947
4720f9e5ba755a82ff72caea5d49817e	.pdata1	6144	4.962182

Relationships

9e4bd9676b... Connected\_To duratransgroup.com

9e4bd9676b... Connected\_To eygingenieros.com

9e4bd9676b... Connected\_To eventum.cwsdev3.biz

Description

This file is a 64-bit DLL and has been identified as Variant B. Refer to 912F87392A889070DBB1097A82CCD93F for analysis.

**duratransgroup.com**

Tags

command-and-control

URLs

[duratransgroup.com/engl/lang.php](http://duratransgroup.com/engl/lang.php)

Relationships

duratransgroup.com Connected\_From 9e4bd9676bb3460be68ba4559a824940a393bde7613850eda9196259e453b9f3

Description

668D5B5761755C9D061DA74CB21A8B75 attempts to connect to the domain.

**eygingenieros.com**

Tags

command-and-control

URLs

[eygingenieros.com/wp-includes/common.php](http://eygingenieros.com/wp-includes/common.php)

Relationships

eygingenieros.com Connected\_From 9e4bd9676bb3460be68ba4559a824940a393bde7613850eda9196259e453b9f3

Description

668D5B5761755C9D061DA74CB21A8B75 attempts to connect to the domain.

**eventum.cwsdev3.biz**

URLs

[eventum.cwsdev3.biz/wp-includes/common.php](http://eventum.cwsdev3.biz/wp-includes/common.php)

Relationships

eventum.cwsdev3.biz Connected\_From 9e4bd9676bb3460be68ba4559a824940a393bde7613850eda9196259e453b9f3

Description

668D5B5761755C9D061DA74CB21A8B75 attempts to connect to the domain.

**eee38c632c62ca95b5c66f8d39a18e23b9175845560af84b6a2f69b7f9b6ec1c**

Tags

trojan

Details

<b>Name</b>	35E38D023B253C0CD9BD3E16AFC362A7
<b>Size</b>	129024 bytes
<b>Type</b>	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
<b>MD5</b>	35e38d023b253c0cd9bd3e16afc362a7
<b>SHA1</b>	c850e733f4e0d4abb34969678f2a1abe3b2f4c24
<b>SHA256</b>	eee38c632c62ca95b5c66f8d39a18e23b9175845560af84b6a2f69b7f9b6ec1c
<b>SHA512</b>	c605f9f895773b8a9a50581b490cfbf2434f687ec4faae0ce37082fb8fb5efa3e76f39fbc891bd38460b6ee56c240c09eada8b58cdaa9368
<b>ssdeep</b>	1536:XbWB4W7YWYCNWf65xAkNbf+QFc9lvmKw77vliLITrK+S31DQeAsWq8McDsX4A8PR:XbWt5yzf6kQolvmx7vliLh+DwsoA8PF
<b>Entropy</b>	6.571364

#### Antivirus

<b>Ahnlab</b>	Trojan/Win32.Manuscript
<b>Antiy</b>	Trojan/Win32.Manuscript
<b>Avira</b>	TR/AD.APTLazerus.qmssk
<b>BitDefender</b>	Trojan.GenericKD.40712007
<b>Cyren</b>	W32/Trojan.BIAI-3752
<b>ESET</b>	a variant of Win32/NukeSped.EN trojan
<b>Emsisoft</b>	Trojan.GenericKD.40712007 (B)
<b>Ikarus</b>	Trojan.Win32.NukeSped
<b>K7</b>	Trojan ( 00539ca21 )
<b>McAfee</b>	Trojan-FQUB!35E38D023B25
<b>Microsoft Security Essentials</b>	Trojan:Win32/Autophyte.F!dha
<b>NANOAV</b>	Trojan.Win32.Manuscript.fkqspx
<b>NetGate</b>	Trojan.Win32.Malware
<b>Sophos</b>	Troj/NukSped-A
<b>Symantec</b>	Trojan.Gen.2
<b>TACHYON</b>	Trojan/W32.Manuscript.129024
<b>TrendMicro</b>	BKDR_NU.A41D576C
<b>TrendMicro House Call</b>	BKDR_NU.A41D576C
<b>VirusBlokAda</b>	BScope.Trojan.Manuscript
<b>Zillya!</b>	Trojan.Manuscript.Win32.22

#### YARA Rules

No matches found.

#### ssdeep Matches

No matches found.

#### PE Metadata

<b>Compile Date</b>	2018-10-19 03:23:31-04:00
<b>Import Hash</b>	95dff862e0b00db0b05bcf957ad9e12e

#### PE Sections

MD5	Name	Raw Size	Entropy
a721b29ba240341403160375cd091c24	header	1024	2.966234

70648fd64041effbf19466b97acb6341	.text	90112	6.601122
eb845e76ca0aac042cc722b086eadc6d	.rdata	28160	5.385942
d8727a0a5051d7418591aae3a42a3f01	.data	3072	4.460652
52ad7e79f4212b855563d2718cca7bbb	.gids	512	1.768774
89b7e19270b2a5563c301b84b28e423f	.rsrc	512	4.714485
54cbc7874c922d6f07d0ebae7a641ffe	.reloc	5632	6.607571

Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

Relationships

eee38c632c... Connected\_To theinspectionconsultant.com

eee38c632c... Connected\_To danagloverinteriors.com

eee38c632c... Connected\_To as-brant.ru

Description

This file is a 32-bit DLL and has been identified as Variant B. Refer to 912F87392A889070DBB1097A82CCD93F for analysis.

**theinspectionconsultant.com**

Tags

command-and-control

URLs

theinspectionconsultant.com/wp-content/plugins/akismet/index1.php

Relationships

theinspectionconsultant.com Connected\_From f6e1a146543d2903146698da5698b2a214201720c0be756c6e8d2a2f27dcfaff

theinspectionconsultant.com Connected\_From eee38c632c62ca95b5c66f8d39a18e23b9175845560af84b6a2f69b7f9b6ec1c

Description

835E38D023B253C0CD9BD3E16AFC362A7 and 72FE869AA394EF0A62BB8324857770DD attempt to connect to the domain.

**danagloverinteriors.com**

Tags

command-and-control

URLs

danagloverinteriors.com/wp-content/plugins/jetpack/common.php

Relationships

danagloverinteriors.com Connected\_From f6e1a146543d2903146698da5698b2a214201720c0be756c6e8d2a2f27dcfaff

danagloverinteriors.com Connected\_From eee38c632c62ca95b5c66f8d39a18e23b9175845560af84b6a2f69b7f9b6ec1c

Description

835E38D023B253C0CD9BD3E16AFC362A7 and 72FE869AA394EF0A62BB8324857770DD attempt to connect to the domain.

**as-brant.ru**

Tags

command-and-control

URLs

as-brant.ru/wp-content/themes/shapely/common.php

Relationships

as-brant.ru Connected\_From f6e1a146543d2903146698da5698b2a214201720c0be756c6e8d2a2f27dcfaff

as-brant.ru Connected\_From eee38c632c62ca95b5c66f8d39a18e23b9175845560af84b6a2f69b7f9b6ec1c

Description

835E38D023B253C0CD9BD3E16AFC362A7 and 72FE869AA394EF0A62BB8324857770DD attempt to connect to the domain.

**f6e1a146543d2903146698da5698b2a214201720c0be756c6e8d2a2f27dcfaff**

Tags

trojan

Details

<b>Name</b>	72FE869AA394EF0A62BB8324857770DD
<b>Size</b>	157696 bytes
<b>Type</b>	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
<b>MD5</b>	72fe869aa394ef0a62bb8324857770dd
<b>SHA1</b>	de03860d8a43358554ee4fab22c3fb25cae8992b
<b>SHA256</b>	f6e1a146543d2903146698da5698b2a214201720c0be756c6e8d2a2f27dcfaff
<b>SHA512</b>	54c86cef7f0b2b795d1e04323432acfeb78c751bcfdc1b693f2048b8f6af7fc06a6ef64d481764ec0c5261d5c4b020f079db6769433c705b
<b>ssdeep</b>	3072:gXFP7wuoSeJOwxFL07qJ/hCIeftBgbRFCLUv3w7uYngn:g1P7wuoSeJOAs7qJ5cfzkKq0G
<b>Entropy</b>	6.200286

Antivirus

<b>Ahnlab</b>	Trojan/Win64.Manuscript
<b>Antiy</b>	Trojan/Win64.Manuscript
<b>Avira</b>	TR/AD.APTLazerus.heseo
<b>BitDefender</b>	Trojan.GenericKD.31313805
<b>ESET</b>	a variant of Win64/NukeSped.BD trojan
<b>Emsisoft</b>	Trojan.GenericKD.31313805 (B)
<b>Ikarus</b>	Trojan.Win64.Nukesped
<b>K7</b>	Trojan ( 0053fa3f1 )
<b>McAfee</b>	Trojan-FQUB!72FE869AA394
<b>Microsoft Security Essentials</b>	Trojan:Win32/Autophyte.F!dha
<b>NANOAV</b>	Trojan.Win64.NukeSped.fjscrm
<b>Sophos</b>	Troj/NukSped-A
<b>Symantec</b>	Trojan Horse
<b>TrendMicro</b>	BKDR64_.BB415F80
<b>TrendMicro House Call</b>	BKDR64_.BB415F80
<b>VirusBlokAda</b>	Trojan.Win64.Manuscript
<b>Zillya!</b>	Trojan.Manuscript.Win64.1

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

<b>Compile Date</b>	2018-10-19 03:23:52-04:00
<b>Import Hash</b>	2013af6912650171ab98cb2d8b0b1a2e

PE Sections

MD5	Name	Raw Size	Entropy
1eb1d7ade0e4b678e553734e2cd3e6f3	header	1024	3.155059
ab0669c74b116223c3de6213940a0268	.text	99328	6.401690
911b91de22fe394f42948a75e7e87817	.rdata	44032	5.166334
97eb24ae73f627856d986c0aaf5f1bd6	.data	4096	3.639072
f1f39a167b5525fd01fdb683d0bf2ca8	.pdata	6144	4.934767
d3a397fe89f106c07d5fa28e0bbf7edb	.gfids	512	1.653715
2d9583cf3eaec364bc8e0e0ad5dadf74	.rsrc	512	4.720823
0814e49777e4a22532b43b74a44c2c72	.reloc	2048	4.794082

#### Relationships

f6e1a14654...	Connected_To	theinspectionconsultant.com
f6e1a14654...	Connected_To	danagloverinteriors.com
f6e1a14654...	Connected_To	as-brant.ru

#### Description

This file is a 64-bit DLL and has been identified as Variant B. Refer to 912F87392A889070DBB1097A82CCD93F for analysis.

**37bb27f4eb40b8947e184afddba019001c12f97588e7f596ab6bc07f7c152602**

#### Tags

backdoorpup Trojan

#### Details

<b>Name</b>	A8B6EC51ED88C0329FD3329CB615BBC9
<b>Size</b>	95744 bytes
<b>Type</b>	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
<b>MD5</b>	a8b6ec51ed88c0329fd3329cb615bbc9
<b>SHA1</b>	f744f5f97ace1a4862e764971449c28c4b880e8f
<b>SHA256</b>	37bb27f4eb40b8947e184afddba019001c12f97588e7f596ab6bc07f7c152602
<b>SHA512</b>	26e1558557e3b44d18a1d97a38cc9881bc025d4979e914d40ef42248d7c5b3d09cfa17ab3893d91d65c29ba9d94047726f42be91bcd4
<b>ssdeep</b>	1536:flbpjZh3Qj6T4T0PY0qBbXP35d5Nh3UCzsW8cdvZ1Q6B:fM3Qe4yY0qtf/hk+vZ1Q6B
<b>Entropy</b>	6.373893

#### Antivirus

<b>Ahnlab</b>	Backdoor/Win32.Agent
<b>Antiy</b>	Trojan/Win32.Manuscript
<b>Avira</b>	TR/Agent.ktlxw
<b>BitDefender</b>	Trojan.GenericKD.32074646
<b>ClamAV</b>	Win.Trojan.GhostPuppet-7404648-0
<b>ESET</b>	a variant of Win32/Agent.AAWV trojan
<b>Emsisoft</b>	Trojan.GenericKD.32074646 (B)
<b>Ikarus</b>	Trojan.Agent
<b>NANOAV</b>	Trojan.Win32.Manuscript.fscabu
<b>Quick Heal</b>	Trojan.Manuscript
<b>Symantec</b>	Trojan Horse

<b>TACHYON</b>	Trojan-Spy/W32.Agent.95744.J
<b>VirusBlokAda</b>	Trojan.Manuscript
<b>Zillya!</b>	Trojan.Agent.Win32.1161280

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

**Compile Date** 2019-06-18 08:03:21-04:00

**Import Hash** 5446c3bf7cbf3287d9a8bfcc3ac95a9

PE Sections

MD5	Name	Raw Size	Entropy
f415a11b78cf73e9c20856ebf542c7c5	header	1024	2.732806
32765031f78d5821a7828a3a03fb509a	.text	61440	6.572955
946000c535906e58ffe121d5cff7c6ba	.rdata	25600	4.984772
25f93d3b0c87967785c3858f1b44cb02	.data	2560	2.163019
065463fcb19d087772450d47229f013f	.rsrc	512	4.717679
f860381eb55d57e79cd6cf5f8972763a	.reloc	4608	6.518570

Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

Relationships

37bb27f4eb...	Connected_To	rxrenew.us
37bb27f4eb...	Connected_To	creativefishstudio.com
37bb27f4eb...	Connected_To	sensationalsecrets.com

Description

This file is a 32-bit DLL and has been identified as Variant C. Variant C can be distinguished from previous versions through the absence of the be ""dJUI\*JE&IM@UNQ@" and the use of a generated cookie to pass certain information instead of multi-part HTTP POST requests. The cookie is a standard Google Analytics cookie. The format used by the malware is noted below:

--Begin cookie format--

Cookie: \_ga=GA1.%d.%02d%d%02d.%d%05d%04d; gid=GA1.%d.%02d%d%03d.%d%05d%04d Cookie: \_ga=GA1.<1>.<2><3><4><5>.<6><9><10><11>.<6><7><8>

where

- 1 = rand % 10
  - 2 = rand % 100
  - 3 = 0 or 1 if implant is ready to receive its first command
  - 4 = sessionID
  - 5 = rand % 100
  - 6 = rand % 10
  - 7 = rand % 100000
  - 8 = rand % 10000
  - 9 = rand % 100
  - 10 = 1879 or 8678 if handshake packet
  - 11 = rand % 1000
- End cookie format--

Variant C will randomly choose from one of three hard-coded Accept-Language headers:

--Begin Accept-Language headers--  
 Accept-Language: en-US,en;q=0.5  
 Accept-Language: de-CH  
 Accept-Language: az-Arab  
 --End Accept-Language headers--

Variant C datagrams are sent in the HTTP POST body and encrypted in the same manner as Variant B with the same RC4 key. Like in Variant B, reset after the SystemInfo command. Variant C performs API loading at runtime but does not obfuscate the strings.

Screenshots

Ordinal	Description
0x21279E	PutFile
0x2AFCB2	SystemInfo
0x38CE55	DrivesInfo
0x3A65F8	Sleep
0x3A6A93	KeepAlive
0x3B187D	Disconnect
0x484B81	GetFile
0x48C82A	TestConnect
0x48D6FC	CreateProcess
0x7FC0A4	RunCommandLine

**Figure 3** - Variant C contains the commands displayed in the table.

**rxrenew.us**

Tags

command-and-control

URLs

[rxrenew.us/wp-content/themes/hestias/index.php](http://rxrenew.us/wp-content/themes/hestias/index.php)

Relationships

rxrenew.us Connected\_From e6fc788b5ff7436da4450191a003966a68e2a1913c83f1d3aec78c65f3ba85ca  
 rxrenew.us Connected\_From 37bb27f4eb40b8947e184afddba019001c12f97588e7f596ab6bc07f7c152602

Description

A8B6EC51ED88C0329FD3329CB615BBC9 and 117FA0B8B8B965680C7B630C6E2BF01D attempt to connect to the domain.

**creativefishstudio.com**

Tags

command-and-control

URLs

[creativefishstudio.com/newbiesspeak/left.php](http://creativefishstudio.com/newbiesspeak/left.php)

Relationships

creativefishstudio.com Connected\_From e6fc788b5ff7436da4450191a003966a68e2a1913c83f1d3aec78c65f3ba85ca  
 creativefishstudio.com Connected\_From 37bb27f4eb40b8947e184afddba019001c12f97588e7f596ab6bc07f7c152602

Description

A8B6EC51ED88C0329FD3329CB615BBC9 and 117FA0B8B8B965680C7B630C6E2BF01D attempt to connect to the domain.

**sensationalsecrets.com**

Tags

command-and-control

URLs

[sensationalsecrets.com/js/left.php](http://sensationalsecrets.com/js/left.php)

Relationships

sensationalsecrets.com Connected\_From e6fc788b5ff7436da4450191a003966a68e2a1913c83f1d3aec78c65f3ba85ca  
 sensationalsecrets.com Connected\_From 37bb27f4eb40b8947e184afddba019001c12f97588e7f596ab6bc07f7c152602

Description

A8B6EC51ED88C0329FD3329CB615BBC9 and 117FA0B8B8B965680C7B630C6E2BF01D attempt to connect to the domain.

**e6fc788b5ff7436da4450191a003966a68e2a1913c83f1d3aec78c65f3ba85ca**

## Tags

puptrojan

## Details

<b>Name</b>	117FA0B8B8B965680C7B630C6E2BF01D
<b>Size</b>	116736 bytes
<b>Type</b>	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
<b>MD5</b>	117fa0b8b8b965680c7b630c6e2bf01d
<b>SHA1</b>	7202fea74865e085104f839574cd150613fbcf99
<b>SHA256</b>	e6fc788b5ff7436da4450191a003966a68e2a1913c83f1d3aec78c65f3ba85ca
<b>SHA512</b>	454703dd49b4b8feb36b71d7a6d18f7811c221675e272b6fe0b3d9f60a7c5c61bb6b0d8f9d84eb13cf68685dd9ef482f39b6026dda8867
<b>ssdeep</b>	3072:iN9F81gu+0WsPxRr0T7V4P2F6U6V641B820D:iN81/+0JpJ0TJrq600D
<b>Entropy</b>	6.008099

## Antivirus

<b>Ahnlab</b>	Trojan/Win64.Manuscript
<b>Antiy</b>	Trojan/Win32.Manuscript
<b>BitDefender</b>	Trojan.GenericKD.32076195
<b>ClamAV</b>	Win.Trojan.GhostPuppet-7404648-0
<b>ESET</b>	a variant of Win64/NukeSped.CA trojan
<b>Emsisoft</b>	Trojan.GenericKD.32076195 (B)
<b>Ikarus</b>	Trojan.Win64.Nukesped
<b>NANOAV</b>	Trojan.Win64.Manuscript.fslzmk
<b>NetGate</b>	Trojan.Win32.Malware
<b>Quick Heal</b>	Trojan.Manuscript
<b>Symantec</b>	Trojan Horse
<b>TACHYON</b>	Trojan-Spy/W64.Agent.116736
<b>TrendMicro</b>	BKDR_NU.F8DCFF65
<b>TrendMicro House Call</b>	BKDR_NU.F8DCFF65
<b>VirusBlokAda</b>	Trojan.Manuscript
<b>Zillya!</b>	Trojan.NukeSped.Win64.35

## YARA Rules

No matches found.

## ssdeep Matches

No matches found.

## PE Metadata

<b>Compile Date</b>	2019-06-18 08:03:26-04:00
<b>Import Hash</b>	912d2b0681d67169c9ee0b4cead2c366

## PE Sections

MD5	Name	Raw Size	Entropy
638c9a9cdf6ecfc555c8c07f4e8c7ecf	header	1024	2.903657
90f4f418377655079d9186062658dd5d	.text	65536	6.364048



d57a642f43ef623527e4bc0870475b20	.rdata	40448	4.798275
025170c7aa8e93ab068076ec3d9e871b	.data	2560	2.321313
082001fb6c468d8828e1019e179b5749	.pdata	4608	4.785751
50c26f8b7696190a236f2e12c71402ce	.rsrc	512	4.717679
611f9b1269513b8c4810c722c5278660	.reloc	2048	4.851328

#### Relationships

e6fc788b5f... Connected\_To rxrenew.us

e6fc788b5f... Connected\_To creativefishstudio.com

e6fc788b5f... Connected\_To sensationalsecrets.com

#### Description

This file is a 64-bit DLL and has been identified as Variant C. Refer to A8B6EC51ED88C0329FD3329CB615BBC9 for analysis.

**284bc471647f951c79e3e333b2b19aa37f84cc39b55441a82e2a5f7319131fac**

#### Tags

puptrojan

#### Details

<b>Name</b>	DB590EA77A92AE6435E2EC954D065ED4
<b>Size</b>	118272 bytes
<b>Type</b>	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
<b>MD5</b>	db590ea77a92ae6435e2ec954d065ed4
<b>SHA1</b>	ef0c0ef95b1542184a6a1f4d1f4ece583046ba0a
<b>SHA256</b>	284bc471647f951c79e3e333b2b19aa37f84cc39b55441a82e2a5f7319131fac
<b>SHA512</b>	07d1da9735f468fd389bcf34052f94977ffc64028b54ae4a7f077aab8488bc5e82cde82671da84c0e649d1ffb3fe05491b7bfde967581799
<b>ssdeep</b>	1536:bUtygCBUwWkWtptf4W9wuJ9r82IVOWenSMwXjGCpsWBMdc9dIMLTQjP8PoRbB:oty7WkYwW9L98gVVZ/zGMWUUM8Ps
<b>Entropy</b>	6.003427

#### Antivirus

<b>Ahnlab</b>	Trojan/Win64.Manuscript
<b>Avira</b>	TR/NukeSped.wnyqo
<b>BitDefender</b>	Gen:Variant.Cerbu.38929
<b>ClamAV</b>	Win.Trojan.GhostPuppet-7404648-0
<b>Cyren</b>	W64/Trojan.MDBT-6130
<b>ESET</b>	a variant of Win64/NukeSped.CA trojan
<b>Emsisoft</b>	Gen:Variant.Cerbu.38929 (B)
<b>Ikarus</b>	Trojan.Win64.Nukesped
<b>McAfee</b>	RDN/Generic.fhb
<b>NANOAV</b>	Trojan.Win64.NukeSped.ftxzll
<b>Symantec</b>	Trojan Horse
<b>VirusBlokAda</b>	Trojan.Agent
<b>Zillya!</b>	Trojan.Agent.Win32.1117465

#### YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

**Compile Date** 2019-07-15 09:20:00-04:00

**Import Hash** 0760d8e97dd31634b3dd017abf4774a0

PE Sections

MD5	Name	Raw Size	Entropy
9514b568295f93b907811e056fb57c35	header	1024	2.987943
c82aed4c6f8d5ed8460b51e35915a90a	.text	66560	6.363581
a8c513f71aaafa5199def8a965ad5e51	.rdata	40448	4.819785
fe894e926ee83c0a9904cd411cdef116	.data	2560	2.327005
aacfa1b64b7343d8d12ddd57154285d	.pdata	4608	4.791352
ed53cfac37dd783aa39a61f036e4f4e9	.rsrc	1024	3.792752
06a0fac8b9ff5aff98362773e499a0f8	.reloc	2048	4.845065

Relationships

284bc47164... Connected\_To rhythm86.com

284bc47164... Connected\_To cabba-cacao.com

284bc47164... Connected\_To 3x-tv.com

Description

This file is a 64-bit DLL and has been identified as Variant C. Refer to A8B6EC51ED88C0329FD3329CB615BBC9 for analysis.

#### **rhythm86.com**

Tags

command-and-control

URLs

rhythm86.com/wp-content/themes/twenty十六/about.php

Relationships

rhythm86.com Connected\_From 284bc471647f951c79e3e333b2b19aa37f84cc39b55441a82e2a5f7319131fac

Description

DB590EA77A92AE6435E2EC954D065ED4 attempts to connect to the domain.

#### **cabba-cacao.com**

Tags

command-and-control

URLs

cabba-cacao.com/wp-content/themes/integral/about.php

Relationships

cabba-cacao.com Connected\_From 284bc471647f951c79e3e333b2b19aa37f84cc39b55441a82e2a5f7319131fac

Description

DB590EA77A92AE6435E2EC954D065ED4 attempts to connect to the domain.

#### **3x-tv.com**

Tags

command-and-control

URLs

3x-tv.com/plugins/editors/about.php

Relationships

3x-tv.com Connected\_From 284bc471647f951c79e3e333b2b19aa37f84cc39b55441a82e2a5f7319131fac

Description

DB590EA77A92AE6435E2EC954D065ED4 attempts to connect to the domain.

**a1cdb784100906d0ac895297c5a0959ab21a9fb39c687baf176324ee84095472**

Tags

backdoorpuptrojan

Details

<b>Name</b>	0856655351ACFFA1EE459EEEEAF164756
<b>Size</b>	119808 bytes
<b>Type</b>	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
<b>MD5</b>	0856655351acffa1ee459eeeeaf164756
<b>SHA1</b>	fe0f8a37887c8f8fb5eb3e8252a8df395b3e66e7
<b>SHA256</b>	a1cdb784100906d0ac895297c5a0959ab21a9fb39c687baf176324ee84095472
<b>SHA512</b>	1dec04eef52a9872de02fa6fc1afcc9ccdc0d756d1b2de35ebda83985aefe7111b21a1e2be45992f3a35e5f70528947f91f50d098571206
<b>ssdeep</b>	1536:iZBO9DuBAnQ2Vv4+BjVHxcTtBEIxyvO1URh+EhmGCpsWBMdc9dIM4bzd2U8EfwVB:uBOZuBUQwPjV+TciUvXh+NGMWU1J&
<b>Entropy</b>	5.978562

Antivirus

<b>Ahnlab</b>	Trojan/Win64.Manuscript
<b>Antiy</b>	Trojan[Backdoor]/Win32.Lazarus
<b>Avira</b>	TR/NukeSped.okrph
<b>BitDefender</b>	Gen:Variant.Cerbu.38929
<b>ClamAV</b>	Win.Trojan.GhostPuppet-7404648-0
<b>Cyren</b>	W64/Trojan.PWEO-6087
<b>ESET</b>	a variant of Win64/NukeSped.CA trojan
<b>Emsisoft</b>	Gen:Variant.Cerbu.38929 (B)
<b>Ikarus</b>	Trojan.Win64.Nukesped
<b>NANOAV</b>	Trojan.Win64.Lazarus.ftxgov
<b>Quick Heal</b>	Backdoor.Lazarus
<b>Symantec</b>	Trojan.Gen.MBT
<b>TrendMicro</b>	BKDR64_.DFFFEE3F
<b>TrendMicro House Call</b>	BKDR64_.DFFFEE3F
<b>Vir.IT eXplorer</b>	Backdoor.Win32.NukeSped.BH
<b>VirusBlokAda</b>	Backdoor.Lazarus
<b>Zillya!</b>	Trojan.NukeSped.Win64.41

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

**Compile Date** 2019-07-23 02:17:02-04:00

**Import Hash** 7712511643053a6d00be14bd064ba3b3

PE Sections

MD5	Name	Raw Size	Entropy
f5ce198af5d5f13f685bf5e7b4321e00	header	1024	2.998958
280ac4987654f06c9b59b6e73d406d0a	.text	66560	6.372604
20923d9916cc0109900b80bcb6f57c21	.rdata	40448	4.826823
fe894e926ee83c0a9904cd411cdef116	.data	2560	2.327005
5268ff6f51de87cfe39fd45f886ed02f	.pdata	4608	4.804507
6ca9b71152093220d3c5306c9ff4512d	.rsrc	2560	2.923477
aec7d049f3081bab81509c1da7ce4f5e	.reloc	2048	4.845016

Relationships

a1cdb78410... Connected\_To castorbyg.dk

a1cdb78410... Connected\_To matthias-dlugi.de

a1cdb78410... Connected\_To locphuland.com

Description

This file is a 64-bit DLL and has been identified as Variant C. Refer to A8B6EC51ED88C0329FD3329CB615BBC9 for analysis.

#### **castorbyg.dk**

Tags

command-and-control

URLs

castorbyg.dk/wp-content/themes/302.php

Relationships

castorbyg.dk Connected\_From a1cdb784100906d0ac895297c5a0959ab21a9fb39c687baf176324ee84095472

Description

0856655351ACFFA1EE459EEAAF164756 attempts to connect to the domain.

#### **matthias-dlugi.de**

Tags

command-and-control

URLs

matthias-dlugi.de/wp-content/themes/twentyfifteen/helper.php

Relationships

matthias-dlugi.de Connected\_From a1cdb784100906d0ac895297c5a0959ab21a9fb39c687baf176324ee84095472

Description

0856655351ACFFA1EE459EEAAF164756 attempts to connect to the domain.

#### **locphuland.com**

Tags

command-and-control

URLs

locphuland.com/wp-content/themes/hikma/total.php

Relationships

locphuland.com Connected\_From a1cdb784100906d0ac895297c5a0959ab21a9fb39c687baf176324ee84095472

Description

0856655351ACFFA1EE459EEEF164756 attempts to connect to the domain.

**b4bf6322c67a23553d5a9af6fcd9510eb613ffac963a21e32a9ced83132a09ba**

Tags

downloadertrojan

Details

<b>Name</b>	34C2AC6DAA44116713F882694B6B41E8
<b>Size</b>	413696 bytes
<b>Type</b>	PE32 executable (GUI) Intel 80386, for MS Windows
<b>MD5</b>	34c2ac6daa44116713f882694b6b41e8
<b>SHA1</b>	323258353c244b373c758906d88a2bf9663abf8d
<b>SHA256</b>	b4bf6322c67a23553d5a9af6fcd9510eb613ffac963a21e32a9ced83132a09ba
<b>SHA512</b>	5d4368d9de8c15b8b2945ad0aebf1bdc9c5e14dfc2927fb43d254f129675285278116ac9f32e0e3b11aeac10b488fa78c9c57ef1634a91
<b>ssdeep</b>	3072:rNXQoaFxes6EiH6Zq2dIvkapOztAzfb7zgnbtGfCDQomoRoYohoYoloodocoomn:rNXQoaFA6TdlvbxHFGfCDtoLb779qPb
<b>Entropy</b>	6.080481

Antivirus

<b>Ahnlab</b>	Win-Trojan/Akdoor.Gen
<b>Antiy</b>	Trojan/Win32.AGeneric
<b>Avira</b>	TR/Agent.413696.177
<b>BitDefender</b>	Trojan.GenericKD.6306955
<b>ESET</b>	a variant of Win32/NukeSped.AS trojan
<b>Emsisoft</b>	Trojan.GenericKD.6306955 (B)
<b>Ikarus</b>	Trojan.Win32.NukeSped
<b>Microsoft Security Essentials</b>	Trojan:Win32/FoggyBrass.A!dha
<b>NANOAV</b>	Trojan.Win32.Agent.dyiqsz
<b>Symantec</b>	Infostealer.Limitail
<b>TACHYON</b>	Trojan.GenericKD.2848758
<b>TrendMicro</b>	TROJ_FR.B20F0867
<b>TrendMicro House Call</b>	TROJ_FR.B20F0867
<b>VirusBlokAda</b>	BScope.Trojan.Downloader
<b>Zillya!</b>	Trojan.NukeSped.Win32.211

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

<b>Compile Date</b>	2015-10-26 02:49:15-04:00
<b>Import Hash</b>	286a6d2c70e3abce9178b4dde553be1e

PE Sections

<b>MD5</b>	<b>Name</b>	<b>Raw Size</b>	<b>Entropy</b>
f99d1ddfaa147735453ba03902858bdd	header	4096	0.707250

e43e40d71706646e57eaa4bab011f1fe	.text	90112	6.601261
6d16ccd8c4bf43898ce90a54570ee55f	.rdata	8192	4.923082
6b290555b2ac46d8971af1ecd979ebd2	.data	20480	2.478666
02a1e02ca134ced49ced1be22c562e26	.rsrc	290816	5.824422

Packers/Compilers/Cryptors

Microsoft Visual C++ v6.0

Description

This file is a 32-bit Windows executable and has been identified as Variant D. Variant D generates an HTTP POST request very similar to that of \ difference is the beacon string, this variant uses "t34kjfdla45l". Datagrams are encrypted with a combination of RC4 and differential XOR. The RC "0x0D06092A864886F70D01010105000382".

Screenshots

Ordinal	Description
0x2009	SystemInfo
0x2010	DrivesInfo
0x2011	DirectoryList
0x2012	RunCmd
0x2013	ZipGetFile
0x2014	PutFile
0x2016	CreateProcess
0x2017	CreateProcessAsUser
0x2019	ProcessList
0x2020	ProcessKill
0x2021	SecureDelete
0x2022	TestConnect
0x2023	ChangeDirectory
0x2027	Timestamp
0x2028	Disconnect
0x2029	Hibernate
0x2030	Uninstall
0x2031	GetConfig
0x2032	SetConfig
0x2033	DirListRecursive
0x2034	GetDiskFreeSpace
0x2037	KeepAlive
0x2038	Sleep
0x2039	GetSelfName

Figure 4 - Variant D contains the commands displayed in the table.

**134b082b418129ffa390fbee1568bd9510c54bfd0e6b1f36bc7b8f867e56283**

Details

<b>Name</b>	633BD738AE63B6CE9C2A48CBDDD15406
<b>Size</b>	110592 bytes
<b>Type</b>	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
<b>MD5</b>	633bd738ae63b6ce9c2a48cbddd15406
<b>SHA1</b>	9807eadca9016f843ee35426d06bf67860d9cc39
<b>SHA256</b>	134b082b418129ffa390fbee1568bd9510c54bfd0e6b1f36bc7b8f867e56283
<b>SHA512</b>	681c659813ab9e7dcccfe4b3f86dfcc69dc63976a78ef93bff745543501c8cdfac988e7cd4f07a1a00f7432be12203b4f77f716f62b21616ffc
<b>ssdeep</b>	3072:xZR0uR/ljCCvWYBra4YUzCbBAHFbEQP:xZm+GCW2m4YUzCbOv
<b>Entropy</b>	6.483560

Antivirus

## YARA Rules

```

rule CISA_10135536_06 : HiddenCobra rat
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10135536"
    Date = "2018-05-04"
    Actor = "HiddenCobra"
    Category = "Trojan RAT"
    Family = "BLINDINGCAN"
    Description = "Detects Trojan RAT"
    MD5_1 = "f9e6c35dbb62101498ec755152a8a67b"
    SHA256_1 = "1ee75106a9113b116c54e7a5954950065b809e0bb4dd0a91dc76f778508c7954"
    MD5_2 = "d742ba8cf5b24affdf77bc6869da0dc5"
    SHA256_2 = "7dce6f30e974ed97a3ed024d4c62350f9396310603e185a753b63a1f9a2d5799"
    MD5_3 = "aefcd8e98a231bccbc9b2c6d578fc8f3"
    SHA256_3 = "96721e13bae587c75618566111675dec2d61f9f5d16e173e69bb42ad7cb2dd8a"
    MD5_4 = "3a6b48871abff2a1ce4c89b08bc0b7d8"
    SHA256_4 = "f71d67659baf0569143874d5d1c5a4d655c7d296b2e86be1b8f931c2335c0cd3"
  strings:
    $s0 = { C7 45 EC 0D 06 09 2A C7 45 F0 86 48 86 F7 C7 45 F4 0D 01 01 01 C7 45 F8 05 00 03 82 }
    $s1 = { 50 4D 53 2A 2E 74 6D 70 }
    $s2 = { 79 67 60 3C 77 F9 BA 77 7A 56 1B 68 51 26 11 96 B7 98 71 39 82 B0 81 78 }
  condition:
    any of them
}

```

## ssdeep Matches

No matches found.

## PE Metadata

**Compile Date** 2018-02-05 01:51:48-05:00

**Import Hash** e323d4ef56b270402fb9e6c461542ad1

## PE Sections

MD5	Name	Raw Size	Entropy
1879db2bfe51d8e1aeef41777c2c97e3	header	1024	2.453253
af4b3b39e5faf6f61340622604f97a0e	.text	81920	6.635901
ddd311c7dca06e585757f426cb9178fc	.rdata	14848	5.124397
086be14d819327c4cb2eecb13da9bef4	.data	4608	3.602410
142b335625420f8ae2ec8fc51de0b6b2	.rsrc	512	5.112624
ec32cc24421e55461a5ad48fc96ff984	.reloc	7680	4.861507

## Packers/Compilers/Cryptors

Microsoft Visual C++ DLL \*sign by CodeRipper

## Description

This file is a 64-bit DLL and has been identified as Variant E. Variant E forgoes the multi-part HTTP POST request format of Variant D and instead POST body with four parameters of Base64 encoded data as displayed below:

--Begin HTTP POST format--

POST /<uri> HTTP/1.1

Connection: Keep-Alive

Cache-Control: no-cache

Content-Type: application/x-www-form-urlencoded

Accept: \*/\*

User-Agent: <obtained from ObtainUserAgentString otherwise: Mozilla/5.0 (Windows NT 6.1; WOW64) Chrome/28.0.1500.95 Safari/537.36>

Host: <domain>

Content-Length: <length>

id=<key><paramList>&<random\_1>=<sessionID>&<random\_2>=<fixedString>&<random\_3>=<datagram>

--End HTTP POST format--

The first parameter, 'id', will consist of two separate base64 encoded parts. The first part consists of nine randomly generated lower case characters for the first three parameters. The second part of the 'id' parameter is a colon delimited list of the other three parameter names encrypted with parameters are randomly selected from a list of 51 strings. The second parameter data is the session id. The third parameter data is a fixed string "T1B7D95256A2001E". When encrypting data from the first three parameters, the encryption starts "0xC00 bytes" into the RC4 key stream. The 1 the datagram to be sent. The datagram is encrypted in the same manner as Variant B Version 1.0 using a combination of RC4 and differential XO the additional layer of Base64 encoding.

Screenshots

Ordinal	Description
0x2009	SystemInfo
0x2010	DrivesInfo
0x2011	DirectoryList
0x2012	RunCmd
0x2013	ZipGetFile
0x2014	PutFile
0x2016	CreateProcess
0x2017	CreateProcessAsUser
0x2019	ProcessList
0x2020	ProcessKill
0x2021	SecureDelete
0x2022	TestConnect
0x2023	ChangeDirectory
0x2027	Timestamp
0x2028	Disconnect
0x2029	Hibernate
0x2030	Uninstall
0x2031	GetConfig
0x2032	SetConfig
0x2033	DirListRecursive
0x2034	GetDiskFreeSpace
0x2037	KeepAlive
0x2038	Sleep
0x2039	GetSelfName
0x2046	PutFileWithPadding
0x2047	KeepAlive
0x2048	CopyFile
0x2049	MoveFile
0x2050	DeleteFile

Figure 5 - Variant E contains the commands displayed in the table.

0a763da26a67cb2b09a3ae6e1ac07828065eb980e452ce7d3354347976038e7e

Tags

trojan

Details

<b>Name</b>	171B9135540F89BF727B690B9E587A4E
<b>Size</b>	1778176 bytes
<b>Type</b>	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
<b>MD5</b>	171b9135540f89bf727b690b9e587a4e
<b>SHA1</b>	930577d155c41ad843be09a5910a75160eb0eca9
<b>SHA256</b>	0a763da26a67cb2b09a3ae6e1ac07828065eb980e452ce7d3354347976038e7e
<b>SHA512</b>	811f9e5302b0a048d56fb54b70df2819c7219accf07c1f69f9d4c9342fbb4748017ae5acb3e3e8c6ab0d5c8c5660f9c0b542e06b306b96e
<b>ssdeep</b>	49152:Z689410GBsVASqabr4nrhKCJiX1zBj7Is:Z604zehqabr4hli1zBH
<b>Entropy</b>	7.951261

Antivirus

<b>Ahnlab</b>	Trojan/Win64.Agent
<b>Antiy</b>	Trojan/Win32.Agentb
<b>Avira</b>	TR/NukeSped.psxmr
<b>BitDefender</b>	Trojan.GenericKD.31831026



<b>ESET</b>	Win32/NukeSped.FL trojan
<b>Emsisoft</b>	Trojan.GenericKD.31831026 (B)
<b>Ikarus</b>	Trojan.Win32.NukeSped
<b>K7</b>	Trojan ( 0054ae921 )
<b>McAfee</b>	Generic Trojan.gv
<b>NANOAV</b>	Trojan.Win32.NukeSped.foyooc
<b>Symantec</b>	Trojan Horse
<b>TACHYON</b>	Trojan/W32.Agent.1778176.N
<b>TrendMicro</b>	TROJ_FR.FB1AA970
<b>TrendMicro House Call</b>	TROJ_FR.FB1AA970
<b>VirusBlokAda</b>	TScope.Malware-Cryptor.SB
<b>Zillya!</b>	Trojan.Agentb.Win32.22138

#### YARA Rules

No matches found.

#### ssdeep Matches

No matches found.

#### PE Metadata

**Compile Date** 2018-10-07 23:05:18-04:00

**Import Hash** baa93d47220682c04d92f7797d9224ce

#### PE Sections

MD5	Name	Raw Size	Entropy
9e19e7fb6309129d9cf0a01c4e736a05	header	4096	0.905647
4ea36d953ccdb30fb625e51136a26969		54272	7.980761
302d4b306fd7974ce2b980a88adb61b2	.rsrc	512	4.514680
59f642fe00bfca3c92c42b2cae802f8	.idata	512	1.308723
f69164b5fe72547bf86a52994b636858		512	0.256865
e45475d50cd89d8688e42771053c8632	bncavhpe	1717760	7.953161
3c91bb7f24d17b602cc359f5fe5d2322	psmxndys	512	3.597543

#### Relationships

0a763da26a... Connected\_To streamf.ru

0a763da26a... Connected\_To vinhsake.com

0a763da26a... Connected\_To bogorcenter.com

#### Description

This file is a 32-bit DLL and has been identified as Variant F. Variant F of the implant uses multi-part HTTP POST messages consisting of three parts: response code, and datagram, as outlined below:

```
--Begin HTTP POST format--
POST /<uri> HTTP/1.1
Content-Type: multipart/form-data; boundary=<boundaryString>
User-Agent: <obtained from ObtainUserAgentString>
Host: <domain>
Content-Length: <length>
Expect: 100-continue
Connection: Keep-Alive
```

```
--<boundaryString>
Content-Disposition: form-data; name="_webident_f"
<victimId>
--<boundaryString>
Content-Disposition: form-data; name="_webident_s"
<response code>
--<boundaryString>
Content-Disposition: form-data; name="file"; filename="<random>.dat"
Content-Type: octet-stream
<datagram>
--<boundaryString>
--End HTTP POST format--
```

Two additional User-Agent strings have been used by this version:

```
--Begin User-Agent strings--
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36
--End User-Agent strings--
```

Datagrams are encoded using a single byte XOR with the value "0xAA".

Screenshots

Ordinal	Description
0x02	Sleep
0x03	Disconnect
0x0B	SystemInfo
0x0C	KeepAlive
0x0E	GetConfig
0x0F	SetConfig
0x12	RunCmd
0x13	RunCmd
0x14	PutFile
0x15	GetFile
0x18	CreateProcess
0x19	CreateProcess

**Figure 6** - Variant F contains the commands displayed in the table.

### streamf.ru

Tags

command-and-control

URLs

streamf.ru/wp-content/index2.php

Relationships

streamf.ru Connected\_From 0a763da26a67cb2b09a3ae6e1ac07828065eb980e452ce7d3354347976038e7e

Description

171B9135540F89BF727B690B9E587A4E attempts to connect to the domain.

### vinhsake.com

Tags

command-and-control

URLs

vinhsake.com/wp-content/uploads/index2.php

Relationships

vinhsake.com Connected\_From 0a763da26a67cb2b09a3ae6e1ac07828065eb980e452ce7d3354347976038e7e

Description

171B9135540F89BF727B690B9E587A4E attempts to connect to the domain.

### bogorcenter.com

Tags

command-and-control

URLs

bogorcenter.com/wp-content/themes/index2.php

Relationships

bogorcenter.com Connected\_From 0a763da26a67cb2b09a3ae6e1ac07828065eb980e452ce7d3354347976038e7e

Description

171B9135540F89BF727B690B9E587A4E attempts to connect to the domain.

**1884ddc53ef66488ca8fc641b438895fcaada77c15210118465377c63223b3bc**

Tags

backdoortrojan

Details

<b>Name</b>	22F8D2A0C8D9B54A553FCA1B2393B266
<b>Size</b>	126976 bytes
<b>Type</b>	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
<b>MD5</b>	22f8d2a0c8d9b54a553fca1b2393b266
<b>SHA1</b>	08bacda419c5c663bd16374ee690e8822af74af0
<b>SHA256</b>	1884ddc53ef66488ca8fc641b438895fcaada77c15210118465377c63223b3bc
<b>SHA512</b>	0a51be4e9d4d95d4e511b97bdfa2aaec5db39388eedf17285922f6057ca171f55734c2e5e7d556a7d3655c6b01430bae045045644013
<b>ssdeep</b>	3072:hdnUhpSA9IybNLYhsmbjzwl3tFMHBNU:vnIUhpS85WsmbnKN
<b>Entropy</b>	6.417310

Antivirus

<b>Ahnlab</b>	Trojan/Win32.Agent
<b>Antiy</b>	Trojan[Backdoor]/Win32.Manuscript
<b>Avira</b>	BDS/Redcap.hcfxr
<b>BitDefender</b>	Trojan.GenericKD.33520232
<b>Cyren</b>	W32/Trojan.ITLW-8523
<b>ESET</b>	a variant of Generik.BTKBSHE trojan
<b>Emsisoft</b>	Trojan.GenericKD.33520232 (B)
<b>NANOAV</b>	Trojan.Win32.Manuscript.hepayr
<b>Quick Heal</b>	Backdoor.Manuscript
<b>TACHYON</b>	Trojan/W32.Agent.126976.DEL
<b>TrendMicro</b>	BKDR_NU.82E0FF6A
<b>TrendMicro House Call</b>	BKDR_NU.82E0FF6A
<b>VirusBlokAda</b>	Backdoor.Manuscript

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

<b>Compile Date</b>	2019-07-23 20:50:45-04:00
<b>Import Hash</b>	33ef573774873705ce44ec95183c2e0f

PE Sections

MD5	Name	Raw Size	Entropy
-----	------	----------	---------

49356d02c29028e4a4986d5770624266	header	1024	2.940664
0bd65b0788f3e6043c6aa53346e88a19	.text	87552	6.583271
a5be05b45ad3419c246cf21f9be20826	.rdata	27136	5.394968
2bc12ba81a6644ceb7fa81303444d333	.data	5120	1.183309
bfe346cfed24683b605f901394c8cf69	.gfids	512	1.429806
904005e1749dcd577a0be29a83ff9ce1	.rsrc	512	4.720823
2adefe9831125b0ab9459ad7733cb42e	.reloc	5120	6.468427

Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

Relationships

1884ddc53e... Connected\_To stokeinvestor.com

1884ddc53e... Connected\_To growthincone.com

1884ddc53e... Connected\_To inverstingpurpose.com

Description

This file is a 32-bit DLL and has been identified as Variant F. Refer to 171B9135540F89BF727B690B9E587A4E for analysis.

**stokeinvestor.com**

Tags

command-and-control

URLs

stokeinvestor.com/common.php

Relationships

stokeinvestor.com Connected\_From c24c322f4535def3f8d1579c39f2f9e323787d15b96e2ee457c38925effe2d39

stokeinvestor.com Connected\_From 1884ddc53ef66488ca8fc641b438895fcaada77c15210118465377c63223b3bc

Description

22F8D2A0C8D9B54A553FCA1B2393B266 and FDD55A38A45DE8AF6F8C34A33BAE11CB attempt to connect to the domain.

**growthincone.com**

Tags

command-and-control

URLs

growthincone.com/board.php

Relationships

growthincone.com Connected\_From c24c322f4535def3f8d1579c39f2f9e323787d15b96e2ee457c38925effe2d39

growthincone.com Connected\_From 1884ddc53ef66488ca8fc641b438895fcaada77c15210118465377c63223b3bc

Description

22F8D2A0C8D9B54A553FCA1B2393B266 and FDD55A38A45DE8AF6F8C34A33BAE11CB attempt to connect to the domain.

**inverstingpurpose.com**

Tags

command-and-control

URLs

inverstingpurpose.com/head.php

Relationships

inverstingpurpose.com Connected\_From c24c322f4535def3f8d1579c39f2f9e323787d15b96e2ee457c38925effe2d39

inverstingpurpose.com Connected\_From 1884ddc53ef66488ca8fc641b438895fcaada77c15210118465377c63223b3bc

Description

22F8D2A0C8D9B54A553FCA1B2393B266 and FDD55A38A45DE8AF6F8C34A33BAE11CB attempt to connect to the domain.

**c24c322f4535def3f8d1579c39f2f9e323787d15b96e2ee457c38925effe2d39**

Tags

backdoortrojan

Details

<b>Name</b>	FDD55A38A45DE8AF6F8C34A33BAE11CB
<b>Size</b>	141312 bytes
<b>Type</b>	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
<b>MD5</b>	fdd55a38a45de8af6f8c34a33bae11cb
<b>SHA1</b>	f2da56d6a565ade77d7ebb0c31eda99b415bcced
<b>SHA256</b>	c24c322f4535def3f8d1579c39f2f9e323787d15b96e2ee457c38925effe2d39
<b>SHA512</b>	f81e0cb975269483f43a35b10b8f01efe708453e675f3909585c1332d477bff69d47abc570563ac1cf8dcecc4133a702db6b0ab19548f3e
<b>ssdeep</b>	3072:RFoydrw7d4uA4LsuvitZmf5eXv91596YPG:PXG7d47wsOiXmfw1DG
<b>Entropy</b>	6.089052

Antivirus

<b>Ahnlab</b>	Trojan/Win64.Agent
<b>Antiy</b>	Trojan[Backdoor]/Win64.Manuscript
<b>BitDefender</b>	Trojan.GenericKD.32627436
<b>Cyren</b>	W64/Trojan.URTH-8310
<b>ESET</b>	a variant of Generik.CETMACQ trojan
<b>Emsisoft</b>	Trojan.GenericKD.32627436 (B)
<b>McAfee</b>	RDN/Generic BackDoor
<b>TACHYON</b>	Trojan/W64.Agent.141312.B
<b>TrendMicro</b>	BKDR64_.DFFFEE3F
<b>TrendMicro House Call</b>	BKDR64_.DFFFEE3F
<b>VirusBlokAda</b>	Backdoor.Win64.Manuscript

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

<b>Compile Date</b>	2019-07-23 20:49:41-04:00
<b>Import Hash</b>	f2da13bb8bffa45aa11aaf82d51d54b5

PE Sections

MD5	Name	Raw Size	Entropy
557352a095b601682822a48dfb6ff35e	header	1024	3.105520
8bb19f482bddce12c71f47569cf5c732	.text	84992	6.415516
a14c6a5866fe494ff5cfd42a0bb2d2c4	.rdata	41984	5.116442

d0c6f887dc794cc7c49bf38a5eba50ff	.data	5120	1.262987
aaed812597858a671260a72da7bcb794	.pdata	5120	4.872234
f0819a00354c53d2e35aa1fc5239ff49	.gfids	512	1.283686
85d6df69cd236ab12321a95d2a49aff1	.rsrc	512	4.720823
62de5951242abfc3312799424b9f0406	.reloc	2048	4.712047

#### Relationships

c24c322f45...	Connected_To	stokeinvestor.com
c24c322f45...	Connected_To	growthincone.com
c24c322f45...	Connected_To	inverstingpurpose.com

#### Description

This file is a 64-bit DLL and has been identified as Variant F. Refer to 171B9135540F89BF727B690B9E587A4E for analysis.

#### Relationship Summary

d8af45210b...	Connected_To	530hr.com
d8af45210b...	Connected_To	028xmz.com
d8af45210b...	Connected_To	168wangpi.com
530hr.com	Connected_From	d8af45210bf931bc5b03215ed30fb731e067e91f25eda02a404bd55169e3e3c3
530hr.com	Connected_From	7985af0a87780d27dc52c4f73c38de44e5ad477cb78b2e8e89708168fbc4a882
028xmz.com	Connected_From	d8af45210bf931bc5b03215ed30fb731e067e91f25eda02a404bd55169e3e3c3
028xmz.com	Connected_From	7985af0a87780d27dc52c4f73c38de44e5ad477cb78b2e8e89708168fbc4a882
168wangpi.com	Connected_From	d8af45210bf931bc5b03215ed30fb731e067e91f25eda02a404bd55169e3e3c3
168wangpi.com	Connected_From	7985af0a87780d27dc52c4f73c38de44e5ad477cb78b2e8e89708168fbc4a882
7985af0a87...	Connected_To	530hr.com
7985af0a87...	Connected_To	028xmz.com
7985af0a87...	Connected_To	168wangpi.com
e98991cdd9...	Connected_To	marmarademo.com
e98991cdd9...	Connected_To	33cow.com
e98991cdd9...	Connected_To	97nb.net
marmarademo.com	Connected_From	e98991cdd9ddd30adf490673c67a4f8241993f26810da09b52d8748c6160a292
33cow.com	Connected_From	e98991cdd9ddd30adf490673c67a4f8241993f26810da09b52d8748c6160a292
97nb.net	Connected_From	e98991cdd9ddd30adf490673c67a4f8241993f26810da09b52d8748c6160a292
4838f85499...	Connected_To	anlway.com
4838f85499...	Connected_To	apshenyihl.com
4838f85499...	Connected_To	ap8898.com
anlway.com	Connected_From	4838f85499e3c68415010d4f19e83e2c9e3f2302290138abe79c380754f97324
apshenyihl.com	Connected_From	4838f85499e3c68415010d4f19e83e2c9e3f2302290138abe79c380754f97324
ap8898.com	Connected_From	4838f85499e3c68415010d4f19e83e2c9e3f2302290138abe79c380754f97324
e76b3fd3e9...	Connected_To	aloe-china.com
e76b3fd3e9...	Connected_To	92myhw.com
e76b3fd3e9...	Connected_To	aisou123.com

aloe-china.com	Connected_From	e76b3fd3e906ac23218b1fbd66fd29c3945ee209a29e9462bbc46b07d1645de2
92myhw.com	Connected_From	e76b3fd3e906ac23218b1fbd66fd29c3945ee209a29e9462bbc46b07d1645de2
aisou123.com	Connected_From	e76b3fd3e906ac23218b1fbd66fd29c3945ee209a29e9462bbc46b07d1645de2
1faaa93908...	Connected_To	markcoprintandcopy.com
1faaa93908...	Connected_To	aedlifepower.com
1faaa93908...	Connected_To	919xy.com
markcoprintandcopy.com	Connected_From	1faaa939087c3479441d9f9c83a80ac7ec9b929e626cb34a7417be9ff0316ff7
aedlifepower.com	Connected_From	1faaa939087c3479441d9f9c83a80ac7ec9b929e626cb34a7417be9ff0316ff7
919xy.com	Connected_From	1faaa939087c3479441d9f9c83a80ac7ec9b929e626cb34a7417be9ff0316ff7
3ff4ebae6c...	Connected_To	pakteb.com
3ff4ebae6c...	Connected_To	nuokejs.com
3ff4ebae6c...	Connected_To	qdbazaar.com
pakteb.com	Connected_From	3ff4ebae6c255d4ae6b747a77f2821f2b619825c7789c7ee5338da5ecb375395
pakteb.com	Connected_From	c2f150dbe9a8efb72dc46416ca29acdbae6fd4a2af16b27f153eaabd4772a2a1
nuokejs.com	Connected_From	3ff4ebae6c255d4ae6b747a77f2821f2b619825c7789c7ee5338da5ecb375395
nuokejs.com	Connected_From	c2f150dbe9a8efb72dc46416ca29acdbae6fd4a2af16b27f153eaabd4772a2a1
qdbazaar.com	Connected_From	3ff4ebae6c255d4ae6b747a77f2821f2b619825c7789c7ee5338da5ecb375395
qdbazaar.com	Connected_From	c2f150dbe9a8efb72dc46416ca29acdbae6fd4a2af16b27f153eaabd4772a2a1
c2f150dbe9...	Connected_To	pakteb.com
c2f150dbe9...	Connected_To	nuokejs.com
c2f150dbe9...	Connected_To	qdbazaar.com
1678327c5f...	Connected_To	aurumgroup.co.id
1678327c5f...	Connected_To	51shousheng.com
1678327c5f...	Connected_To	new.titanik.fr
aurumgroup.co.id	Connected_From	1678327c5f36074cf5f18d1a92c2d9fea9bfae6c245eaad01640fd75af4d6c11
aurumgroup.co.id	Connected_From	c0ee19d7545f98fcd15725a3d9f0dbd0f35b2091e1c5b9cf4744f16e81a030c5
51shousheng.com	Connected_From	1678327c5f36074cf5f18d1a92c2d9fea9bfae6c245eaad01640fd75af4d6c11
51shousheng.com	Connected_From	c0ee19d7545f98fcd15725a3d9f0dbd0f35b2091e1c5b9cf4744f16e81a030c5
new.titanik.fr	Connected_From	1678327c5f36074cf5f18d1a92c2d9fea9bfae6c245eaad01640fd75af4d6c11
new.titanik.fr	Connected_From	c0ee19d7545f98fcd15725a3d9f0dbd0f35b2091e1c5b9cf4744f16e81a030c5
c0ee19d754...	Connected_To	aurumgroup.co.id
c0ee19d754...	Connected_To	51shousheng.com
c0ee19d754...	Connected_To	new.titanik.fr
9e4bd9676b...	Connected_To	duratransgroup.com
9e4bd9676b...	Connected_To	eygingenieros.com
9e4bd9676b...	Connected_To	eventum.cwsdev3.biz
duratransgroup.com	Connected_From	9e4bd9676bb3460be68ba4559a824940a393bde7613850eda9196259e453b9f3
eygingenieros.com	Connected_From	9e4bd9676bb3460be68ba4559a824940a393bde7613850eda9196259e453b9f3
eventum.cwsdev3.biz	Connected_From	9e4bd9676bb3460be68ba4559a824940a393bde7613850eda9196259e453b9f3
eee38c632c...	Connected_To	theinspectionconsultant.com

eee38c632c...	Connected_To	danagloverinteriors.com
eee38c632c...	Connected_To	as-brant.ru
theinspectionconsultant.com	Connected_From	f6e1a146543d2903146698da5698b2a214201720c0be756c6e8d2a2f27dcfaff
theinspectionconsultant.com	Connected_From	eee38c632c62ca95b5c66f8d39a18e23b9175845560af84b6a2f69b7f9b6ec1c
danagloverinteriors.com	Connected_From	f6e1a146543d2903146698da5698b2a214201720c0be756c6e8d2a2f27dcfaff
danagloverinteriors.com	Connected_From	eee38c632c62ca95b5c66f8d39a18e23b9175845560af84b6a2f69b7f9b6ec1c
as-brant.ru	Connected_From	f6e1a146543d2903146698da5698b2a214201720c0be756c6e8d2a2f27dcfaff
as-brant.ru	Connected_From	eee38c632c62ca95b5c66f8d39a18e23b9175845560af84b6a2f69b7f9b6ec1c
f6e1a14654...	Connected_To	theinspectionconsultant.com
f6e1a14654...	Connected_To	danagloverinteriors.com
f6e1a14654...	Connected_To	as-brant.ru
37bb27f4eb...	Connected_To	rxrenew.us
37bb27f4eb...	Connected_To	creativefishstudio.com
37bb27f4eb...	Connected_To	sensationalsecrets.com
rxrenew.us	Connected_From	e6fc788b5ff7436da4450191a003966a68e2a1913c83f1d3aec78c65f3ba85ca
rxrenew.us	Connected_From	37bb27f4eb40b8947e184afddba019001c12f97588e7f596ab6bc07f7c152602
creativefishstudio.com	Connected_From	e6fc788b5ff7436da4450191a003966a68e2a1913c83f1d3aec78c65f3ba85ca
creativefishstudio.com	Connected_From	37bb27f4eb40b8947e184afddba019001c12f97588e7f596ab6bc07f7c152602
sensationalsecrets.com	Connected_From	e6fc788b5ff7436da4450191a003966a68e2a1913c83f1d3aec78c65f3ba85ca
sensationalsecrets.com	Connected_From	37bb27f4eb40b8947e184afddba019001c12f97588e7f596ab6bc07f7c152602
e6fc788b5f...	Connected_To	rxrenew.us
e6fc788b5f...	Connected_To	creativefishstudio.com
e6fc788b5f...	Connected_To	sensationalsecrets.com
284bc47164...	Connected_To	rhythm86.com
284bc47164...	Connected_To	cabba-cacao.com
284bc47164...	Connected_To	3x-tv.com
rhythm86.com	Connected_From	284bc471647f951c79e3e333b2b19aa37f84cc39b55441a82e2a5f7319131fac
cabba-cacao.com	Connected_From	284bc471647f951c79e3e333b2b19aa37f84cc39b55441a82e2a5f7319131fac
3x-tv.com	Connected_From	284bc471647f951c79e3e333b2b19aa37f84cc39b55441a82e2a5f7319131fac
a1cdb78410...	Connected_To	castorbyg.dk
a1cdb78410...	Connected_To	matthias-dlugi.de
a1cdb78410...	Connected_To	locphuland.com
castorbyg.dk	Connected_From	a1cdb784100906d0ac895297c5a0959ab21a9fb39c687baf176324ee84095472
matthias-dlugi.de	Connected_From	a1cdb784100906d0ac895297c5a0959ab21a9fb39c687baf176324ee84095472
locphuland.com	Connected_From	a1cdb784100906d0ac895297c5a0959ab21a9fb39c687baf176324ee84095472
0a763da26a...	Connected_To	streamf.ru
0a763da26a...	Connected_To	vinhsake.com
0a763da26a...	Connected_To	bogorcenter.com
streamf.ru	Connected_From	0a763da26a67cb2b09a3ae6e1ac07828065eb980e452ce7d3354347976038e7e
vinhsake.com	Connected_From	0a763da26a67cb2b09a3ae6e1ac07828065eb980e452ce7d3354347976038e7e



bogorcenter.com	Connected_From	0a763da26a67cb2b09a3ae6e1ac07828065eb980e452ce7d3354347976038e7e
1884ddc53e...	Connected_To	stokeinvestor.com
1884ddc53e...	Connected_To	growthincone.com
1884ddc53e...	Connected_To	inverstingpurpose.com
stokeinvestor.com	Connected_From	c24c322f4535def3f8d1579c39f2f9e323787d15b96e2ee457c38925effe2d39
stokeinvestor.com	Connected_From	1884ddc53ef66488ca8fc641b438895fcaada77c15210118465377c63223b3bc
growthincone.com	Connected_From	c24c322f4535def3f8d1579c39f2f9e323787d15b96e2ee457c38925effe2d39
growthincone.com	Connected_From	1884ddc53ef66488ca8fc641b438895fcaada77c15210118465377c63223b3bc
inverstingpurpose.com	Connected_From	c24c322f4535def3f8d1579c39f2f9e323787d15b96e2ee457c38925effe2d39
inverstingpurpose.com	Connected_From	1884ddc53ef66488ca8fc641b438895fcaada77c15210118465377c63223b3bc
c24c322f45...	Connected_To	stokeinvestor.com
c24c322f45...	Connected_To	growthincone.com
c24c322f45...	Connected_To	inverstingpurpose.com

## Mitigation

Snort rules for this malware family is displayed below:

```

alert tcp any any -> any 80 (msg:"handshake detected"; content:"*dJU!*JE&IM@UNQ@"; sid:5; rev:1;)
alert tcp any any -> any 80 (msg:"handshake detected"; content:"t34kjfdla45!"; sid:6; rev:1;)
alert tcp any any -> any 80 (msg:"malware traffic detected"; content: "_webident_f"; http_client_body; content: "_webident_s "; http_client_body; s
alert tcp any any -> any 80 (msg:"malware traffic detected"; content: "_webident_f"; http_client_body; content: "_webident_s"; http_client_body; si

```

## Recommendations

CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organization. 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 necessary.
- 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 name).
- 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 800-151, **"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 <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 cases, 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 analysis. 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 [soc@us-cert.gov](mailto:soc@us-cert.gov) or 1-888-282-0870.

**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](mailto: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 Reporting forms can be found on CISA's homepage at [www.us-cert.gov](http://www.us-cert.gov).

## Revisions

---

May 12, 2020: Initial Version

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

### **Please share your thoughts.**

We recently updated our anonymous [product survey](#); we'd welcome your feedback.