ID: 586425
Sample Name: cANdLlHS4N
Cookbook: default.jbs
Time: 07:20:28
Date: 10/03/2022
Version: 34.0.0 Boulder Opal

Table of Contents

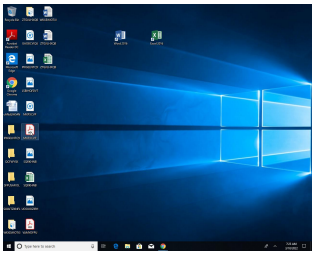
Windows Analysis Report

cANdLlHS4N

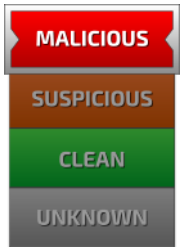
Overview

General Information

Sample Name:	cANdLlHS4N (renamed file extension from none to exe)
Analysis ID:	586425
MD5:	b3139b26a2dabb.
SHA1:	de5672c7940e4f..
SHA256:	5262cb9791df50..
Infos:	



Detection

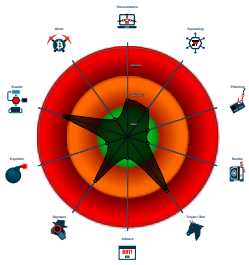


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Icon mismatch, binary includes an i…
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Submitted sample is a known malwa…
- Writes to foreign memory regions
- Contains functionality to start revers…
- Connects to many ports of the same…
- Allocates memory in foreign process…
- Contains functionality to detect slee…

Classification



Process Tree

- **System is w10x64**
- cANdLlHS4N.exe (PID: 6048 cmdline: "C:\Users\user\Desktop\cANdLlHS4N.exe" MD5: B3139B26A2DABB9B6E728884D8FA8B33)
  - obedience.exe (PID: 488 cmdline: C:\Users\user\AppData\Local\Temp\obedience.exe MD5: 6A1C14D5F16A07BEF55943134FE618C0)
    - iexplore.exe (PID: 5844 cmdline: C:\Program Files (x86)\Internet Explorer\iexplore.exe MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- obedience.exe (PID: 5080 cmdline: "C:\Users\user\AppData\Local\Temp\obedience.exe" MD5: 6A1C14D5F16A07BEF55943134FE618C0)
  - iexplore.exe (PID: 244 cmdline: C:\Program Files (x86)\Internet Explorer\iexplore.exe MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
cANdLlHS4N.exe	Dropper_DeploysMalwareViaSideLoading	Detect a dropper used to deploy an implant via side loading. This dropper has specifically been observed deploying REDLEAVES & PlugX	USG	• 0x135bf2:$UniqueString: 2E 6C 6E 6B 00 00 5C 00 00 00 61 76 70 75 69 2E 65 78 65 • 0x30f9:$PsuedoRandomStringGenerator: B9 1A 00 00 00 F7 F9 46 80 C2 41 88 54 35 8B 83 FE 64

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\handkerchief.dat	REDLEAVES_DroppedFile_ObfuscatedShellcodeAndRAT_handkerchief	Detect obfuscated .dat file containing shellcode and core REDLEAVES RAT	USG	• 0x38a81:$RedleavesStringObfu: 73 64 65 5E 60 74 75 74 6C 6F 60 6D 5E 6D 64 60 77 64 72 5E 65 6D 6D 6C 60 68 6F 2F 65 6D 6D
C:\Users\user\AppData\Local\Temp\handkerchief.dat	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x14c7:$xo1: Osrh;kit|izv;xzuuto;y~;inu;ru;_TH;vt\x7F~
C:\Users\user\AppData\Local\Temp\StarBurn.dll	REDLEAVES_DroppedFile_ImplantLoader_Starburn	Detect the DLL responsible for loading and deobfuscating the DAT file containing shellcode and core REDLEAVES RAT	USG	• 0x11d0:$XOR_Loop: 32 0C 3A 83 C2 02 88 0E 83 FA 08 7C F3 EB 12 BA 08 00 00 00 32 0C 3A 83 C2 02 88 0E 83 FA 10
C:\Users\user\AppData\Local\Temp\StarBurn.dll	OpCloudHopper_Malware_6	Detects malware from Operation Cloud Hopper	Florian Roth	• 0x17d3c:$s4: SOFTWARE\EGGORG

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.246163618.0000000002710000.00000004.00000800.00020000.00000000.sdmp	REDLEAVES_DroppedFile_ObfuscatedShellcodeAndRAT_handkerchief	Detect obfuscated .dat file containing shellcode and core REDLEAVES RAT	USG	• 0x38a81:$RedleavesStringObfu: 73 64 65 5E 60 74 75 74 6C 6F 60 6D 5E 6D 64 60 77 64 72 5E 65 6D 6D 6C 60 68 6F 2F 65 6D 6D
00000000.00000002.246163618.0000000002710000.00000004.00000800.00020000.00000000.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x14c7:$xo1: Osrh;kit|izv;xzuuto;y~;inu;ru;_TH;vt\x7F~
00000003.00000002.273655894.000000006EE51000.00000020.00000001.01000000.00000005.sdmp	REDLEAVES_DroppedFile_ImplantLoader_Starburn	Detect the DLL responsible for loading and deobfuscating the DAT file containing shellcode and core REDLEAVES RAT	USG	• 0xdd0:$XOR_Loop: 32 0C 3A 83 C2 02 88 0E 83 FA 08 7C F3 EB 12 BA 08 00 00 00 32 0C 3A 83 C2 02 88 0E 83 FA 10
00000001.00000002.248376246.000000006ED91000.00000020.00000001.01000000.00000005.sdmp	REDLEAVES_DroppedFile_ImplantLoader_Starburn	Detect the DLL responsible for loading and deobfuscating the DAT file containing shellcode and core REDLEAVES RAT	USG	• 0xdd0:$XOR_Loop: 32 0C 3A 83 C2 02 88 0E 83 FA 08 7C F3 EB 12 BA 08 00 00 00 32 0C 3A 83 C2 02 88 0E 83 FA 10
00000000.00000000.235573187.0000000000CA2000.00000008.00000001.01000000.00000003.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x6c46:$xo1: 6\x0A\x0B\x11B\x12\x10\x0D\x05\x10\x03\x0FB\x01\x03\x0C\x0C\x0D\x16B\x07B\x10\x17\x0CB\x0B\x0CB&-1B\x0F\x0D\x06\x07 • 0x28ccf:$xo1: Mqpj9ikv~kxt9zxwwvm9{|9klw9pw9]VJ9tv}|
Click to see the 37 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.cANdLIHS4N.exe.ca8bf8.1.unpack	REDLEAVES_DroppedFile_ImplantLoader_Starburn	Detect the DLL responsible for loading and deobfuscating the DAT file containing shellcode and core REDLEAVES RAT	USG	• 0x5d0:$XOR_Loop: 32 0C 3A 83 C2 02 88 0E 83 FA 08 7C F3 EB 12 BA 08 00 00 00 32 0C 3A 83 C2 02 88 0E 83 FA 10
0.2.cANdLIHS4N.exe.ca8bf8.1.unpack	OpCloudHopper_Malware_6	Detects malware from Operation Cloud Hopper	Florian Roth	• 0x16b3c:$s4: SOFTWARE\EGGORG
0.2.cANdLIHS4N.exe.26e0000.2.raw.unpack	REDLEAVES_DroppedFile_ImplantLoader_Starburn	Detect the DLL responsible for loading and deobfuscating the DAT file containing shellcode and core REDLEAVES RAT	USG	• 0x11d0:$XOR_Loop: 32 0C 3A 83 C2 02 88 0E 83 FA 08 7C F3 EB 12 BA 08 00 00 00 32 0C 3A 83 C2 02 88 0E 83 FA 10
0.2.cANdLIHS4N.exe.26e0000.2.raw.unpack	OpCloudHopper_Malware_6	Detects malware from Operation Cloud Hopper	Florian Roth	• 0x17d3c:$s4: SOFTWARE\EGGORG

Source	Rule	Description	Author	Strings
0.2.cANdLIHS4N.exe.26e0000.2.unpack	REDLEAVES_DroppedFile_ImplantLoader_Starburn	Detect the DLL responsible for loading and deobfuscating the DAT file containing shellcode and core REDLEAVES RAT	USG	• 0x5d0:$XOR_Loop: 32 0C 3A 83 C2 02 88 0E 83 FA 08 7C F3 EB 12 BA 08 00 00 00 32 0C 3A 83 C2 02 88 0E 83 FA 10
Click to see the 11 entries				

Sigma Signatures

There are no malicious signatures, click here to show all signatures.

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Networking

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Connects to many ports of the same IP (likely port scanning)

System Summary

Malicious sample detected (through community Yara rule)

Submitted sample is a known malware sample

Hooking and other Techniques for Hiding and Protection

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Malware Analysis System Evasion

Contains functionality to detect sleep reduction / modifications

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

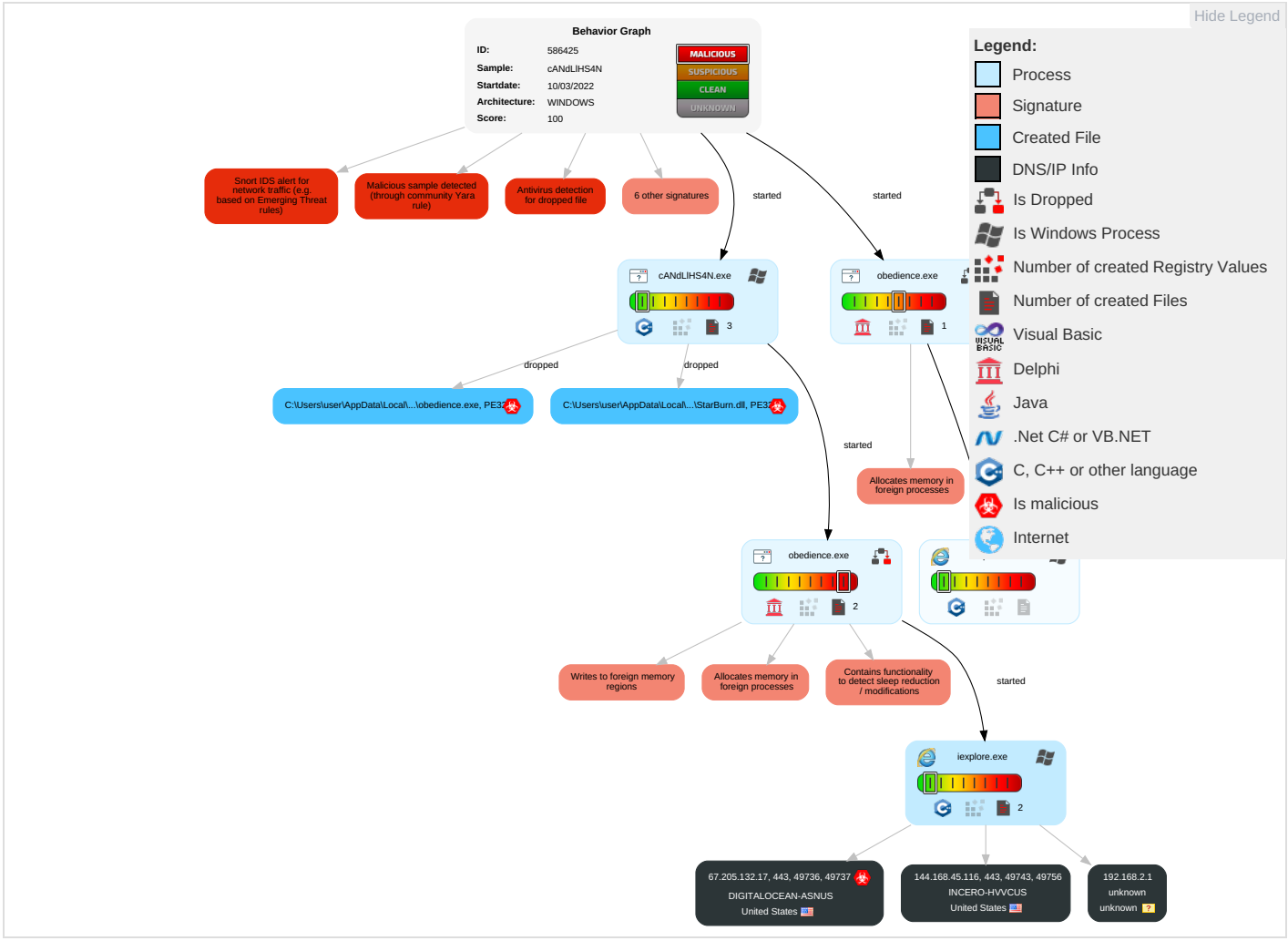
Remote Access Functionality

Contains functionality to start reverse TCP shell (cmd.exe)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Valid Accounts	2 Native API	1 Valid Accounts	1 Valid Accounts	1 Deobfuscate/Decode Files or Information	2 1 Input Capture	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Command and Scripting Interpreter	2 Registry Run Keys / Startup Folder	1 Access Token Manipulation	2 Obfuscated Files or Information	LSASS Memory	3 File and Directory Discovery	Remote Desktop Protocol	1 Screen Capture	Exfiltration Over Bluetooth	2 2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	2 1 2 Process Injection	1 Software Packing	Security Account Manager	3 5 System Information Discovery	SMB/Windows Admin Shares	2 1 Input Capture	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	2 Registry Run Keys / Startup Folder	1 1 Masquerading	NTDS	1 4 Security Software Discovery	Distributed Component Object Model	2 Clipboard Data	Scheduled Transfer	1 Remote Access Software	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Valid Accounts	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	1 Non-Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Access Token Manipulation	Cached Domain Credentials	1 1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	2 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 1 2 Process Injection	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

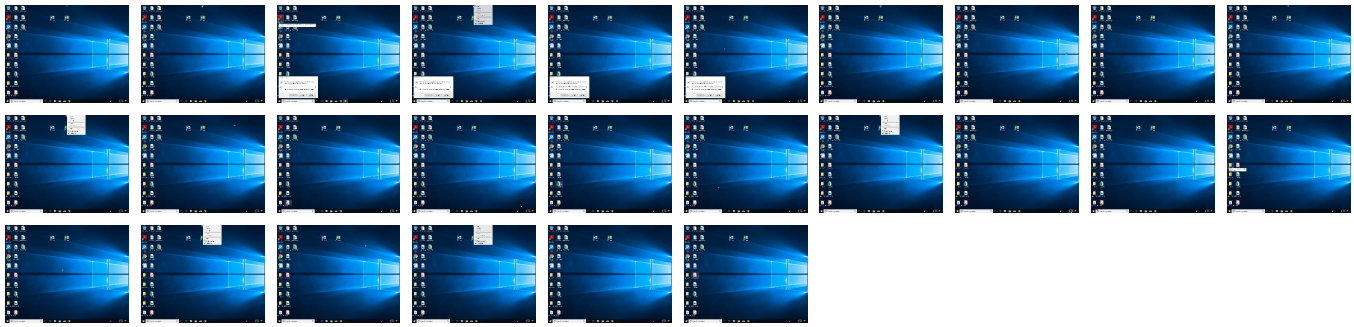
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
cANdLIHS4N.exe	78%	Virustotal		Browse
cANdLIHS4N.exe	65%	Metadefender		Browse
cANdLIHS4N.exe	84%	ReversingLabs	Win32.Dropper.RedLeaves	
cANdLIHS4N.exe	100%	Avira	TR/Korplug.dryww	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\StarBurn.dll	100%	Avira	HEUR/AGEN.1226539	
C:\Users\user\AppData\Local\Temp\obedience.exe	8%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\obedience.exe	9%	ReversingLabs	Win32.PUA.Tsingsoft	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.obedience.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1232827		Download File
3.2.obedience.exe.6ee50000.1.unpack	100%	Avira	HEUR/AGEN.1226539		Download File

Source	Detection	Scanner	Label	Link	Download
1.2.obedience.exe.6ed90000.1.unpack	100%	Avira	HEUR/AGEN.1226539		Download File
0.2.cANdLIHS4N.exe.2880000.3.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
1.2.obedience.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1232827		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://67.205.132.17:443	1%	Virustotal		Browse
http://67.205.132.17:443	0%	Avira URL Cloud	safe	
http://secure.globalsign.net/cacert/PrimObject.crt0	0%	URL Reputation	safe	
http://secure.globalsign.net/cacert/ObjectSign.crt09	0%	URL Reputation	safe	
http://www.globalsign.net/repository09	0%	URL Reputation	safe	
http://https://67.205.132.17:443/23I9/index.php	0%	Avira URL Cloud	safe	
http://https://67.205.132.17:443/NEZTI2/index.php	0%	Avira URL Cloud	safe	
http://https://67.205.132.17:443/hvnqlRD8z/index.php	0%	Avira URL Cloud	safe	
http://www.globalsign.net/repository/0	0%	URL Reputation	safe	
http://https://67.205.132.17:443/M2c1Nb/index.php	0%	Avira URL Cloud	safe	
http://https://67.205.132.17:443/3T3t/index.php	0%	Avira URL Cloud	safe	
http://www.globalsign.net/repository/03	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

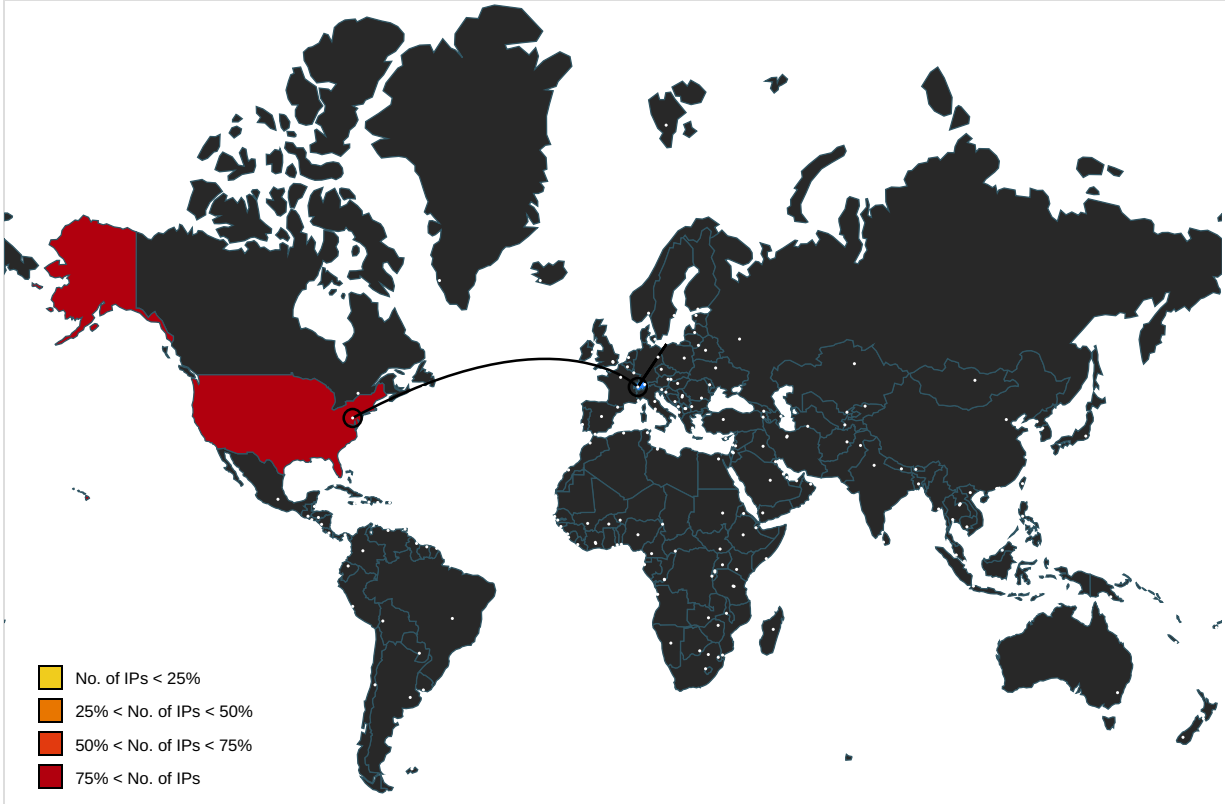
Name	Malicious	Antivirus Detection	Reputation
http://https://67.205.132.17:443/23I9/index.php	true	• Avira URL Cloud: safe	unknown
http://https://67.205.132.17:443/NEZTI2/index.php	true	• Avira URL Cloud: safe	unknown
http://https://67.205.132.17:443/hvnqlRD8z/index.php	true	• Avira URL Cloud: safe	unknown
http://https://67.205.132.17:443/M2c1Nb/index.php	true	• Avira URL Cloud: safe	unknown
http://https://67.205.132.17:443/3T3t/index.php	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://67.205.132.17:443	iexplore.exe, 00000002.00000002.50022467 6.0000000004C70000.00000004.00000020.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://secure.globalsign.net/cacert/PrimObject.crt0	cANdLIHS4N.exe, 00000000.00000002.246524283.00000000029EF000.00000004.00000800.00020000.00000000.sdmp, cANdLIHS4N.exe, 00000000.00000002.246010185.0000000000CA2000.00000004.00000001.01000000.00000003.sdmp, obedience.exe.0.dr	false	• URL Reputation: safe	unknown
http://secure.globalsign.net/cacert/ObjectSign.crt09	cANdLIHS4N.exe, 00000000.00000002.246524283.00000000029EF000.00000004.00000800.00020000.00000000.sdmp, cANdLIHS4N.exe, 00000000.00000002.246010185.0000000000CA2000.00000004.00000001.01000000.00000003.sdmp, obedience.exe.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.globalsign.net/repository09	cANdLlHS4N.exe, 00000000.00000002.246524283.00000000029EF000.00000004.00000800.00020000.00000000.sdmp, cANdLlHS4N.exe, 00000000.00000002.246010185.0000000000CA2000.00000004.00000001.01000000.00000003.sdmp, obedience.exe.0.dr	false	• URL Reputation: safe	unknown
http://www.audio-tool.net	cANdLlHS4N.exe, 00000000.00000002.246215033.0000000002880000.00000004.00000800.00020000.00000000.sdmp, cANdLlHS4N.exe, 00000000.00000002.245799041.0000000000B1E000.00000004.00000001.01000000.00000003.sdmp, obedience.exe, 00000001.00000002.247605132.000000000496000.00000002.00000001.01000000.00000004.sdmp, obedience.exe, 00000003.00000000.262529824.0000000000496000.00000002.00000001.01000000.00000004.sdmp, obedience.exe.0.dr	false		high
http://www.globalsign.net/repository/0	cANdLlHS4N.exe, 00000000.00000002.246524283.00000000029EF000.00000004.00000800.00020000.00000000.sdmp, cANdLlHS4N.exe, 00000000.00000002.246010185.0000000000CA2000.00000004.00000001.01000000.00000003.sdmp, obedience.exe.0.dr	false	• URL Reputation: safe	unknown
http://www.globalsign.net/repository/03	cANdLlHS4N.exe, 00000000.00000002.246524283.00000000029EF000.00000004.00000800.00020000.00000000.sdmp, cANdLlHS4N.exe, 00000000.00000002.246010185.0000000000CA2000.00000004.00000001.01000000.00000003.sdmp, obedience.exe.0.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
144.168.45.116	unknown	United States		54540	INCERO-HVVCUS	false
67.205.132.17	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	586425
Start date:	10.03.2022
Start time:	07:20:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	cANdLlHS4N (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/4@0/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 27.5% (good quality ratio 26.9%) • Quality average: 82.1% • Quality standard deviation: 23.5%
HCA Information:	• Successful, ratio: 87% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:21:35	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\persuasion.lnk

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\StarBurn.dll

Process:	C:\Users\user\Desktop\cANdLlHS4N.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	134244
Entropy (8bit):	6.439912486566814
Encrypted:	false
SSDEEP:	3072:JmeUE3TxGh4MwlW7AzD7Lcv4L2ZbDdlWG/4:Jm7EUhTwljDS4LevXWGg
MD5:	A03FFF06A20EE6943154481C883174A8
SHA1:	4470E24C366AD001ED6FE77B6A09C845D4EF6A86
SHA-256:	2F3C5A34E0483A5F1739AFAA3E893955F4D81869506A49F28F6A3AC944050900
SHA-512:	DCF944225471940C4C84F31A1409715EB1AE0B68AA1DA21ADCA23477D3C589D8D15213BAA3C105710D532190570C55492885E515220E3B18941096571A292A73
Malicious:	**true**
Yara Hits:	• Rule: REDLEAVES_DroppedFile_ImplantLoader_Starburn, Description: Detect the DLL responsible for loading and deobfuscating the DAT file containing shellcode and core REDLEAVES RAT, Source: C:\Users\user\AppData\Local\Temp\StarBurn.dll, Author: USG • Rule: OpCloudHopper_Malware_6, Description: Detects malware from Operation Cloud Hopper, Source: C:\Users\user\AppData\Local\Temp\StarBurn.dll, Author: Florian Roth
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U.^...0...0...0.~...<.0.~.....0.~...e.0.....0.....0...1.N.0.~.....0.~.....0.~.....0.Rich..0.....PE..L...\|..X.....!.....J.....u.....`.....p.....9.....@.....`...,.....x....0.....@..... .@.....`..\|.....text...xI.....J..... ..`.rdata..]....`.....N.....@..@.data...\7.....@....rsrc.....0.....@..@.reloc...#...@...$..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\handkerchief.dat

Process:	C:\Users\user\Desktop\cANdLlHS4N.exe
File Type:	data
Category:	dropped
Size (bytes):	254593
Entropy (8bit):	6.992551822422355
Encrypted:	false
SSDEEP:	6144:cMq9yyNTKrkgMEVAUtmEXlW+/xf8GQ6/Ta2QSirGf23YJKRluri9Zoqip3:Q9lNTokREm0mN+/uGQ6/O2orsKHt9Zo1
MD5:	FB0C714CD2EBDCC6F33817ABE7813C36
SHA1:	FC4F3698E768F690425523CDFD548B81D891C3B0
SHA-256:	773B176B3A68C3D21FAE907AF8FBA7908B55726BD591C5335C8C0BC9DE179B76
SHA-512:	65EF996A9A9BD47D50F7649C7895D000C943346B17385390B951691CEC07ED7AA487CA3225EE84022B67643F2A574E7DE8C18F81F2576F0BE92BD3930EE9FDC
Malicious:	false
Yara Hits:	• Rule: REDLEAVES_DroppedFile_ObfuscatedShellcodeAndRAT_handkerchief, Description: Detect obfuscated .dat file containing shellcode and core REDLEAVES RAT, Source: C:\Users\user\AppData\Local\Temp\handkerchief.dat, Author: USG • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: C:\Users\user\AppData\Local\Temp\handkerchief.dat, Author: Florian Roth

Reputation:	low
Preview:	0891@VR68D748062..D.....N.....HML.....^.{(....+....m..m..e.....o..-...n.E....f..\'.O.c..Q..A;..R./...\~oK".n.itxZ"].n..A?..}..P.A.....^.q.szibZsWryisWtz.OL..^...z.^.}..}.V .N.....N..^..^.V..V..^.....N..N.^.#.oD.V.V..N.....o..V....V...N.a.5.wwn..^.K.N.^....V.J.N.I.N.V._...N....N.^....^.V.V....N.0N.N.{0.^.....^.....R...n.z.^....^..^.....V.V.N.!.o$.^ .^..V.....o..^....^...V.N..O..^....^.V....V.N.N..^.0^.^.....N.....[...(.....}...+.....[...(..*....}.....7....../.....(..#.....?.....3.....c.. .....^.....g.....^.^.....(.....#.....s.....+...Kq..N.....c.....c.....c...c.....f...c....+.../H..c....+.....c.....c.....c...c.....f.....c.....c.....c.. .....c...c.....f.....c...c....+.....

C:\Users\user\AppData\Local\Temp\obedience.exe

Process:	C:\Users\user\Desktop\cANdLlHS4N.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1616040
Entropy (8bit):	7.373866112987865
Encrypted:	false
SSDEEP:	49152:fFdy58d2Bqc8Y7IDbauSVGDzhGjThGDzhmj8L5NsmCY:fFs58d2Bqc8Y7IDbauSVGDzhGjThGDzo
MD5:	6A1C14D5F16A07BEF55943134FE618C0
SHA1:	1A46E961BFFC6BCC1ADAC9708393462024F0F6AD
SHA-256:	ABA4DF64717462C61801D737C9FA20A7FADA61539EAEF50954331D31F7306D27
SHA-512:	07A8D9899CE04C4248CEBDFC105A37F3D8A337FF8F498F23853EDD05AC054DD99F976B13B2348660099C9135CE16A0876F7CFDF87E4B7139E88C27F9C598CF9
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 8%, Browse • Antivirus: ReversingLabs, Detection: 9%
Reputation:	low
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....@.....c,.....@.....`..$.....P..... .....CODE....$..... ..`DATA.....@...BSS.....idata.../.....0.....@....tls.....@.....rdata .....P.....@..P.reloc..$....`.....@..P.rsrc.....@..P.....@..P..... .....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\persuasion.lnk

Process:	C:\Users\user\AppData\Local\Temp\obedience.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Archive, ctime=Thu Mar 10 05:21:32 2022, mtime=Thu Mar 10 05:21:44 2022, atime=Thu Mar 10 05:21:32 2022, length=1616040, window=hide
Category:	dropped
Size (bytes):	1118
Entropy (8bit):	5.008588795039891
Encrypted:	false
SSDEEP:	24:8mrk3tHwNeRhHgKGUsAwZfaBJ9YC7aB6m:8mrk3tIeRhTrOaBJ9GB6
MD5:	D47E7BF51A9E2A6A44377FBC009DDB8D
SHA1:	4EF66D3777808262BD963A9188EF9C5D4B298AD9
SHA-256:	C755D52F273156F5C8F2D133260A8332C71FB8252398834379588949A8F8AE2D
SHA-512:	0CBA99F6751C04383823984474BF8A23DBD094BEAFE60B9E89BBFE4309822EC65C8E2306EA8D916056826D9A3EDE8691F4444FD7183C7C8A2DA0F14D5FE8D26 6
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....G4..k.I.G4.....G4.....:..DG..Yr?.D..U..k0.&...&.....-....$..2...hy.G4.....t...CFSF..1.....N....AppData...t.Y^...H.g.3..(....gVA.G..k... @.....N..jT.2.....Y.....yN|.A.p.p.D.a.t.a...B.P.1.....>Q.;..Local.<.....N..jT.2.....Y.....L.o.c.a.l.....N.1.....jT.2..Temp..:.....N..jT.2.....Y.....J..T.e .m.p.....h.2.....jT.2 .OBEDIE~1.EXE..L.....jT.2jT.2.....S.....$Z..o.b.e.d.i.e.n.c.e...e.x.e.....^.....-.....]..... '.....C:\Users\user\AppData\Local\Temp \obedience.exe..*.....\.....\.....\.....\.....\.....\.L.o.c.a.l.\.T.e.m.p.\.o.b.e.d.i.e.n.c.e...e.x.e.".C.:.\.U.s.e.r.s.\.j.o.n.e.s.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.....\....I.J.H..K..:...`.....X.. .....971342.....!a..%.H.VZAj....%$.....!a..%.H.VZAj....%$.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.349238472441651
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	cANdLlHS4N.exe
File size:	3804160

MD5:	b3139b26a2dabb9b6e728884d8fa8b33
SHA1:	de5672c7940e4fad3c8145ce9e8a5fcb1da0fcee
SHA256:	5262cb9791df50fafcb2fbd5f93226050b51efe400c2924eecba97b7ce437481
SHA512:	f6b857fdb4b393e9e80893d081c46471cb75a92289d53a8d457fe889eee46b7212c5188032aa24400da6e8ba56168716aeb3e48c77758b4fbb74817ba4b13951
SSDEEP:	98304:drzo0aM7e5O92nAv/tyE6peB1IY8CEueiSH0h292bNcx:pzo0S4yRY8tueiSUh1bCx
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a.....x\.....xL.....vA.....vu. [....vt.....vE.....vB.....Rich.....PE..L...M..X.....

File Icon

Icon Hash:	e4e4b2b2a4b4b4a4

Static PE Info

General

Entrypoint:	0x50cf91
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x58ACFA4D [Wed Feb 22 02:41:17 2017 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	c20231bee688c91a492f8eb02fe15604

Entrypoint Preview

Instruction
call 00007F907CA3EEFEh
jmp 00007F907CA34F0Eh
mov edi, edi
push ebp
mov ebp, esp
push ebx
mov ebx, dword ptr [ebp+08h]
cmp ebx, FFFFFFE0h
jnbe 00007F907CA350F1h
push esi
push edi
cmp dword ptr [00773A24h], 00000000h
jne 00007F907CA3509Ah
call 00007F907CA3E88Dh
push 0000001Eh
call 00007F907CA3E6D7h
push 000000FFh
call 00007F907CA34A3Fh
pop ecx
pop ecx
test ebx, ebx
je 00007F907CA35086h
mov eax, ebx

Instruction
jmp 00007F907CA35085h
xor eax, eax
inc eax
push eax
push 00000000h
push dword ptr [00773A24h]
call dword ptr [0053626Ch]
mov edi, eax
test edi, edi
jne 00007F907CA350A8h
push 0000000Ch
pop esi
cmp dword ptr [007742E8h], eax
je 00007F907CA3508Fh
push ebx
call 00007F907CA3E48Bh
pop ecx
test eax, eax
jne 00007F907CA3502Bh
jmp 00007F907CA35089h
call 00007F907CA35B82h
mov dword ptr [eax], esi
call 00007F907CA35B7Bh
mov dword ptr [eax], esi
mov eax, edi
pop edi
pop esi
jmp 00007F907CA35096h
push ebx
call 00007F907CA3E46Ah
pop ecx
call 00007F907CA35B67h
mov dword ptr [eax], 0000000Ch
xor eax, eax
pop ebx
pop ebp
ret
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push esi
mov esi, ecx
mov byte ptr [esi+0Ch], 00000000h
test eax, eax
jne 00007F907CA350E5h
call 00007F907CA3C2C2h
mov dword ptr [esi+08h], eax
mov ecx, dword ptr [eax+6Ch]
mov dword ptr [esi], ecx
mov ecx, dword ptr [eax+68h]
mov dword ptr [esi+04h], ecx
mov ecx, dword ptr [esi]
cmp ecx, dword ptr [00000000h]

Rich Headers

Programming Language:	• [C] VS2008 SP1 build 30729 • [ASM] VS2010 build 30319 • [C] VS2010 build 30319 • [C++] VS2010 build 30319 • [RES] VS2010 build 30319 • [IMP] VS2008 SP1 build 30729 • [LNK] VS2010 build 30319

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x179b14	0x168	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x376000	0x9c28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x380000	0x1bb70	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x160b10	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x136000	0x9d0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x134938	0x134a00	False	0.562648719117	data	6.53626347491	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x136000	0x47062	0x47200	False	0.270200598638	data	5.08185706308	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x17e000	0x1f7724	0x1f0200	False	0.373334258472	data	7.60576445986	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x376000	0x9c28	0x9e00	False	0.375247231013	data	5.1750982001	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x380000	0x2aa6e	0x2ac00	False	0.271872715643	data	5.04489445576	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x376f58	0x134	data	Chinese	China
RT_CURSOR	0x37708c	0xb4	data	Chinese	China
RT_CURSOR	0x377140	0x134	AmigaOS bitmap font	Chinese	China
RT_CURSOR	0x377274	0x134	data	Chinese	China
RT_CURSOR	0x3773a8	0x134	data	Chinese	China
RT_CURSOR	0x3774dc	0x134	data	Chinese	China
RT_CURSOR	0x377610	0x134	data	Chinese	China
RT_CURSOR	0x377744	0x134	data	Chinese	China
RT_CURSOR	0x377878	0x134	data	Chinese	China
RT_CURSOR	0x3779ac	0x134	data	Chinese	China
RT_CURSOR	0x377ae0	0x134	data	Chinese	China
RT_CURSOR	0x377c14	0x134	data	Chinese	China
RT_CURSOR	0x377d48	0x134	AmigaOS bitmap font	Chinese	China
RT_CURSOR	0x377e7c	0x134	data	Chinese	China
RT_CURSOR	0x377fb0	0x134	data	Chinese	China
RT_CURSOR	0x3780e4	0x134	data	Chinese	China
RT_BITMAP	0x378218	0xb8	data	Chinese	China
RT_BITMAP	0x3782d0	0x144	data	Chinese	China

Name	RVA	Size	Type	Language	Country
RT_ICON	0x378414	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 2290679807, next used block 8912767		
RT_ICON	0x3786fc	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x378824	0xea8	data		
RT_ICON	0x3796cc	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x379f74	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x37a4dc	0x25a8	data		
RT_ICON	0x37ca84	0x10a8	data		
RT_ICON	0x37db2c	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x37df94	0x2e8	data		
RT_ICON	0x37e27c	0x128	GLS_BINARY_LSB_FIRST		
RT_MENU	0x37e3a4	0x18c	data	Chinese	China
RT_DIALOG	0x37e530	0xd6	data		
RT_DIALOG	0x37e608	0xe2	data	Chinese	China
RT_DIALOG	0x37e6ec	0x34	data	Chinese	China
RT_STRING	0x37e720	0x2e	data		
RT_STRING	0x37e750	0x30	data		
RT_STRING	0x37e780	0x8e	data		
RT_STRING	0x37e810	0xc0	data		
RT_STRING	0x37e8d0	0x136	data		
RT_STRING	0x37ea08	0x3c	data		
RT_STRING	0x37ea44	0x60	data		
RT_STRING	0x37eaa4	0x54	data		
RT_STRING	0x37eaf8	0x3a	data		
RT_STRING	0x37eb34	0xa4	data		
RT_STRING	0x37ebd8	0x3e	data		
RT_STRING	0x37ec18	0x4e	data	Chinese	China
RT_STRING	0x37ec68	0x2c	data	Chinese	China
RT_STRING	0x37ec94	0x84	data	Chinese	China
RT_STRING	0x37ed18	0x1c4	data	Chinese	China
RT_STRING	0x37eedc	0x14e	data	Chinese	China
RT_STRING	0x37f02c	0x10e	data	Chinese	China
RT_STRING	0x37f13c	0x50	data	Chinese	China
RT_STRING	0x37f18c	0x44	data	Chinese	China
RT_STRING	0x37f1d0	0x68	data	Chinese	China
RT_STRING	0x37f238	0x1b2	data	Chinese	China
RT_STRING	0x37f3ec	0xf4	data	Chinese	China
RT_STRING	0x37f4e0	0x24	data	Chinese	China
RT_STRING	0x37f504	0x1a6	data	Chinese	China
RT_ACCELERATOR	0x37f6ac	0x68	data		
RT_GROUP_CURSOR	0x37f714	0x22	Lotus unknown worksheet or configuration, revision 0x2	Chinese	China
RT_GROUP_CURSOR	0x37f738	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x37f74c	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x37f760	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x37f774	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x37f788	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x37f79c	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x37f7b0	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x37f7c4	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x37f7d8	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China

Name	RVA	Size	Type	Language	Country
RT_GROUP_CURSOR	0x37f7ec	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x37f800	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x37f814	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x37f828	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_CURSOR	0x37f83c	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	China
RT_GROUP_ICON	0x37f850	0x76	data		
RT_GROUP_ICON	0x37f8c8	0x22	data		
RT_VERSION	0x37f8ec	0xdc	data		
RT_MANIFEST	0x37f9c8	0x25f	ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	LCMapStringW, GetTimeZoneInformation, WriteConsoleW, CompareStringW, IsValidLocale, CreateFileW, SetEnvironmentVariableA, GetStringTypeW, IsValidCodePage, GetEnvironmentStringsW, QueryPerformanceCounter, FreeEnvironmentStringsW, GetLocaleInfoW, GetConsoleMode, GetConsoleCP, GetStdHandle, SetHandleCount, HeapCreate, IsDebuggerPresent, SetUnhandledExceptionFilter, UnhandledExceptionFilter, TerminateProcess, IsProcessorFeaturePresent, GetFileType, SetStdHandle, GetSystemTimeAsFileTime, HeapSize, HeapQueryInformation, HeapReAlloc, VirtualQuery, GetSystemInfo, CreateThread, ExitThread, HeapAlloc, GetStartupInfoW, HeapSetInformation, GetCommandLineA, EncodePointer, DecodePointer, ExitProcess, RaiseException, RtlUnwind, HeapFree, FindResourceExW, SearchPathA, GetProfileIntA, InitializeCriticalSectionAndSpinCount, SetErrorMode, GetNumberFormatA, GetWindowsDirectoryA, GetFileSizeEx, LocalFileTimeToFileTime, GetFileAttributesExA, FileTimeToLocalFileTime, FileTimeToSystemTime, GetShortPathNameA, GetVolumeInformationA, FindFirstFileA, FindClose, GetCurrentProcess, DuplicateHandle, GetFileSize, SetEndOfFile, UnlockFile, LockFile, FlushFileBuffers, SetFilePointer, WriteFile, ReadFile, MoveFileA, CreateFileA, lstrcmpiA, GetThreadLocale, GetStringTypeExA, DeleteFileA, GetCurrentDirectoryA, GetACP, GetOEMCP, GetCPInfo, GetModuleFileNameW, ReleaseActCtx, CreateActCtxW, TlsFree, DeleteCriticalSection, LocalReAlloc, TlsSetValue, TlsAlloc, InitializeCriticalSection, GlobalHandle, GlobalReAlloc, EnterCriticalSection, TlsGetValue, LeaveCriticalSection, LocalAlloc, GlobalFlags, CopyFileA, GlobalSize, FormatMessageA, LocalFree, lstrlenW, MulDiv, GetDiskFreeSpaceA, GetFullPathNameA, GetTempFileNameA, GetFileTime, SetFileTime, ReplaceFileA, SystemTimeToFileTime, GetFileAttributesA, GetUserDefaultLCID, GlobalFree, GetPrivateProfileStringA, WritePrivateProfileStringA, GetPrivateProfileIntA, WaitForSingleObject, ResumeThread, SetThreadPriority, GetCurrentThread, GetUserDefaultUILanguage, ConvertDefaultLocale, GetSystemDefaultUILanguage, GetModuleFileNameA, GetLocaleInfoA, InterlockedExchange, lstrcmpA, GlobalAlloc, GetModuleHandleW, FindResourceA, FreeResource, GetCurrentThreadId, GlobalFindAtomA, GlobalDeleteAtom, GetVersionExA, FreeLibrary, CompareStringA, LoadLibraryW, lstrcmpW, GlobalLock, GlobalUnlock, GetCurrentProcessId, GetProcAddress, GetModuleHandleA, LoadLibraryA, lstrlenA, GlobalGetAtomNameA, GlobalAddAtomA, ActivateActCtx, DeactivateActCtx, SetLastError, FindResourceW, LoadResource, LockResource, SizeofResource, InterlockedDecrement, InterlockedIncrement, CreateMutexA, GetLastError, WideCharToMultiByte, GetTempPathA, CreateProcessA, GetTickCount, VirtualAlloc, lstrcpyA, lstrcatA, MultiByteToWideChar, Sleep, CreateToolhelp32Snapshot, Process32First, Process32Next, CloseHandle, EnumSystemLocalesA, VirtualProtect, GetProcessHeap

DLL	Import
USER32.dll	CharUpperA, KillTimer, SetTimer, UnionRect, SetParent, GetSystemMenu, DeleteMenu, IsRectEmpty, LoadCursorW, SetLayeredWindowAttributes, EnumDisplayMonitors, LoadCursorA, GetSysColorBrush, MapVirtualKeyA, GetKeyNameTextA, SystemParametersInfoA, GetSystemMetrics, GetMenuItemInfoA, InflateRect, RealChildWindowFromPoint, EndPaint, BeginPaint, GetWindowDC, ClientToScreen, GrayStringA, DrawTextExA, DrawTextA, TabbedTextOutA, FillRect, GetMenuStringA, AppendMenuA, InsertMenuA, RemoveMenu, GetDC, ReleaseDC, SetWindowContextHelpId, MapDialogRect, CreateDialogIndirectParamA, GetNextDlgTabItem, EndDialog, ShowOwnedPopups, GetMessageA, TranslateMessage, GetCursorPos, ValidateRect, PostQuitMessage, MoveWindow, SetWindowTextA, IsDialogMessageA, CheckDlgButton, SetMenuItemBitmaps, GetMenuCheckMarkDimensions, LoadBitmapW, ModifyMenuA, GetMenuState, EnableMenuItem, CheckMenuItem, RegisterWindowMessageA, LoadIconA, SendDlgItemMessageA, IsChild, SetWindowsHookExA, CallNextHookEx, GetClassLongA, SetPropA, GetPropA, RemovePropA, GetFocus, GetWindowTextLengthA, GetWindowTextA, GetForegroundWindow, DispatchMessageA, BeginDeferWindowPos, EndDeferWindowPos, GetTopWindow, DestroyWindow, UnhookWindowsHookEx, CloseClipboard, GetMessagePos, GetMonitorInfoA, MapWindowPoints, ScrollWindow, TrackPopupMenu, SetScrollRange, GetScrollRange, SetScrollPos, GetScrollPos, SetForegroundWindow, ShowScrollBar, MessageBoxA, CreateWindowExA, GetClassInfoExA, RegisterClassA, AdjustWindowRectEx, GetWindowRect, ScreenToClient, DeferWindowPos, GetScrollInfo, SetScrollInfo, SetWindowPlacement, GetWindowPlacement, DefWindowProcA, CallWindowProcA, GetClassNameA, GetSysColor, UnpackDDElParam, ReuseDDElParam, LoadMenuA, DestroyMenu, WinHelpA, SetWindowPos, LoadImageA, DestroyIcon, SetFocus, GetWindowThreadProcessId, GetActiveWindow, IsWindowEnabled, EqualRect, GetDlgItem, SetWindowLongA, GetDlgCtrlID, GetKeyState, LoadIconW, SetCursor, PeekMessageA, GetCapture, ReleaseCapture, SetClipboardData, OpenClipboard, GetUpdateRect, LoadAcceleratorsA, GetParent, UpdateWindow, EnableWindow, PtInRect, GetClientRect, FrameRect, SetActiveWindow, IsWindowVisible, IsIconic, SendMessageA, InsertMenuItemA, GetSubMenu, GetMenuItemID, GetMenuItemCount, CreatePopupMenu, GetClassInfoA, IntersectRect, OffsetRect, SetRectEmpty, CopyRect, GetMenu, GetLastActivePopup, LoadAcceleratorsW, LoadMenuW, CharNextA, CopyAcceleratorTableA, SetRect, GetWindowRgn, DestroyCursor, DrawIcon, SubtractRect, MapVirtualKeyExA, BringWindowToTop, PostMessageA, SetMenu, GetDesktopWindow, GetWindow, ShowWindow, GetWindowLongA, IsWindow, TranslateAcceleratorA, InvalidateRect, IsCharLowerA, GetDoubleClickTime, CharUpperBuffA, CopyIcon, LoadImageW, MonitorFromWindow, EmptyClipboard, IsClipboardFormatAvailable, SetMenuDefaultItem, WaitMessage, PostThreadMessageA, CreateMenu, IsMenu, UpdateLayeredWindow, MonitorFromPoint, InvalidateRgn, DrawMenuBar, DefMDIChildProcA, DefFrameProcA, RegisterClipboardFormatA, CopyImage, GetIconInfo, EnableScrollBar, HideCaret, InvertRect, GetMenuDefaultItem, LockWindowUpdate, SetCursorPos, CreateAcceleratorTableA, GetKeyboardState, GetKeyboardLayout, ToAsciiEx, DrawFocusRect, DrawFrameControl, DrawEdge, DrawIconEx, DrawStateA, SetClassLongA, GetAsyncKeyState, NotifyWinEvent, WindowFromPoint, DestroyAcceleratorTable, RedrawWindow, SetWindowRgn, IsZoomed, UnregisterClassA, MessageBeep, GetNextDlgGroupItem, GetMessageTime, SetCapture, TranslateMDISysAccel
GDI32.dll	GetLayout, SetLayout, DeleteObject, SelectClipRgn, CreateRectRgn, GetViewportExtEx, GetWindowExtEx, BitBlt, GetPixel, PtVisible, RectVisible, TextOutA, ExtTextOutA, Escape, SelectObject, SetViewportOrgEx, OffsetViewportOrgEx, SetViewportExtEx, ScaleViewportExtEx, SetWindowOrgEx, OffsetWindowOrgEx, SetWindowExtEx, ScaleWindowExtEx, ExtSelectClipRgn, DeleteDC, CreatePatternBrush, GetStockObject, SelectPalette, GetObjectType, CreatePen, CreateSolidBrush, CreateHatchBrush, GetTextExtentPoint32A, CreateRectRgnIndirect, PatBlt, CreateDIBitmap, GetTextMetricsA, EnumFontFamiliesA, GetTextCharsetInfo, CombineRgn, GetMapMode, DPtoLP, GetBkColor, GetTextColor, GetRgnBox, CreateDIBSection, CreateRoundRectRgn, CreatePolygonRgn, CreateEllipticRgn, Polyline, Polygon, CreatePalette, GetPaletteEntries, GetNearestPaletteIndex, RealizePalette, GetSystemPaletteEntries, OffsetRgn, SetDIBColorTable, StretchBlt, SetPixel, Rectangle, EnumFontFamiliesExA, LPtoDP, GetWindowOrgEx, GetViewportOrgEx, PtInRegion, FillRgn, FrameRgn, GetBoundsRect, ExtFloodFill, SetPaletteEntries, GetTextFaceA, SetPixelV, MoveToEx, SetTextAlign, LineTo, IntersectClipRect, ExcludeClipRect, GetClipBox, SetMapMode, SetROP2, SetPolyFillMode, SetBkMode, RestoreDC, SaveDC, CreateDCA, CopyMetaFileA, GetDeviceCaps, CreateFontIndirectA, CreateBitmap, GetObjectA, SetBkColor, SetTextColor, CreateCompatibleDC, SetRectRgn, Ellipse, CreateCompatibleBitmap
MSIMG32.dll	AlphaBlend, TransparentBlt
COMDLG32.dll	GetFileTitleA
WINSPOOL.DRV	OpenPrinterA, DocumentPropertiesA, ClosePrinter
ADVAPI32.dll	RegEnumValueA, RegQueryValueExA, RegOpenKeyExA, RegCreateKeyExA, RegSetValueExA, RegDeleteValueA, RegDeleteKeyA, RegEnumKeyA, RegQueryValueA, RegEnumKeyExA, RegOpenKeyExW, RegCloseKey, RegSetValueA, GetFileSecurityA, SetFileSecurityA
SHELL32.dll	SHAppBarMessage, ShellExecuteA, DragFinish, DragQueryFileA, SHAddToRecentDocs, ExtractIconA, SHBrowseForFolderA, SHGetSpecialFolderPathA, SHGetSpecialFolderLocation, SHGetPathFromIDListA, SHGetDesktopFolder, SHGetFileInfoA
COMCTL32.dll	ImageList_GetIconSize
SHLWAPI.dll	PathFindFileNameA, PathStripToRootA, PathIsUNCA, PathFindExtensionA, PathRemoveFileSpecW
ole32.dll	OleIsCurrentClipboard, OleLockRunning, IsAccelerator, OleTranslateAccelerator, OleDestroyMenuDescriptor, OleCreateMenuDescriptor, OleInitialize, CoFreeUnusedLibraries, OleUninitialize, CoInitializeEx, CreateStreamOnHGlobal, CreateILockBytesOnHGlobal, StgCreateDocfileOnILockBytes, CoGetClassObject, OleFlushClipboard, OleDuplicateData, ReleaseStgMedium, StringFromCLSID, CoTaskMemFree, CoTaskMemAlloc, CLSIDFromString, CoCreateGuid, CLSIDFromProgID, CoInitialize, CoCreateInstance, CoUninitialize, DoDragDrop, RevokeDragDrop, CoLockObjectExternal, RegisterDragDrop, OleGetClipboard, CoRegisterMessageFilter, CoRevokeClassObject, StgOpenStorageOnILockBytes
OLEAUT32.dll	SysStringLen, OleCreateFontIndirect, VariantTimeToSystemTime, SystemTimeToVariantTime, SafeArrayDestroy, VariantCopy, VarBstrFromDate, SysAllocStringByteLen, SysFreeString, VariantChangeType, SysAllocStringLen, VariantInit, VariantClear, SysAllocString
oledlg.dll	
OLEACC.dll	AccessibleObjectFromWindow, CreateStdAccessibleObject, LresultFromObject
gdiplus.dll	GdipGetImageGraphicsContext, GdipBitmapUnlockBits, GdipBitmapLockBits, GdipCreateBitmapFromScan0, GdipCreateBitmapFromStream, GdipGetImagePalette, GdipGetImagePaletteSize, GdipGetImagePixelFormat, GdipGetImageHeight, GdipGetImageWidth, GdipCloneImage, GdipDrawImageRectI, GdipSetInterpolationMode, GdipCreateFromHDC, GdiplusShutdown, GdiplusStartup, GdipCreateBitmapFromHBITMAP, GdipDisposeImage, GdipDeleteGraphics, GdipAlloc, GdipFree, GdipDrawImageI

DLL	Import
IMM32.dll	ImmReleaseContext, ImmGetContext, ImmGetOpenStatus
WINMM.dll	PlaySoundA

Version Infos

Description	Data
Translation	0x0009 0x04b0

Possible Origin

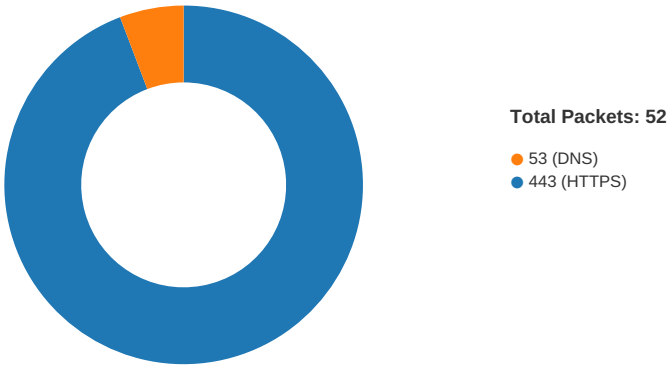
Language of compilation system	Country where language is spoken	Map
Chinese	China	
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
03/10/22-07:23:02.013122	TCP	2024173	ET TROJAN Red Leaves magic packet detected (APT10 implant)	49764	80	192.168.2.4	67.205.132.17

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 10, 2022 07:21:37.608027935 CET	49736	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:37.608115911 CET	443	49736	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:37.608268023 CET	49736	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:37.608624935 CET	49736	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:37.608640909 CET	443	49736	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:37.608659029 CET	49736	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:37.608669996 CET	443	49736	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:37.608793974 CET	443	49736	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:42.973103046 CET	49737	443	192.168.2.4	67.205.132.17

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 10, 2022 07:21:42.973156929 CET	443	49737	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:42.973328114 CET	49737	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:42.974839926 CET	49737	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:42.974857092 CET	443	49737	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:42.974925041 CET	443	49737	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:42.974950075 CET	49737	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:42.974972963 CET	443	49737	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:42.976782084 CET	49738	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:42.976818085 CET	443	49738	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:42.976900101 CET	49738	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:42.977200031 CET	49738	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:42.977219105 CET	443	49738	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:42.977279902 CET	49738	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:42.977293015 CET	443	49738	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:42.977401018 CET	443	49738	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:42.992253065 CET	49739	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:42.992326021 CET	443	49739	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:42.992415905 CET	49739	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:42.993453026 CET	49739	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:42.993479013 CET	443	49739	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:42.993547916 CET	443	49739	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:42.995389938 CET	49740	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:42.995440960 CET	443	49740	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:42.995537996 CET	49740	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:42.995886087 CET	49740	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:42.995913029 CET	443	49740	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:42.995955944 CET	443	49740	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:42.995991945 CET	49740	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:42.996011972 CET	443	49740	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:42.997436047 CET	49741	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:42.997484922 CET	443	49741	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:42.998003960 CET	49741	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:42.998060942 CET	49741	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:42.998078108 CET	443	49741	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:42.998094082 CET	49741	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:21:42.998102903 CET	443	49741	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:42.998209000 CET	443	49741	67.205.132.17	192.168.2.4
Mar 10, 2022 07:21:53.106363058 CET	49743	443	192.168.2.4	144.168.45.116
Mar 10, 2022 07:21:53.106456041 CET	443	49743	144.168.45.116	192.168.2.4
Mar 10, 2022 07:21:53.106570959 CET	49743	443	192.168.2.4	144.168.45.116
Mar 10, 2022 07:21:53.108678102 CET	49743	443	192.168.2.4	144.168.45.116
Mar 10, 2022 07:21:53.108748913 CET	443	49743	144.168.45.116	192.168.2.4
Mar 10, 2022 07:21:53.108772039 CET	49743	443	192.168.2.4	144.168.45.116
Mar 10, 2022 07:21:53.108789921 CET	443	49743	144.168.45.116	192.168.2.4
Mar 10, 2022 07:21:53.108952999 CET	443	49743	144.168.45.116	192.168.2.4
Mar 10, 2022 07:22:03.153788090 CET	49746	53	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:06.168540955 CET	49746	53	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:12.184732914 CET	49746	53	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:12.366229057 CET	49747	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:12.366271973 CET	443	49747	67.205.132.17	192.168.2.4
Mar 10, 2022 07:22:12.366451979 CET	49747	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:12.366818905 CET	49747	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:12.366833925 CET	443	49747	67.205.132.17	192.168.2.4
Mar 10, 2022 07:22:12.366939068 CET	443	49747	67.205.132.17	192.168.2.4
Mar 10, 2022 07:22:12.368575096 CET	49748	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:12.368624926 CET	443	49748	67.205.132.17	192.168.2.4
Mar 10, 2022 07:22:12.368717909 CET	49748	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:12.369051933 CET	49748	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:12.369082928 CET	443	49748	67.205.132.17	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 10, 2022 07:22:12.369129896 CET	443	49748	67.205.132.17	192.168.2.4
Mar 10, 2022 07:22:12.369153023 CET	49748	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:12.369174957 CET	443	49748	67.205.132.17	192.168.2.4
Mar 10, 2022 07:22:12.370532990 CET	49749	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:12.370563984 CET	443	49749	67.205.132.17	192.168.2.4
Mar 10, 2022 07:22:12.370745897 CET	49749	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:12.372329950 CET	49749	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:12.372349024 CET	443	49749	67.205.132.17	192.168.2.4
Mar 10, 2022 07:22:12.372400045 CET	443	49749	67.205.132.17	192.168.2.4
Mar 10, 2022 07:22:12.372473955 CET	49749	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:12.372488022 CET	443	49749	67.205.132.17	192.168.2.4
Mar 10, 2022 07:22:12.374878883 CET	49750	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:12.374902964 CET	443	49750	67.205.132.17	192.168.2.4
Mar 10, 2022 07:22:12.374969959 CET	49750	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:12.375251055 CET	49750	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:12.375267029 CET	443	49750	67.205.132.17	192.168.2.4
Mar 10, 2022 07:22:12.375308990 CET	443	49750	67.205.132.17	192.168.2.4
Mar 10, 2022 07:22:12.375382900 CET	49750	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:12.375394106 CET	443	49750	67.205.132.17	192.168.2.4
Mar 10, 2022 07:22:12.396006107 CET	49751	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:12.396064997 CET	443	49751	67.205.132.17	192.168.2.4
Mar 10, 2022 07:22:12.396150112 CET	49751	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:12.396461010 CET	49751	443	192.168.2.4	67.205.132.17
Mar 10, 2022 07:22:12.396492958 CET	443	49751	67.205.132.17	192.168.2.4
Mar 10, 2022 07:22:12.396565914 CET	443	49751	67.205.132.17	192.168.2.4
Mar 10, 2022 07:22:22.436521053 CET	49756	443	192.168.2.4	144.168.45.116
Mar 10, 2022 07:22:22.436614990 CET	443	49756	144.168.45.116	192.168.2.4
Mar 10, 2022 07:22:22.436717033 CET	49756	443	192.168.2.4	144.168.45.116
Mar 10, 2022 07:22:22.437103033 CET	49756	443	192.168.2.4	144.168.45.116
Mar 10, 2022 07:22:22.437125921 CET	443	49756	144.168.45.116	192.168.2.4
Mar 10, 2022 07:22:22.437145948 CET	49756	443	192.168.2.4	144.168.45.116
Mar 10, 2022 07:22:22.437156916 CET	443	49756	144.168.45.116	192.168.2.4

HTTP Request Dependency Graph

- 67.205.132.17:443

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49737	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:21:42.974839926 CET	838	OUT	POST /NEZTI2/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49738	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:21:42.977200031 CET	838	OUT	POST /NEZTl2/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49758	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:22:41.757384062 CET	1124	OUT	POST /hvnqlRD8z/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49759	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:22:41.760591984 CET	1125	OUT	POST /hvnqlRD8z/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49760	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:22:41.762743950 CET	1126	OUT	POST /hvnqlRD8z/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49761	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:22:41.764647961 CET	1126	OUT	POST /hvnqlRD8z/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49762	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:22:41.821583033 CET	1127	OUT	POST /hvnqlRD8z/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.4	49764	67.205.132.17	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:23:02.116496086 CET	1129	IN	HTTP/1.1 400 Bad Request Server: nginx Date: Thu, 10 Mar 2022 06:23:02 GMT Content-Type: text/html Content-Length: 150 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>400 Bad Request</title></head><body> 400 Bad Request <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.4	49765	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:23:07.487189054 CET	1129	OUT	POST /23l9/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.4	49766	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:23:07.489439964 CET	1130	OUT	POST /23l9/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.4	49767	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:23:07.491816044 CET	1131	OUT	POST /23l9/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.4	49768	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:23:07.497479916 CET	1131	OUT	POST /23l9/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49739	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:21:42.993453026 CET	839	OUT	POST /NEZTl2/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.4	49769	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:23:07.508974075 CET	1132	OUT	POST /23I9/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.4	49772	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:23:32.738704920 CET	1135	OUT	POST /M2c1Nb/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.4	49773	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:23:32.745321989 CET	1136	OUT	POST /M2c1Nb/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.4	49774	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:23:32.748333931 CET	1136	OUT	POST /M2c1Nb/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.4	49775	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:23:32.760200977 CET	1137	OUT	POST /M2c1Nb/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.4	49776	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:23:32.765038967 CET	1138	OUT	POST /M2c1Nb/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49740	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:21:42.995886087 CET	840	OUT	POST /NEZTl2/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49741	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:21:42.998060942 CET	840	OUT	POST /NEZTl2/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49747	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:22:12.366818905 CET	1112	OUT	POST /3T3t/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49748	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:22:12.369051933 CET	1112	OUT	POST /3T3t/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49749	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:22:12.372329950 CET	1113	OUT	POST /3T3t/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49750	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

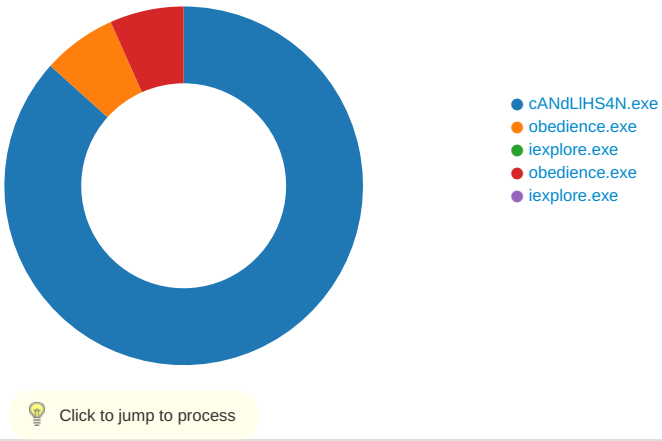
Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:22:12.375251055 CET	1114	OUT	POST /3T3t/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49751	67.205.132.17	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 10, 2022 07:22:12.396461010 CET	1114	OUT	POST /3T3t/index.php HTTP/1.1 Connection: Keep-Alive Accept: */* Content-Length: 133 Host: 67.205.132.17:443

Statistics

Behavior



System Behavior

Analysis Process: cANdLlHS4N.exe PID: **6048**, Parent PID: **1796**

General

Target ID:	0
Start time:	07:21:31
Start date:	10/03/2022
Path:	C:\Users\user\Desktop\cANdLlHS4N.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\cANdLlHS4N.exe"
Imagebase:	0x9a0000
File size:	3804160 bytes
MD5 hash:	B3139B26A2DABB9B6E728884D8FA8B33
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: REDLEAVES_DroppedFile_ObfuscatedShellcodeAndRAT_handkerchief, Description: Detect obfuscated .dat file containing shellcode and core REDLEAVES RAT, Source: 00000000.00000002.246163618.0000000002710000.00000004.00000800.00020000.00000000.sdmp, Author: USG • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000000.00000002.246163618.0000000002710000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000000.00000000.235573187.0000000000CA2000.00000008.00000001.01000000.00000003.sdmp, Author: Florian Roth • Rule: Dropper_DeploysMalwareViaSideLoading, Description: Detect a dropper used to deploy an implant via side loading. This dropper has specifically been observed deploying REDLEAVES & PlugX, Source: 00000000.00000002.245756146.0000000000AD6000.00000002.00000001.01000000.00000003.sdmp, Author: USG • Rule: REDLEAVES_DroppedFile_ImplantLoader_Starburn, Description: Detect the DLL responsible for loading and deobfuscating the DAT file containing shellcode and core REDLEAVES RAT, Source: 00000000.00000002.246143559.00000000026E0000.00000004.00000800.00020000.00000000.sdmp, Author: USG • Rule: OpCloudHopper_Malware_6, Description: Detects malware from Operation Cloud Hopper, Source: 00000000.00000002.246143559.00000000026E0000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: Dropper_DeploysMalwareViaSideLoading, Description: Detect a dropper used to deploy an implant via side loading. This dropper has specifically been observed deploying REDLEAVES & PlugX, Source: 00000000.00000000.235322946.0000000000AD6000.00000002.00000001.01000000.00000003.sdmp, Author: USG • Rule: Dropper_DeploysMalwareViaSideLoading, Description: Detect a dropper used to deploy an implant via side loading. This dropper has specifically been observed deploying REDLEAVES & PlugX, Source: 00000000.00000002.245504697.00000000009A1000.00000020.00000001.01000000.00000003.sdmp, Author: USG • Rule: REDLEAVES_DroppedFile_ImplantLoader_Starburn, Description: Detect the DLL responsible for loading and deobfuscating the DAT file containing shellcode and core REDLEAVES RAT, Source: 00000000.00000002.246010185.0000000000CA2000.00000004.00000001.01000000.00000003.sdmp, Author: USG • Rule: REDLEAVES_DroppedFile_ObfuscatedShellcodeAndRAT_handkerchief, Description: Detect obfuscated .dat file containing shellcode and core REDLEAVES RAT, Source: 00000000.00000002.246010185.0000000000CA2000.00000004.00000001.01000000.00000003.sdmp, Author: USG • Rule: Dropper_DeploysMalwareViaSideLoading, Description: Detect a dropper used to deploy an implant via side loading. This dropper has specifically been observed deploying REDLEAVES & PlugX, Source: 00000000.00000000.235102933.00000000009A1000.00000020.00000001.01000000.00000003.sdmp, Author: USG
Reputation:	low

File Activities

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications	success or wait	1	9B33A9	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\Triple	success or wait	1	9B33D4	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\Triple\Recent File List	success or wait	1	9B3442	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\Triple\Settings	success or wait	1	9B3442	RegCreateKeyExA

Analysis Process: obedience.exe PID: **488**, Parent PID: **6048**

General

Target ID:	1
Start time:	07:21:33
Start date:	10/03/2022
Path:	C:\Users\user\AppData\Local\Temp\obedience.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\obedience.exe

Imagebase:	0x400000
File size:	1616040 bytes
MD5 hash:	6A1C14D5F16A07BEF55943134FE618C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: REDLEAVES_DroppedFile_ImplantLoader_Starburn, Description: Detect the DLL responsible for loading and deobfuscating the DAT file containing shellcode and core REDLEAVES RAT, Source: 00000001.00000002.248376246.000000006ED91000.00000020.00000001.01000000.00000005.sdmp, Author: USG • Rule: REDLEAVES_CoreImplant_UniqueStrings, Description: Strings identifying the core REDLEAVES RAT in its deobfuscated state, Source: 00000001.00000002.248128854.0000000002580000.00000040.00000800.00020000.00000000.sdmp, Author: USG • Rule: malware_red_leaves_generic, Description: Red Leaves malware, related to APT10, Source: 00000001.00000002.248128854.0000000002580000.00000040.00000800.00020000.00000000.sdmp, Author: David Cannings • Rule: RedLeaf, Description: RedLeaf crypto function, Source: 00000001.00000002.248128854.0000000002580000.00000040.00000800.00020000.00000000.sdmp, Author: kev
Antivirus matches:	• Detection: 8%, Metadefender, Browse • Detection: 9%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\handkerchief.dat	unknown	4096	success or wait	63	6ED9D316	ReadFile

Analysis Process: iexplore.exe PID: **5844**, Parent PID: **488**

General

Target ID:	2
Start time:	07:21:35
Start date:	10/03/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Imagebase:	0x920000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: REDLEAVES_CoreImplant_UniqueStrings, Description: Strings identifying the core REDLEAVES RAT in its deobfuscated state, Source: 00000002.00000002.499777419.0000000003000000.00000040.00000400.00020000.00000000.sdmp, Author: USG • Rule: malware_red_leaves_generic, Description: Red Leaves malware, related to APT10, Source: 00000002.00000002.499777419.0000000003000000.00000040.00000400.00020000.00000000.sdmp, Author: David Cannings • Rule: RedLeaf, Description: RedLeaf crypto function, Source: 00000002.00000002.499777419.0000000003000000.00000040.00000400.00020000.00000000.sdmp, Author: kev • Rule: REDLEAVES_CoreImplant_UniqueStrings, Description: Strings identifying the core REDLEAVES RAT in its deobfuscated state, Source: 00000002.00000000.244543247.0000000003000000.00000040.00000400.00020000.00000000.sdmp, Author: USG • Rule: malware_red_leaves_generic, Description: Red Leaves malware, related to APT10, Source: 00000002.00000000.244543247.0000000003000000.00000040.00000400.00020000.00000000.sdmp, Author: David Cannings • Rule: RedLeaf, Description: RedLeaf crypto function, Source: 00000002.00000000.244543247.0000000003000000.00000040.00000400.00020000.00000000.sdmp, Author: kev • Rule: REDLEAVES_CoreImplant_UniqueStrings, Description: Strings identifying the core REDLEAVES RAT in its deobfuscated state, Source: 00000002.00000000.244858067.0000000003000000.00000040.00000400.00020000.00000000.sdmp, Author: USG • Rule: malware_red_leaves_generic, Description: Red Leaves malware, related to APT10, Source: 00000002.00000000.244858067.0000000003000000.00000040.00000400.00020000.00000000.sdmp, Author: David Cannings • Rule: RedLeaf, Description: RedLeaf crypto function, Source: 00000002.00000000.244858067.0000000003000000.00000040.00000400.00020000.00000000.sdmp, Author: kev • Rule: REDLEAVES_CoreImplant_UniqueStrings, Description: Strings identifying the core REDLEAVES RAT in its deobfuscated state, Source: 00000002.00000002.500129541.0000000004B40000.00000040.00000800.00020000.00000000.sdmp, Author: USG • Rule: malware_red_leaves_generic, Description: Red Leaves malware, related to APT10, Source: 00000002.00000002.500129541.0000000004B40000.00000040.00000800.00020000.00000000.sdmp, Author: David Cannings • Rule: RedLeaves, Description: detect RedLeaves in memory, Source: 00000002.00000002.500129541.0000000004B40000.00000040.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: obedience.exe PID: **5080**, Parent PID: **3616**

General

Target ID:	3
Start time:	07:21:44
Start date:	10/03/2022
Path:	C:\Users\user\AppData\Local\Temp\obedience.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\obedience.exe"
Imagebase:	0x400000
File size:	1616040 bytes
MD5 hash:	6A1C14D5F16A07BEF55943134FE618C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: REDLEAVES_DroppedFile_ImplantLoader_Starburn, Description: Detect the DLL responsible for loading and deobfuscating the DAT file containing shellcode and core REDLEAVES RAT, Source: 00000003.00000002.273655894.000000006EE51000.00000020.00000001.01000000.00000005.sdmp, Author: USG • Rule: REDLEAVES_CoreImplant_UniqueStrings, Description: Strings identifying the core REDLEAVES RAT in its deobfuscated state, Source: 00000003.00000002.273510822.0000000002410000.00000040.00000800.00020000.00000000.sdmp, Author: USG • Rule: malware_red_leaves_generic, Description: Red Leaves malware, related to APT10, Source: 00000003.00000002.273510822.0000000002410000.00000040.00000800.00020000.00000000.sdmp, Author: David Cannings • Rule: RedLeaf, Description: RedLeaf crypto function, Source: 00000003.00000002.273510822.0000000002410000.00000040.00000800.00020000.00000000.sdmp, Author: kev
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\handkerchief.dat	unknown	4096	success or wait	63	6EE5D316	ReadFile

Analysis Process: iexplore.exe PID: **244**, Parent PID: **5080**

General

Target ID:	4
Start time:	07:21:46
Start date:	10/03/2022
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	
Commandline:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Imagebase:	
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly