ID: 597511
Sample Name: 7.exe
Cookbook: default.jbs
Time: 07:58:25
Date: 26/03/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 7.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
Initial Sample 4
Dropped Files 5
Memory Dumps 5
Unpacked PEs 6
Sigma Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 7
Key, Mouse, Clipboard, Microphone and Screen Capturing 7
System Summary 7
Data Obfuscation 7
Hooking and other Techniques for Hiding and Protection 7
HIPS / PFW / Operating System Protection Evasion 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 11
Domains 11
URLs 11
Domains and IPs 12
Contacted Domains 12
Contacted URLs 13
URLs from Memory and Binaries 13
World Map of Contacted IPs 18
Public IPs 18
Private 19
General Information 19
Warnings 19
Simulations 20
Behavior and APIs 20
Joe Sandbox View / Context 20
IPs 20
Domains 20
ASNs 20
JA3 Fingerprints 20
Dropped Files 20
Created / dropped Files 20
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\WindowsUpdate.exe.log 20
C:\Users\user\AppData\Local\Temp\bhv4267.tmp 21
C:\Users\user\AppData\Local\Temp\holderwb.txt 21
C:\Users\user\AppData\Roaming\WindowsUpdate.exe 21
C:\Users\user\AppData\Roaming\WindowsUpdate.exe:Zone.Identifier 22
C:\Users\user\AppData\Roaming\pid.txt 22
C:\Users\user\AppData\Roaming\pidloc.txt 22
Static File Info 23
General 23
File Icon 23
Static PE Info 23
General 23
Entrypoint Preview 23
Data Directories 25
Sections 25
Resources 26
Imports 26
Version Infos 26
Network Behavior 26
Network Port Distribution 26
TCP Packets 27

UDP Packets 27
DNS Queries 28
DNS Answers 28
HTTP Request Dependency Graph 28
HTTP Packets 28
HTTPS Proxied Packets 29
FTP Packets 31
Statistics 31
Behavior 31
System Behavior 31
Analysis Process: 7.exePID: 6464, Parent PID: 5500 31
General 31
File Activities 32
File Created 32
File Deleted 33
File Written 33
File Read 33
Registry Activities 34
Key Value Created 34
Key Value Modified 34
Analysis Process: vbc.exePID: 7048, Parent PID: 6464 34
General 34
File Activities 34
File Created 34
Analysis Process: vbc.exePID: 7064, Parent PID: 6464 34
General 34
File Activities 35
File Created 35
File Deleted 35
File Written 35
File Read 35
Analysis Process: WindowsUpdate.exePID: 5692, Parent PID: 3616 36
General 36
File Activities 36
File Created 36
File Written 37
File Read 37
Analysis Process: WindowsUpdate.exePID: 2372, Parent PID: 3616 38
General 38
File Activities 38
File Created 38
File Read 38
Disassembly 39

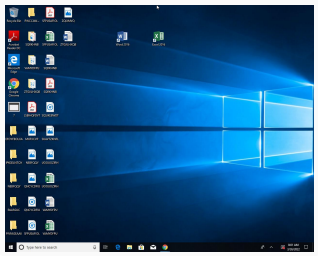
Windows Analysis Report

7.exe

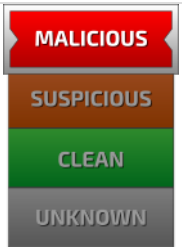
Overview

General Information

Sample Name:	7.exe
Analysis ID:	597511
MD5:	ed666bf7f4a0766.
SHA1:	1b90f1a4cb6059..
SHA256:	d1330d349bfbd3..
Tags:	exe
Infos:	



Detection



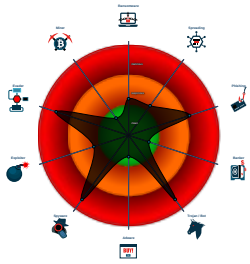
HawkEye
MailPassView

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

Signatures

- Yara detected MailPassView
- Yara detected HawkEye Keylogger
- Antivirus detection for dropped file
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Detected HawkEye Rat
- Multi AV Scanner detection for drop…
- Tries to steal Mail credentials (via fi…
- Tries to steal Mail credentials (via fi…
- Machine Learning detection for sam…
- Allocates memory in foreign process…

Classification



Process Tree

- **System is w10x64**
- 7.exe (PID: 6464 cmdline: "C:\Users\user\Desktop\7.exe" MD5: ED666BF7F4A0766FCEC0E9C8074B089B)
  - vbc.exe (PID: 7048 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext "C:\Users\user\AppData\Local\Temp\holdermail.txt" MD5: C63ED21D5706A527419C9FBD730FFB2E)
  - vbc.exe (PID: 7064 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext "C:\Users\user\AppData\Local\Temp\holderwb.txt" MD5: C63ED21D5706A527419C9FBD730FFB2E)
- WindowsUpdate.exe (PID: 5692 cmdline: "C:\Users\user\AppData\Roaming\WindowsUpdate.exe" MD5: ED666BF7F4A0766FCEC0E9C8074B089B)
- WindowsUpdate.exe (PID: 2372 cmdline: "C:\Users\user\AppData\Roaming\WindowsUpdate.exe" MD5: ED666BF7F4A0766FCEC0E9C8074B089B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
7.exe	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b8d9:$key: HawkEyeKeylogger • 0x7db15:$salt: 099u787978786 • 0x7bf12:$string1: HawkEye_Keylogger • 0x7cd65:$string1: HawkEye_Keylogger • 0x7da75:$string1: HawkEye_Keylogger • 0x7c2fb:$string2: holdermail.txt • 0x7c31b:$string2: holdermail.txt • 0x7c23d:$string3: wallet.dat • 0x7c255:$string3: wallet.dat • 0x7c26b:$string3: wallet.dat • 0x7d657:$string4: Keylog Records • 0x7d96f:$string4: Keylog Records • 0x7db6d:$string5: do not script --> • 0x7b8c1:$string6: \pidloc.txt • 0x7b927:$string7: BSPLIT • 0x7b937:$string7: BSPLIT
7.exe	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x7423:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
7.exe	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
7.exe	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
7.exe	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
Click to see the 1 entries				

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b8d9:$key: HawkEyeKeylogger • 0x7db15:$salt: 099u787978786 • 0x7bf12:$string1: HawkEye_Keylogger • 0x7cd65:$string1: HawkEye_Keylogger • 0x7da75:$string1: HawkEye_Keylogger • 0x7c2fb:$string2: holdermail.txt • 0x7c31b:$string2: holdermail.txt • 0x7c23d:$string3: wallet.dat • 0x7c255:$string3: wallet.dat • 0x7c26b:$string3: wallet.dat • 0x7d657:$string4: Keylog Records • 0x7d96f:$string4: Keylog Records • 0x7db6d:$string5: do not script --> • 0x7b8c1:$string6: \pidloc.txt • 0x7b927:$string7: BSPLIT • 0x7b937:$string7: BSPLIT
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x7423:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000000.295698908.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000006.00000000.294953383.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000007.00000002.336555805.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000000.294308364.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
0000000B.00000002.319064303.00000000004A2000.00000002.00000001.01000000.00000008.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b6d9:$key: HawkEyeKeylogger • 0x7d915:$salt: 099u787978786 • 0x7bd12:$string1: HawkEye_Keylogger • 0x7cb65:$string1: HawkEye_Keylogger • 0x7d875:$string1: HawkEye_Keylogger • 0x7c0fb:$string2: holdermail.txt • 0x7c11b:$string2: holdermail.txt • 0x7c03d:$string3: wallet.dat • 0x7c055:$string3: wallet.dat • 0x7c06b:$string3: wallet.dat • 0x7d457:$string4: Keylog Records • 0x7d76f:$string4: Keylog Records • 0x7d96d:$string5: do not script --> • 0x7b6c1:$string6: \pidloc.txt • 0x7b727:$string7: BSPLIT • 0x7b737:$string7: BSPLIT
Click to see the 50 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.WindowsUpdate.exe.c99c0d.2.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
13.2.WindowsUpdate.exe.cefa72.3.raw.unpack	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x1dc67:$key: HawkEyeKeylogger • 0x1fea3:$salt: 099u787978786 • 0x1e2a0:$string1: HawkEye_Keylogger • 0x1f0f3:$string1: HawkEye_Keylogger • 0x1fe03:$string1: HawkEye_Keylogger • 0x1e689:$string2: holdermail.txt • 0x1e6a9:$string2: holdermail.txt • 0x1e5cb:$string3: wallet.dat • 0x1e5e3:$string3: wallet.dat • 0x1e5f9:$string3: wallet.dat • 0x1f9e5:$string4: Keylog Records • 0x1fcfd:$string4: Keylog Records • 0x1fefb:$string5: do not script --> • 0x1dc4f:$string6: \pidloc.txt • 0x1dcb5:$string7: BSPLIT • 0x1dcc5:$string7: BSPLIT
13.2.WindowsUpdate.exe.cefa72.3.raw.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
13.2.WindowsUpdate.exe.cefa72.3.raw.unpack	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
13.2.WindowsUpdate.exe.cefa72.3.raw.unpack	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	• 0x1e2f8:$hawkstr1: HawkEye Keylogger • 0x1f139:$hawkstr1: HawkEye Keylogger • 0x1f468:$hawkstr1: HawkEye Keylogger • 0x1f5c3:$hawkstr1: HawkEye Keylogger • 0x1f726:$hawkstr1: HawkEye Keylogger • 0x1f9bd:$hawkstr1: HawkEye Keylogger • 0x1de86:$hawkstr2: Dear HawkEye Customers! • 0x1f4bb:$hawkstr2: Dear HawkEye Customers! • 0x1f612:$hawkstr2: Dear HawkEye Customers! • 0x1f779:$hawkstr2: Dear HawkEye Customers! • 0x1dfa7:$hawkstr3: HawkEye Logger Details:
Click to see the 164 entries				

Sigma Signatures

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

Joe Sandbox Signatures

AV Detection

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected HawkEye Keylogger

Contains functionality to log keystrokes (.Net Source)

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

Changes the view of files in windows explorer (hidden files and folders)

HIPS / PFW / Operating System Protection Evasion

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Sample uses process hollowing technique

Writes to foreign memory regions

.NET source code references suspicious native API functions

Stealing of Sensitive Information

Yara detected MailPassView

Yara detected HawkEye Keylogger

Tries to steal Mail credentials (via file / registry access)

Tries to steal Mail credentials (via file registry)

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

Yara detected WebBrowserPassView password recovery tool

Tries to steal Instant Messenger accounts or passwords

Remote Access Functionality

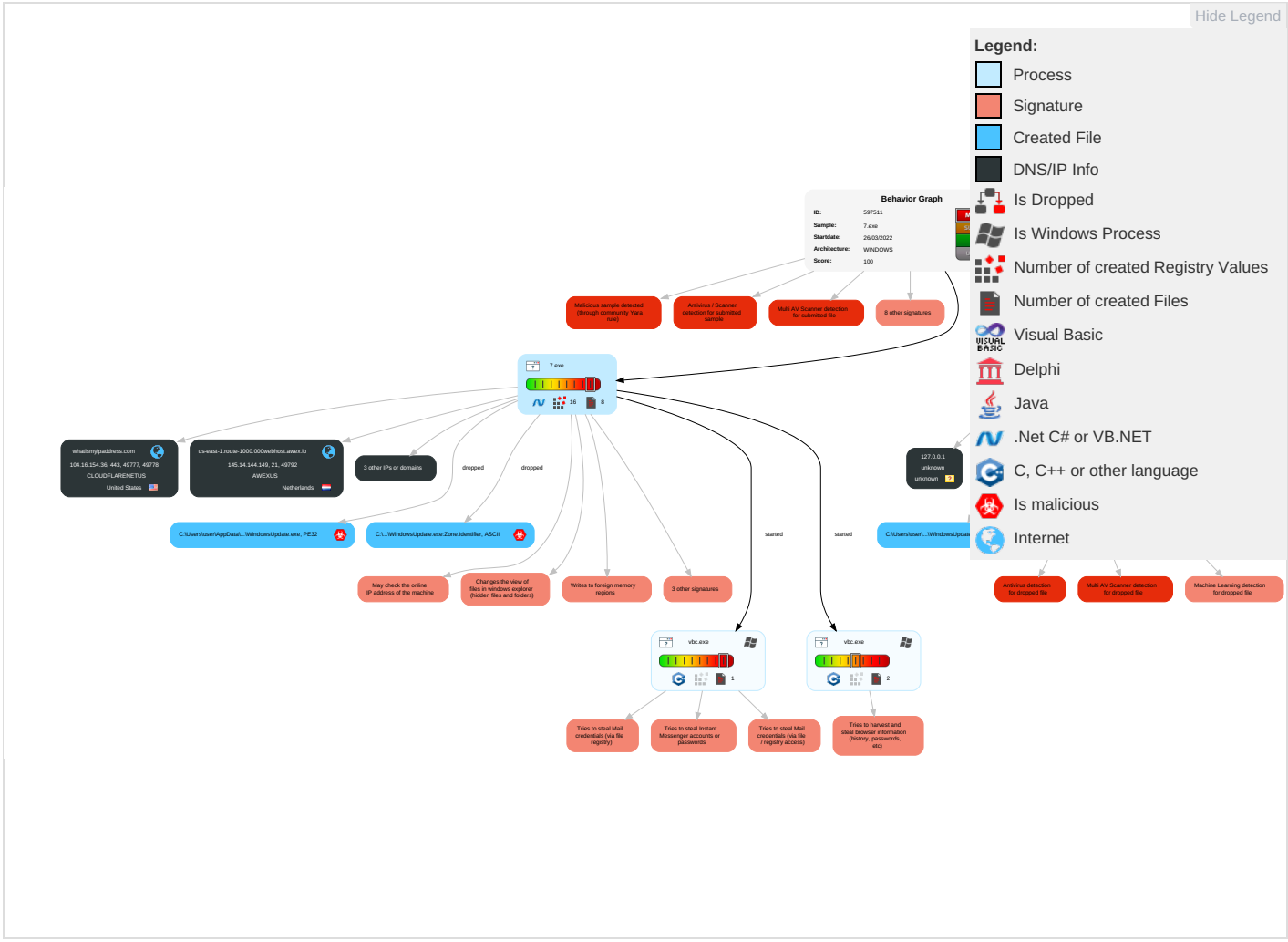
Yara detected HawkEye Keylogger

Detected HawkEye Rat

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Replication Through Removable Media	1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	1 OS Credential Dumping	1 System Time Discovery	1 Replication Through Removable Media	1 1 Archive Collected Data	1 Exfiltration Over Alternative Protocol	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 1 Native API	1 Registry Run Keys / Startup Folder	4 1 1 Process Injection	1 1 Deobfuscate/Decode Files or Information	1 1 Input Capture	1 Peripheral Device Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Shared Modules	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	3 1 Obfuscated Files or Information	2 Credentials in Registry	1 Account Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 Command and Scripting Interpreter	Logon Script (Mac)	Logon Script (Mac)	1 1 Software Packing	1 Credentials In Files	1 File and Directory Discovery	Distributed Component Object Model	1 1 Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	1 8 System Information Discovery	SSH	1 Clipboard Data	Data Transfer Size Limits	1 4 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	1 Query Registry	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 1 Virtualization/Sandbox Evasion	DCSync	1 3 1 Security Software Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	4 1 1 Process Injection	Proc Filesystem	2 1 Virtualization/Sandbox Evasion	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	3 Process Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 System Owner/User Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	1 Remote System Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	1 System Network Configuration Discovery	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery

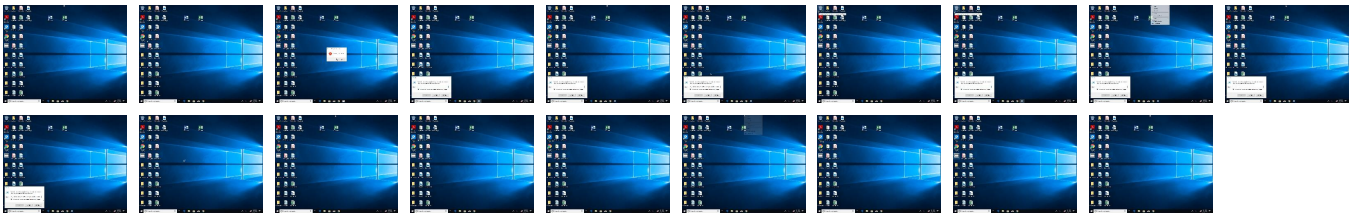
Behavior Graph



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
7.exe	84%	Virustotal		Browse
7.exe	69%	Metadefender		Browse
7.exe	95%	ReversingLabs	ByteCode-MSIL.Trojan.Golroted	
7.exe	100%	Avira	TR/AD.MExecute.Izrac	
7.exe	100%	Avira	SPR/Tool.MailPassView.473	
7.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	100%	Avira	TR/AD.MExecute.Izrac	
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	100%	Avira	SPR/Tool.MailPassView.473	
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	69%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	95%	ReversingLabs	ByteCode-MSIL.Trojan.Golroted	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.0.vbc.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1227086		Download File
6.0.vbc.exe.400000.1.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
0.2.7.exe.140000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
0.2.7.exe.140000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
7.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1227086		Download File
7.0.vbc.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1227086		Download File
0.0.7.exe.140000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
0.0.7.exe.140000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
13.2.WindowsUpdate.exe.c90000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
13.2.WindowsUpdate.exe.c90000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
6.0.vbc.exe.400000.4.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
7.0.vbc.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1227086		Download File
11.2.WindowsUpdate.exe.4a0000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
11.2.WindowsUpdate.exe.4a0000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
6.0.vbc.exe.400000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
6.0.vbc.exe.400000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
11.0.WindowsUpdate.exe.4a0000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
11.0.WindowsUpdate.exe.4a0000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
6.0.vbc.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
13.0.WindowsUpdate.exe.c90000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
13.0.WindowsUpdate.exe.c90000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
7.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1227086		Download File
7.0.vbc.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1227086		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://deff.nelreports.net/api/report?cat=msn	0%	URL Reputation	safe	
http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meCore.min.js	0%	URL Reputation	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6Ijk4OGQ1ZDgwMWE2ODQ2NDNkM2ZkMmYyMGEwOTgwMWQ3MDE2Z	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://https://whatismyipaddress.comx&Qq	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000/Converged_v21033_-0mnSwu67knBd7qR7YN9GQ2.css	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000.28666.10/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc1937	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_white_5ac590ee72bfe06a7cecfd75b5	0%	URL Reputation	safe	
http://www.sandoll.co.kru	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/R	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/D	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://mem.gfx.ms/meversion?partner=RetailStore2&market=en-us&uhf=1	0%	URL Reputation	safe	
http://www.carterandcone.comcoc	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cnlYM	0%	Avira URL Cloud	safe	
http://https://172.217.23.78/	0%	URL Reputation	safe	
http://www.founder.com.cn/cnicr	0%	URL Reputation	safe	
http://www.carterandcone.comnte	0%	Avira URL Cloud	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6ImYxODk5OTBhOWZjYjFmZjNjNmMxNDhmYjkzM2M3NzY1Mzk3Z	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://www.founder.com.cn/cnate	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/a	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTSGIAG3.crt0)	0%	URL Reputation	safe	
http://www.carterandcone.com$	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://adservice.google.co.uk/adsid/google/ui?gadsid=AORoGNQXg7AHkvg6J6S0TqGFa_0HynGV3_XxYfs4fLINJG	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn-u~	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.carterandcone.comyo	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnte	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.monotype.EN~	0%	Avira URL Cloud	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6IjJkYTFhZDAwNDEyNzQ2M2E3MGUyMWVkZmIxNmUyZjQ2MjBkM	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn-u	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.comT	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000/content/js/ConvergedLoginPaginatedStrings.en_5QoHC_ilFOmb96M0pIeJ	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
whatismyipaddress.com	104.16.154.36	true	false		high
us-east-1.route-1000.000webhost.awex.io	145.14.144.149	true	false		high
files.000webhost.com	unknown	unknown	false		high
49.124.12.0.in-addr.arpa	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://whatismyipaddress.com/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/chrome/static/css/main.v2.min.css	bhv4267.tmp.7.dr	false		high
http://https://www.msn.com//searchp/LinkId=255141	vbc.exe, 00000007.00000003.326997633.0000000002205000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj8k7G9rJDsAhWNTxUIHZZGDCQQ	vbc.exe, 00000007.00000003.324973841.000000000221A000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000007.00000003.326556191.00000000021FD000.00000004.00000800.00020000.00000000.sdmp, bhv4267.tmp.7.dr	false		high
http://https://dl.google.com/tag/s/appguid%3D%7B8A69D345-D564-463C-AFF1-A69D9E530F96%7D%26iid%3D%7B83C84637	bhv4267.tmp.7.dr	false		high
http://www.msn.com	bhv4267.tmp.7.dr	false		high
http://www.fontbureau.com/designers	7.exe, 00000000.00000002.520413464.00000000006122000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://deff.nelreports.net/api/report?cat=msn	bhv4267.tmp.7.dr	false	• URL Reputation: safe	unknown
http://https://contextual.media.net/__media__/js/util/nrrV9140.js	bhv4267.tmp.7.dr	false		high
http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meCore.min.js	bhv4267.tmp.7.dr	false	• URL Reputation: safe	unknown
http://https://www.google.com/chrome/static/images/download-browser/big_pixel_phone.png	bhv4267.tmp.7.dr	false		high
http://images.outbrainimg.com/transform/v3/eyJpdSI6Ijk4OGQ1ZDgwMWE2ODQ2NDNkM2ZkMmYyMGEwOTgwMWQ3MDE2Z	bhv4267.tmp.7.dr	false	• URL Reputation: safe	unknown
http://https://s.yimg.com/lo/api/res/1.2/BXjlWewXmZ47HeV5NPvUYA--~A/Zmk9ZmlsbDt3PTYyMjtoPTM2ODthcHBpZD1nZW1	bhv4267.tmp.7.dr	false		high
http://https://www.google.com/intl/en_uk/chrome/thank-you.html?statcb=0&installdataindex=empty&defaultbrows	bhv4267.tmp.7.dr	false		high
http://whatismyipaddress.com/-	7.exe, WindowsUpdate.exe.0.dr	false		high
http://www.galapagosdesign.com/DPlease	7.exe, 00000000.00000002.520413464.00000000006122000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/)	7.exe, 00000000.00000003.257894998.0000000004E97000.00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.258148677.0000000004E99000.00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.257636111.0000000004E97000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.site.com/logs.php	7.exe, 00000000.00000002.516506794.00000000002771000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	7.exe, 00000000.00000002.520413464.00000 00006122000.00000004.00000800.00020000.0 0000000.sdmp, 7.exe, 00000000.00000003.2 55428541.0000000004EC1000.00000004.00000 800.00020000.00000000.sdmp, 7.exe, 00000 000.00000003.255600555.0000000004EC1000. 00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.255298245.000 0000004EC1000.00000004.00000800.00020000 .00000000.sdmp, 7.exe, 00000000.00000003 .255021465.0000000004EC1000.00000004.000 00800.00020000.00000000.sdmp, 7.exe, 000 00000.00000003.255516238.0000000004EC100 0.00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.255733439.0000000004E C1000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.como.	7.exe, 00000000.00000003.255298245.00000 00004EC1000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://https://whatismyipaddress.comx&Qq	7.exe, 00000000.00000002.516506794.00000 00002771000.00000004.00000800.00020000.0 0000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://logincdn.msauth.net/16.000/Converged_v21033_-0mnSwu67knBd7qR7YN9GQ2.css	bhv4267.tmp.7.dr	false	• URL Reputation: safe	unknown
http://https://www.google.com/complete/search?q&cp=0&client=psy-ab&xssi=t&gs_ri=gws-wiz&hl=en&authuser=0&ps	bhv4267.tmp.7.dr	false		high
http://https://logincdn.msauth.net/16.000.28666.10/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc1937	bhv4267.tmp.7.dr	false	• URL Reputation: safe	unknown
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_white_5ac590ee72bfe06a7cecfd75b5	bhv4267.tmp.7.dr	false	• URL Reputation: safe	unknown
http://www.sandoll.co.kru	7.exe, 00000000.00000003.252539610.00000 00004EBF000.00000004.00000800.00020000.0 0000000.sdmp, 7.exe, 00000000.00000003.2 52440722.0000000004EBF000.00000004.00000 800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/complete/search?q&cp=0&client=psy-ab&xssi=t&gs_ri=gws-wiz&hl=en&authuser=0&pq	bhv4267.tmp.7.dr	false		high
http://www.jiyu-kobo.co.jp/R	7.exe, 00000000.00000003.257894998.00000 00004E97000.00000004.00000800.00020000.0 0000000.sdmp, 7.exe, 00000000.00000003.2 56933810.0000000004E9A000.00000004.00000 800.00020000.00000000.sdmp, 7.exe, 00000 000.00000003.256584450.0000000004E92000. 00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.257240105.000 0000004E9A000.00000004.00000800.00020000 .00000000.sdmp, 7.exe, 00000000.00000003 .257636111.0000000004E97000.00000004.000 00800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.com/search?source=hp&ei=djJ0X6TKCL6IjLsPqriogAY&q=chrome&oq=chrome&gs_lcp=CgZwc3k	bhv4267.tmp.7.dr	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC5bdddb231cf54f958a5b6e76e9d8eee	bhv4267.tmp.7.dr	false		high
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e	bhv4267.tmp.7.dr	false	• URL Reputation: safe	unknown
http://https://cvision.media.net/new/300x300/2/41/100/83/b5cbfa68-1c93-41c9-8797-4f9b532bc0b6.jpg?v=9	bhv4267.tmp.7.dr	false		high
http://https://www.google.com/chrome/static/images/download-browser/pixel_phone.png	bhv4267.tmp.7.dr	false		high
http://https://www.google.com/chrome/static/images/homepage/hero-anim-top-right.png	bhv4267.tmp.7.dr	false		high

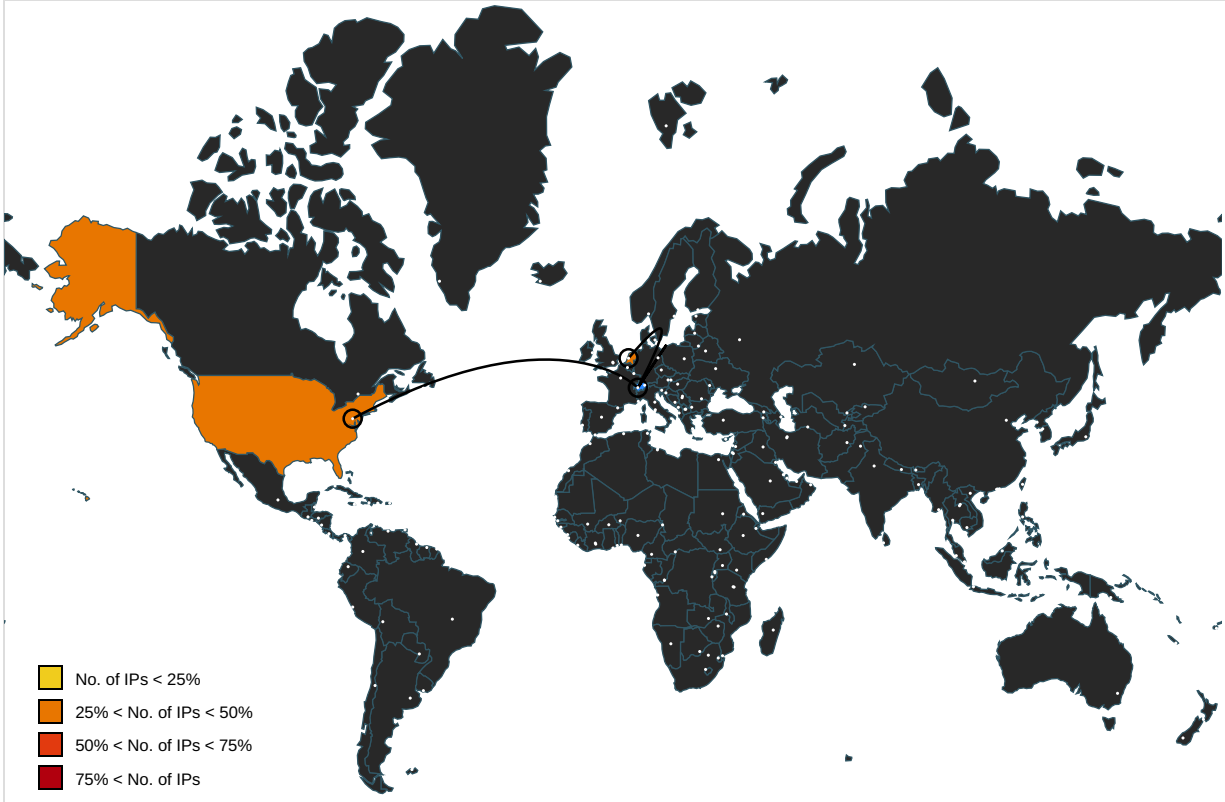
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/D	7.exe, 00000000.00000003.257894998.00000 00004E97000.00000004.00000800.00020000.0 0000000.sdmp, 7.exe, 00000000.00000003.2 56933810.0000000004E9A000.00000004.00000 800.00020000.00000000.sdmp, 7.exe, 00000 000.00000003.258148677.0000000004E99000. 00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.257240105.000 0000004E9A000.00000004.00000800.00020000 .00000000.sdmp, 7.exe, 00000000.00000003 .257636111.0000000004E97000.00000004.000 00800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://pki.goog/repository/0	bhv4267.tmp.7.dr	false	• URL Reputation: safe	unknown
http://https://www.msn.com/	vbc.exe, 00000007.00000003.327136256.000 0000002205000.00000004.00000800.00020000 .00000000.sdmp, vbc.exe, 00000007.000000 03.327359764.000000000220A000.00000004.0 0000800.00020000.00000000.sdmp, vbc.exe, 00000007.00000003.326799116.00000000022 0A000.00000004.00000800.00020000.0000000 0.sdmp, vbc.exe, 00000007.00000003.32699 7633.0000000002205000.00000004.00000800. 00020000.00000000.sdmp, bhv4267.tmp.7.dr	false		high
http://https://mem.gfx.ms/meversion?partner=RetailStore2&market=en-us&uhf=1	bhv4267.tmp.7.dr	false	• URL Reputation: safe	unknown
http://www.carterandcone.comcoc	7.exe, 00000000.00000003.255428541.00000 00004EC1000.00000004.00000800.00020000.0 0000000.sdmp, 7.exe, 00000000.00000003.2 55298245.0000000004EC1000.00000004.00000 800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/xjs/_/js/k=xjs.s.en_GB.u8fwEfmm86E.O/ck=xjs.s.hyRG9kR79v8.L.I11.O/m=lvlUe	bhv4267.tmp.7.dr	false		high
http://https://www.google.com/favicon.ico	bhv4267.tmp.7.dr	false		high
http://www.carterandcone.coml	7.exe, 00000000.00000002.520413464.00000 00006122000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://www.msn.com/	bhv4267.tmp.7.dr	false		high
http://www.founder.com.cn/cnlYM	7.exe, 00000000.00000003.253812592.00000 00004EC0000.00000004.00000800.00020000.0 0000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/chrome/static/images/fallback/google-logo-one-color.jpg	bhv4267.tmp.7.dr	false		high
http://https://172.217.23.78/	vbc.exe, 00000007.00000003.329240962.000 000000221A000.00000004.00000800.00020000 .00000000.sdmp, vbc.exe, 00000007.000000 03.329711659.00000000021FD000.00000004.0 0000800.00020000.00000000.sdmp, bhv4267. tmp.7.dr	false	• URL Reputation: safe	unknown
http://https://www.google.com/images/nav_logo299.png	bhv4267.tmp.7.dr	false		high
http://https://www.google.com/chrome/static/images/fallback/icon-help.jpg	bhv4267.tmp.7.dr	false		high
http://www.founder.com.cn/cnicr	7.exe, 00000000.00000003.253912284.00000 00004E9E000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.com/complete/search?q=c&cp=1&client=psy-ab&xssi=t&gs_ri=gws-wiz&hl=en&authuser=0&	bhv4267.tmp.7.dr	false		high
http://https://www.google.com/accounts/servicelogin	WindowsUpdate.exe	false		high
http://www.carterandcone.comnte	7.exe, 00000000.00000003.255428541.00000 00004EC1000.00000004.00000800.00020000.0 0000000.sdmp, 7.exe, 00000000.00000003.2 55600555.0000000004EC1000.00000004.00000 800.00020000.00000000.sdmp, 7.exe, 00000 000.00000003.255298245.0000000004EC1000. 00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.255516238.000 0000004EC1000.00000004.00000800.00020000 .00000000.sdmp, 7.exe, 00000000.00000003 .255733439.0000000004EC1000.00000004.000 00800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://consent.google.com/set?pc=s&uxe=4421591	bhv4267.tmp.7.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://images.outbrainimg.com/transform/v3/eyJpdSI6ImYxODk5OTBhOWZjYjFmZjNjNmMxNDhmYjkzM2M3NzY1Mzk3Z	bhv4267.tmp.7.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/images/hpp/Chrome_Owned_96x96.png	bhv4267.tmp.7.dr	false		high
http://crl.pki.goog/gsr2/gsr2.crl0?	bhv4267.tmp.7.dr	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnate	7.exe, 00000000.00000003.253646233.0000000004EBF000.00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.253468400.0000000004EBF000.00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.254218270.0000000004EC1000.00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.253342487.0000000004EBF000.00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.254533517.0000000004EC1000.00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.255021465.0000000004EC1000.00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.254350013.0000000004EC1000.00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.253812592.0000000004EC0000.00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.254694365.0000000004EC1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/a	7.exe, 00000000.00000003.257894998.00000004E97000.00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.256933810.0000000004E9A000.00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.257240105.0000000004E9A000.00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.257636111.0000000004E97000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://pki.goog/gsr2/GTSGIAG3.crt0)	bhv4267.tmp.7.dr	false	• URL Reputation: safe	unknown
http://https://googleads.g.doubleclick.net/adsid/google/ui?gadsid=AORoGNQP1yCl9r5iywZTFTjpazv-DURVxDidzMfrF	bhv4267.tmp.7.dr	false		high
http://https://googleads.g.doubleclick.net/adsid/google/ui?gadsid=AORoGNSrZsXAj6n_sYvivJecwrpYgMhb9ihVGAlz2	bhv4267.tmp.7.dr	false		high
http://https://www.google.com/chrome/static/images/fallback/icon-fb.jpg	bhv4267.tmp.7.dr	false		high
http://https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.9Ky5Gf3gP0o.O/m=gapi_iframes	bhv4267.tmp.7.dr	false		high
http://https://adservice.google.com/adsid/google/si?gadsid=AORoGNSvKHbjRugN8Bruw1IrFif72u8bwsJvZ4BRSrMAhil_	bhv4267.tmp.7.dr	false		high
http://www.carterandcone.com$	7.exe, 00000000.00000003.255331043.00000000000CCC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cn/bThe	7.exe, 00000000.00000002.520413464.00000000006122000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ogs.google.com/widget/callout?prid=19020392&pgid=19020380&puid=93eb0881ae9ec1db&origin=https	vbc.exe, 00000007.00000003.324973841.000000000221A000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000007.00000003.326556191.00000000021FD000.00000004.00000800.00020000.00000000.sdmp, bhv4267.tmp.7.dr	false		high
http://https://www.google.com/complete/search?q=chrome&cp=6&client=psy-ab&xssi=t&gs_ri=gws-wiz&hl=en&authus	bhv4267.tmp.7.dr	false		high
http://https://www.google.com/images/phd/px.gif	bhv4267.tmp.7.dr	false		high
http://https://www.google.com/chrome/static/images/homepage/google-canary.png	bhv4267.tmp.7.dr	false		high
http://https://adservice.google.co.uk/adsid/google/ui?gadsid=AORoGNQXg7AHkvg6J6S0TqGFa_0HynGV3_XxYfs4fLINJG	bhv4267.tmp.7.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://play.google.com/intl/en_us/badges/images/generic/de_badge_web_generic.png	bhv4267.tmp.7.dr	false		high
http://https://assets.adobedtm.com/launch-EN7b3d710ac67a4a1195648458258f97dd.min.js	bhv4267.tmp.7.dr	false		high
http://https://www.google.com/chrome/static/js/main.v2.min.js	bhv4267.tmp.7.dr	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCfd484f9188564713bbc5d13d862ebbf	bhv4267.tmp.7.dr	false		high
http://https://cvision.media.net/new/100x75/2/89/162/29/8ee7a9a3-dec9-4d15-94e1-5c73b17d2de1.jpg?v=9	bhv4267.tmp.7.dr	false		high
http://www.founder.com.cn/cnn-u~	7.exe, 00000000.00000003.253912284.00000000004E9E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	7.exe, 00000000.00000002.520413464.00000000006122000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comyo	7.exe, 00000000.00000003.255298245.00000000004EC1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cnte	7.exe, 00000000.00000003.255298245.00000000004EC1000.00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.255021465.0000000004EC1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com	7.exe, 00000000.00000002.520413464.00000000006122000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://googleads.g.doubleclick.net/adsid/google/si?gadsid=AORoGNTXuGHPo1zFjYPXt7mTG-4GALGGk8bjqjvBm	bhv4267.tmp.7.dr	false		high
http://www.monotype.EN~	7.exe, 00000000.00000003.262076697.00000000004EC1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	bhv4267.tmp.7.dr	false		high
http://https://www.google.com/intl/en_uk/chrome/	bhv4267.tmp.7.dr	false		high
http://https://www.google.com/chrome/static/images/fallback/icon-youtube.jpg	bhv4267.tmp.7.dr	false		high
http://https://googleads.g.doubleclick.net/adsid/google/si?gadsid=AORoGNQXwBwQrE_SUsnWzwpadcOOdc8yOg6JxthQN	bhv4267.tmp.7.dr	false		high
http://https://www.google.com/intl/en_uk/chrome/application/x-msdownloadC:	bhv4267.tmp.7.dr	false		high
http://images.outbrainimg.com/transform/v3/eyJpdSI6IjJkYTFhZDAwNDEyNzQ2M2E3MGUyMWVkZmIxNmUyZjQ2MjBkM	bhv4267.tmp.7.dr	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnn-u	7.exe, 00000000.00000003.253912284.00000000004E9E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	7.exe, 00000000.00000002.520413464.00000000006122000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	7.exe, 00000000.00000002.520413464.00000000006122000.00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.252539610.0000000004EBF000.00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.252440722.0000000004EBF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comT	7.exe, 00000000.00000003.255428541.00000 00004EC1000.00000004.00000800.00020000.0 0000000.sdmp, 7.exe, 00000000.00000003.2 55600555.0000000004EC1000.00000004.00000 800.00020000.00000000.sdmp, 7.exe, 00000 000.00000003.255298245.0000000004EC1000. 00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.255516238.000 0000004EC1000.00000004.00000800.00020000 .00000000.sdmp, 7.exe, 00000000.00000003 .255733439.0000000004EC1000.00000004.000 00800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=clien612;cat=chromx;ord=1;num=4510094	bhv4267.tmp.7.dr	false		high
http://https://www.google.com/chrome/static/js/installer.min.js	bhv4267.tmp.7.dr	false		high
http://https://www.google.com/search	bhv4267.tmp.7.dr	false		high
http://https://www.google.com/chrome/static/images/download-browser/pixel_tablet.png	bhv4267.tmp.7.dr	false		high
http://whatismyipaddress.com	7.exe, 00000000.00000002.516506794.00000 00002771000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/	7.exe, 00000000.00000003.257894998.00000 00004E97000.00000004.00000800.00020000.0 0000000.sdmp, 7.exe, 00000000.00000003.2 56933810.0000000004E9A000.00000004.00000 800.00020000.00000000.sdmp, 7.exe, 00000 000.00000003.258148677.0000000004E99000. 00000004.00000800.00020000.00000000.sdmp, 7.exe, 00000000.00000003.257240105.000 0000004E9A000.00000004.00000800.00020000 .00000000.sdmp, 7.exe, 00000000.00000003 .257636111.0000000004E97000.00000004.000 00800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://logincdn.msauth.net/16.000/content/js/ConvergedLoginPaginatedStrings.en_5QoHC_ilFOmb96M0pIeJ	bhv4267.tmp.7.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.154.36	whatismyipaddress.com	United States		13335	CLOUDFLARENETUS	false
145.14.144.149	us-east-1.route-1000.000webhost.awex.io	Netherlands		204915	AWEXUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	597511
Start date and time:	2022-03-26 06:58:25 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	7.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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.spyw.evad.winEXE@7/7@4/4
EGA Information:	• Successful, ratio: 80%
HDC Information:	• Successful, ratio: 27.3% (good quality ratio 25.2%) • Quality average: 73.4% • Quality standard deviation: 29.9%
HCA Information:	• Successful, ratio: 100% • 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

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target 7.exe, PID 6464 because there are no executed fu nction
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing d isassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtCreateFile calls found.
- 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
07:59:51	API Interceptor	5x Sleep call for process: 7.exe modified
07:59:54	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe
08:00:04	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\WindowsUpdate.exe.log

Process:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	916
Entropy (8bit):	5.282390836641403
Encrypted:	false
SSDEEP:	24:MLF20NaL3z2p29hJ5g522rW2xAi3AP26K95rKoO2+g2+:MwLLD2Y9h3go2rxxAcAO6ox+g2+
MD5:	5AD8E7ABEADADAC4CE06FF693476581A
SHA1:	81E42A97BBE3D7DE8B1E8B54C2B03C48594D761E
SHA-256:	BAA1A28262BA27D51C3A1FA7FB0811AD1128297ABB2EDCCC785DC52667D2A6FD
SHA-512:	7793E78E84AD36CE65B5B1C015364E340FB9110FAF199BC0234108CE9BCB1AEDACBD25C6A012AC99740E08BEA5E5C373A88E553E47016304D8AE6AEEAB58EBFF
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\de460308a9099237864d2ec2328fc958\System.Configuration.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d83c619a3e1d3\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Temp\bhv4267.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x8b6baa0f, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	29884416
Entropy (8bit):	1.0170449202764986
Encrypted:	false
SSDEEP:	24576:crjyt8HVmyG4w781NfXy7R4aUpP9dCr6f63rsLOZ:Kwy9ry
MD5:	934C3D1A99E6E4B191ED8CB784676BF1
SHA1:	9E97CB6DA3429A6C12B629E8A3527210FF7A96BE
SHA-256:	3611926483D1CA01A1DB2B8C7F61F432767BFA24BD6C16CCC58B24AF44269D64
SHA-512:	5225052FC33EA70B40EAEF6180F6A6A788DBF2E5DA1BD22BC4743A2170933809B4A4FBBF6ADC6939BC0C5433C31A881AE4D3F3CC882EB928E6C94569754C9E44
Malicious:	false
Reputation:	unknown
Preview:	.k..... ....?......_e..*....w........................=......+...z...;...z#.h.?.........................b...*....w..{............B......................... ....;...z... ....U...;...zu..................{...;...z#.. ....

C:\Users\user\AppData\Local\Temp\holderwb.txt

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Reputation:	unknown
Preview:	..

C:\Users\user\AppData\Roaming\WindowsUpdate.exe

Process:	C:\Users\user\Desktop\7.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	913920
Entropy (8bit):	7.376805169532317
Encrypted:	false
SSDEEP:	12288:ypEQtqB5urTIoYWBQk1E+VF9mOx9wi1T0hnbkOWAvyPx4+c/bUUCy:HQtqBorTlYWBhE+V3mO5vWgxE/nb
MD5:	ED666BF7F4A0766FCEC0E9C8074B089B
SHA1:	1B90F1A4CB6059D573FFF115B3598604825D76E6
SHA-256:	D1330D349BFBD3AEA545FA08EF63339E82A3F4D04E27216ECC4C45304F079264
SHA-512:	D0791EAA9859D751F946FD3252D2056C29328FC97E147A5234A52A3728588A3A1AAA003A8E32863D338EBDCA92305C48B6FA12CA1E620CF27460BF091C3B6D4
Malicious:	**true**
Yara Hits:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: JPCERT/CC Incident Response Group

Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 69%, Browse • Antivirus: ReversingLabs, Detection: 95%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....C.a.....4..... .....@.. ....@.....S.... ...2.....`..... ..... ..H.....text..... ..... ..`.rsrc....2... ...2.....@..@.reloc.....` ....@..B.....H.....0}..h.....X.....2s.....*....0.....~.....(.....~....o....~....o.....9.....~....o.....+G~.....o.....o.....,). .....,.~.....~.....o....o.....1.~.....~....o.....o.....~....~....o....o.....~.....(....s....o.....(.....*.....0.. .....(....(.....(.....o.....*.....(.....(.....o... ....o.....o.....o.....*.R..(....o....o.....

C:\Users\user\AppData\Roaming\WindowsUpdate.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\7.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\pid.txt

Process:	C:\Users\user\Desktop\7.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:3:3
MD5:	894A9B94BCC5969B60BD18E8EA9C0DDC
SHA1:	F04A8305CF42ECB7BD5B110ADAB57CE9F68AF30C
SHA-256:	7EE3819BF62F7E4563A2A9476DF6E18A6CD17CCEB30B92F00A24A6C8175E3740
SHA-512:	56088DA0021FBDB8F45EC54B65B929FF335DC38DE3532911125F7783D5FC04142DF54CAA595CBF666E74EE9CF414F8AE8811E4CA3C1AFB14DDE49B15F57CC55
Malicious:	false
Reputation:	unknown
Preview:	6464

C:\Users\user\AppData\Roaming\pidloc.txt

Process:	C:\Users\user\Desktop\7.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	28
Entropy (8bit):	3.7498677622562893
Encrypted:	false
SSDEEP:	3:oNt+WfWS0dAn:oNwvSJn
MD5:	5441150DCB31D2321C8B08EB4F2229F9
SHA1:	32624BFDA16A24F5156DF6CDC6599059BB28806A
SHA-256:	CF3960D86A865004B36F3967A25596F06F3EDBBA9EF41800BD5239020BA894EF
SHA-512:	8F07350A103D3091B3CF99F72CBBC7FE1E35607D555FC6A2664E28B6FC4BE30D531FC442833B688D0DE2805B1AA8CAB32DB0069D632FFBEC46998486EC9A7F59
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\Desktop\7.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.376805169532317
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.69% • Win32 Executable (generic) a (10002005/4) 49.65% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • InstallShield setup (43055/19) 0.21% • Windows Screen Saver (13104/52) 0.07%
File name:	7.exe
File size:	913920
MD5:	ed666bf7f4a0766fcec0e9c8074b089b
SHA1:	1b90f1a4cb6059d573fff115b3598604825d76e6
SHA256:	d1330d349bfbd3aea545fa08ef63339e82a3f4d04e27216ecc4c45304f079264
SHA512:	d0791eaa9859d751f946fd3252d2056c29328fc97e147a5234a52a3728588a3a1aaa003a8e32863d338ebdca92305c48b6fa12ca1e620cf27460bf091c3b6d49
SSDEEP:	12288:ypEQtqB5urTIoYWBQk1E+VF9mOx9wi1T0hnbkOWAvyPx4+c/bUUCy:HQtqBorTlYWBhE+V3mO5vWgxE/nb
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....C.a.....4..... .....@.. .....@.....

File Icon

Icon Hash:	41455554545445a2

Static PE Info

General

Entrypoint:	0x480bee
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:	0x61A643FF [Tue Nov 30 15:32:15 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x80b98	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x82000	0x3200	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x86000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7ebf4	0x7ec00	False	0.572708641519	data	6.54105917207	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x82000	0x3200	0x3200	False	0.105390625	data	3.5876692887	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x86000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x824f0	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 2004318071, next used block 4286019447		
RT_ICON	0x827d8	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x82900	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x831a8	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x83710	0x353	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x83a68	0x10a8	data		
RT_ICON	0x84b10	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x84f78	0x68	data		
RT_VERSION	0x82250	0x2a0	data		
RT_MANIFEST	0x84fe0	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2014
Assembly Version	1.0.0.0
InternalName	Phulli.exe
FileVersion	1.0.0.0
ProductName	Phulli
ProductVersion	1.0.0.0
FileDescription	Phulli
OriginalFilename	Phulli.exe

Network Behavior

Network Port Distribution

Total Packets: 30

- 53 (DNS)
- 21 (FTP -- Control)
- 443 (HTTPS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 26, 2022 07:59:50.573096991 CET	49777	80	192.168.2.4	104.16.154.36
Mar 26, 2022 07:59:50.589638948 CET	80	49777	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:50.589754105 CET	49777	80	192.168.2.4	104.16.154.36
Mar 26, 2022 07:59:50.590919018 CET	49777	80	192.168.2.4	104.16.154.36
Mar 26, 2022 07:59:50.607353926 CET	80	49777	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:50.617904902 CET	80	49777	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:50.680655003 CET	49778	443	192.168.2.4	104.16.154.36
Mar 26, 2022 07:59:50.680695057 CET	443	49778	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:50.680774927 CET	49778	443	192.168.2.4	104.16.154.36
Mar 26, 2022 07:59:50.733393908 CET	49777	80	192.168.2.4	104.16.154.36
Mar 26, 2022 07:59:50.918349981 CET	49778	443	192.168.2.4	104.16.154.36
Mar 26, 2022 07:59:50.918375015 CET	443	49778	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:50.965903997 CET	443	49778	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:50.966053009 CET	49778	443	192.168.2.4	104.16.154.36
Mar 26, 2022 07:59:50.977786064 CET	49778	443	192.168.2.4	104.16.154.36
Mar 26, 2022 07:59:50.977813005 CET	443	49778	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:50.978216887 CET	443	49778	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:51.029911041 CET	49778	443	192.168.2.4	104.16.154.36
Mar 26, 2022 07:59:51.317478895 CET	49778	443	192.168.2.4	104.16.154.36
Mar 26, 2022 07:59:51.344531059 CET	443	49778	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:51.344666004 CET	443	49778	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:51.344749928 CET	49778	443	192.168.2.4	104.16.154.36
Mar 26, 2022 07:59:51.344755888 CET	443	49778	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:51.344796896 CET	443	49778	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:51.344851017 CET	49778	443	192.168.2.4	104.16.154.36
Mar 26, 2022 07:59:51.344872952 CET	443	49778	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:51.345206976 CET	443	49778	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:51.345288992 CET	49778	443	192.168.2.4	104.16.154.36
Mar 26, 2022 07:59:51.345308065 CET	443	49778	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:51.345385075 CET	443	49778	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:51.345438004 CET	49778	443	192.168.2.4	104.16.154.36
Mar 26, 2022 07:59:51.345452070 CET	443	49778	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:51.345685005 CET	443	49778	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:51.345746994 CET	443	49778	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:51.345772028 CET	49778	443	192.168.2.4	104.16.154.36
Mar 26, 2022 07:59:51.345789909 CET	443	49778	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:51.345833063 CET	49778	443	192.168.2.4	104.16.154.36
Mar 26, 2022 07:59:51.345851898 CET	443	49778	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:51.345997095 CET	443	49778	104.16.154.36	192.168.2.4
Mar 26, 2022 07:59:51.346059084 CET	49778	443	192.168.2.4	104.16.154.36
Mar 26, 2022 07:59:51.353233099 CET	49778	443	192.168.2.4	104.16.154.36
Mar 26, 2022 08:00:23.179586887 CET	49777	80	192.168.2.4	104.16.154.36
Mar 26, 2022 08:00:23.196544886 CET	80	49777	104.16.154.36	192.168.2.4
Mar 26, 2022 08:00:23.196640015 CET	49777	80	192.168.2.4	104.16.154.36
Mar 26, 2022 08:00:23.253387928 CET	49792	21	192.168.2.4	145.14.144.149
Mar 26, 2022 08:00:23.378848076 CET	21	49792	145.14.144.149	192.168.2.4
Mar 26, 2022 08:00:23.378952026 CET	49792	21	192.168.2.4	145.14.144.149
Mar 26, 2022 08:00:23.518426895 CET	21	49792	145.14.144.149	192.168.2.4
Mar 26, 2022 08:00:23.523405075 CET	49792	21	192.168.2.4	145.14.144.149
Mar 26, 2022 08:00:23.649051905 CET	21	49792	145.14.144.149	192.168.2.4
Mar 26, 2022 08:00:24.476912975 CET	21	49792	145.14.144.149	192.168.2.4
Mar 26, 2022 08:00:24.480254889 CET	49792	21	192.168.2.4	145.14.144.149
Mar 26, 2022 08:00:24.606931925 CET	21	49792	145.14.144.149	192.168.2.4
Mar 26, 2022 08:00:24.607055902 CET	49792	21	192.168.2.4	145.14.144.149

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 26, 2022 07:59:50.148940086 CET	54069	53	192.168.2.4	8.8.8.8
Mar 26, 2022 07:59:50.168469906 CET	53	54069	8.8.8.8	192.168.2.4
Mar 26, 2022 07:59:50.442208052 CET	57747	53	192.168.2.4	8.8.8.8
Mar 26, 2022 07:59:50.465178013 CET	53	57747	8.8.8.8	192.168.2.4
Mar 26, 2022 07:59:50.660053015 CET	58171	53	192.168.2.4	8.8.8.8
Mar 26, 2022 07:59:50.678874016 CET	53	58171	8.8.8.8	192.168.2.4
Mar 26, 2022 08:00:23.184053898 CET	51679	53	192.168.2.4	8.8.8.8
Mar 26, 2022 08:00:23.216795921 CET	53	51679	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 26, 2022 07:59:50.148940086 CET	192.168.2.4	8.8.8.8	0x2e5f	Standard query (0)	49.124.12.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Mar 26, 2022 07:59:50.442208052 CET	192.168.2.4	8.8.8.8	0x7775	Standard query (0)	whatismyipaddress.com	A (IP address)	IN (0x0001)
Mar 26, 2022 07:59:50.660053015 CET	192.168.2.4	8.8.8.8	0x1bc3	Standard query (0)	whatismyipaddress.com	A (IP address)	IN (0x0001)
Mar 26, 2022 08:00:23.184053898 CET	192.168.2.4	8.8.8.8	0xd189	Standard query (0)	files.000webhost.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 26, 2022 07:59:50.168469906 CET	8.8.8.8	192.168.2.4	0x2e5f	Name error (3)	49.124.12.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Mar 26, 2022 07:59:50.465178013 CET	8.8.8.8	192.168.2.4	0x7775	No error (0)	whatismyipaddress.com		104.16.154.36	A (IP address)	IN (0x0001)
Mar 26, 2022 07:59:50.465178013 CET	8.8.8.8	192.168.2.4	0x7775	No error (0)	whatismyipaddress.com		104.16.155.36	A (IP address)	IN (0x0001)
Mar 26, 2022 07:59:50.678874016 CET	8.8.8.8	192.168.2.4	0x1bc3	No error (0)	whatismyipaddress.com		104.16.154.36	A (IP address)	IN (0x0001)
Mar 26, 2022 07:59:50.678874016 CET	8.8.8.8	192.168.2.4	0x1bc3	No error (0)	whatismyipaddress.com		104.16.155.36	A (IP address)	IN (0x0001)
Mar 26, 2022 08:00:23.216795921 CET	8.8.8.8	192.168.2.4	0xd189	No error (0)	files.000webhost.com	us-east-1.route-1000.000webhost.awex.io		CNAME (Canonical name)	IN (0x0001)
Mar 26, 2022 08:00:23.216795921 CET	8.8.8.8	192.168.2.4	0xd189	No error (0)	us-east-1.route-1000.000webhost.awex.io		145.14.144.149	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- whatismyipaddress.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49778	104.16.154.36	443	C:\Users\user\Desktop\7.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49777	104.16.154.36	80	C:\Users\user\Desktop\7.exe

Timestamp	kBytes transferred	Direction	Data
Mar 26, 2022 07:59:50.590919018 CET	1051	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Mar 26, 2022 07:59:50.617904902 CET	1052	IN	HTTP/1.1 301 Moved Permanently Date: Sat, 26 Mar 2022 06:59:50 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Sat, 26 Mar 2022 07:59:50 GMT Location: https://whatismyipaddress.com/ Set-Cookie: __cf_bm=S_s1CS7DGOM6eBfXmUtivKhK4v54G0jBWizUnEhD0hc-1648277990-0-AcT/wi4ZYVZB1IWa1ExFH8BRgzGuiMz541nIRM/73gJ1Yt+VLI8/WZDyVzjjF+3OkKYGGrFmIvzzTmB27VGgnO4=; path=/; expires=Sat, 26-Mar-22 07:29:50 GMT; domain=.whatismyipaddress.com; HttpOnly Server: cloudflare CF-RAY: 6f1e01813e6b9ba6-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49778	104.16.154.36	443	C:\Users\user\Desktop\7.exe

Timestamp	kBytes transferred	Direction	Data
2022-03-26 06:59:51 UTC	0	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
2022-03-26 06:59:51 UTC	0	IN	HTTP/1.1 403 Forbidden Date: Sat, 26 Mar 2022 06:59:51 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close CF-Chl-Bypass: 1 Permissions-Policy: accelerometer=(),autoplay=(),camera=(),clipboard-read=(),clipboard-write=(),fullscreen=(),geolocation=(),gyroscope=(),hid=(),interest-cohort=(),magnetometer=(),microphone=(),payment=(),publickey-credentials-get=(),screen-wake-lock=(),serial=(),sync-xhr=(),usb=() Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Expires: Thu, 01 Jan 1970 00:00:01 GMT X-Frame-Options: SAMEORIGIN Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Set-Cookie: __cf_bm=Vd7oHkl86VCkRNhJ2ufFFOkskwgzG61jnL7.1ngI0ZI-1648277991-0-AXKGAVonDzYglQ/tiv8FR+qwypp7BnEq4lYKCAOahVihbQj4Dc3wxS0Ubdt8j3dqzSOLMUDxNAMCmdmFvxUXhL8=; path=/; expires=Sat, 26-Mar-22 07:29:51 GMT; domain=.whatismyipaddress.com; HttpOnly; Secure Server: cloudflare CF-RAY: 6f1e0185c8788ffa-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-03-26 06:59:51 UTC	1	IN	Data Raw: 33 33 39 61 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 Data Ascii: 339a<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->...[if
2022-03-26 06:59:51 UTC	1	IN	Data Raw: 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 0a 3c 74 69 74 6c 65 3e 50 6c 65 61 73 65 20 57 61 69 74 2e 2e 2e 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 20 20 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 63 61 70 74 63 68 61 2d 62 79 70 61 73 73 22 20 69 64 3d 22 63 61 70 74 63 68 61 2d 62 79 70 61 73 73 22 20 2f 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 Data Ascii: o-js" lang="en-US"> ...<![endif]--><head><title>Please Wait... | Cloudflare</title> <meta name="captcha-bypass" id="captcha-bypass" /><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="
2022-03-26 06:59:51 UTC	2	IN	Data Raw: 47 7a 4e 42 7a 30 22 2c 0a 20 20 20 20 20 20 20 20 63 46 50 57 76 3a 20 22 62 22 2c 0a 20 20 20 20 20 20 20 20 63 54 54 69 6d 65 4d 73 3a 20 22 31 30 30 30 22 2c 0a 20 20 20 20 20 20 20 20 63 4c 74 3a 20 22 6e 22 2c 0a 20 20 20 20 20 20 20 20 20 20 63 52 71 3a 20 7b 0a 20 20 20 20 20 20 20 20 20 20 72 75 3a 20 22 61 48 52 30 63 48 4d 36 4c 79 39 33 61 47 46 30 61 58 4e 74 65 57 6c 77 59 57 52 6b 63 6d 56 7a 63 79 35 6a 62 32 30 76 22 2c 0a 20 20 20 20 20 20 20 20 20 20 72 61 3a 20 22 22 2c 0a 20 20 20 20 20 20 20 20 20 20 72 6d 3a 20 22 52 30 56 55 22 2c 0a 20 20 20 20 20 20 20 20 20 20 64 3a 20 22 5a 53 65 4f 37 53 74 2f 6e 36 56 6a 6c 33 2f 79 74 51 64 65 61 31 57 47 70 4e 79 66 2b 47 57 63 47 55 33 45 61 49 6a 41 74 6a 6f 46 6b 53 6e 48 42 49 47 45 72 34 6a Data Ascii: GzNBz0", cFPWv: "b", cTTimeMs: "1000", cLt: "n", cRq: { ru: "aHR0cHM6Ly93aGF0aXNteWlwYWRkcmVzcy5jb20v", ra: "", rm: "R0VU", d: "ZSeO7St/n6Vjl3/ytQdea1WGpNyf+GWcGU3EaIjAtjoFkSnHBIGEr4j

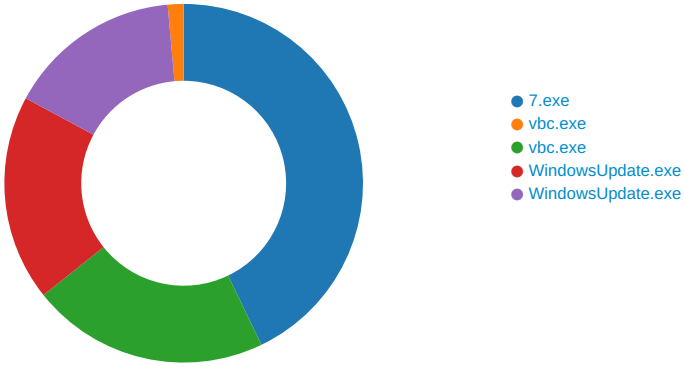
Timestamp	kBytes transferred	Direction	Data
2022-03-26 06:59:51 UTC	4	IN	Data Raw: 3a 36 39 70 78 3b 20 6d 61 72 67 69 6e 3a 20 20 61 75 74 6f 3b 7d 0a 20 20 23 63 66 2d 77 72 61 70 70 65 72 20 23 63 66 2d 70 6c 65 61 73 65 2d 77 61 69 74 7b 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 7d 0a 20 20 2e 61 74 74 72 69 62 75 74 69 6f 6e 20 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 33 32 70 78 3b 7d 0a 20 20 2e 62 75 62 62 6c 65 73 20 7b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 35 38 32 32 30 3b 20 77 69 64 74 68 3a 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 32 30 70 78 3b 20 6d 61 72 67 69 6e 3a 32 70 78 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 31 30 30 25 3b 20 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 20 7d 0a 20 20 23 63 66 2d 77 72 61 70 70 65 72 20 23 63 68 61 6c 6c 65 6e 67 65 2d 66 Data Ascii: :69px; margin: auto;} #cf-wrapper #cf-please-wait{text-align:center} .attribution {margin-top: 32px;} .bubbles { background-color: #f58220; width:20px; height: 20px; margin:2px; border-radius:100%; display:inline-block; } #cf-wrapper #challenge-f
2022-03-26 06:59:51 UTC	5	IN	Data Raw: 20 20 20 20 20 20 0a 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 66 2d 73 65 63 74 69 6f 6e 20 63 66 2d 68 69 67 68 6c 69 67 68 74 20 63 66 2d 63 61 70 74 63 68 61 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 0a 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 66 2d 77 72 61 70 70 65 72 22 3e 0a 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 66 2d 63 6f 6c 75 6d 6e 73 20 74 77 6f 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 66 2d 63 6f 6c 75 6d 6e 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 66 2d 68 69 67 68 6c 69 67 68 74 2d 69 6e 76 65 72 73 65 20 63 66 2d 72 6d 2d 73 74 61 63 6b 65 Data Ascii: <div class="cf-highlight-inverse cf-form-stacked
2022-03-26 06:59:51 UTC	6	IN	Data Raw: 64 31 35 58 45 30 54 36 70 41 55 73 31 73 32 6d 6d 62 67 47 50 55 49 75 52 63 45 54 7a 51 35 74 5f 33 34 45 77 57 48 37 73 64 75 74 4f 67 35 78 31 61 78 7a 68 5a 38 71 58 46 74 6c 5f 39 42 4b 68 68 6d 33 4a 64 47 44 58 78 44 37 65 43 44 4b 54 6d 69 68 6d 41 31 63 57 7a 70 5a 73 6e 42 36 77 38 5f 5a 69 5a 6e 46 39 30 76 62 5a 35 4a 30 76 72 39 4a 33 42 64 78 70 5a 6d 74 36 55 6f 6e 66 4a 70 68 69 34 57 41 65 6a 35 4d 72 53 78 58 5a 76 4f 42 31 34 35 30 6e 72 5f 47 32 6f 72 53 73 71 34 4d 43 70 44 76 52 31 51 48 4f 46 49 43 49 5f 71 31 32 5a 73 42 59 58 43 6d 58 5a 78 76 48 41 55 56 67 2d 6d 4e 70 61 70 56 69 77 4d 6f 47 4d 74 55 59 41 37 55 42 70 76 76 6e 6c 55 48 77 4b 50 33 45 71 43 4a 34 58 42 31 4a 6c 52 69 38 5f 51 66 6a 66 36 50 47 4a 5f 4b 36 57 30 Data Ascii: d15XE0T6pAUs1s2mmbgGPUIuRcETzQ5t_34EwWH7sdutOg5x1axzhZ8qXFtl_9BKhhm3JdGDXxD7eC DKTmihmA1cWzpZsnB6w8_ZiZnF90vbZ5J0vr9J3BdxpZmt6UonfJphi4WAej5MrSxXZvOB1450nr_G2orSsq4MCpDv R1QHOFICI_q12ZsBYXCmXZxvHAUVg-mNpapViwMoGMtUYA7UBpvvnlUHwKP3EqCJ4XB1JlRi8_Qfjf6PGJ_K6W0
2022-03-26 06:59:51 UTC	8	IN	Data Raw: 6b 4d 37 61 4b 75 58 30 31 7a 41 65 6a 4f 30 69 42 4f 50 41 49 57 58 64 63 72 63 71 63 73 4e 52 4e 50 62 68 76 38 57 58 34 32 65 6b 49 4c 41 75 43 34 56 2f 30 31 73 2b 61 2b 71 71 53 6f 49 59 42 42 67 43 75 6e 4f 37 79 72 52 4f 70 66 32 76 56 68 50 38 45 64 63 36 53 66 43 70 36 36 32 46 47 70 2f 78 72 58 41 51 30 31 70 55 52 6c 6d 48 38 6b 61 6c 2f 76 6c 69 51 50 69 79 42 55 50 73 4a 2b 44 65 53 6b 41 69 64 6b 71 6a 75 68 34 71 2f 35 6a 61 2b 6a 67 57 45 76 61 44 5a 49 34 65 75 44 6c 37 6e 59 38 6f 35 61 66 39 30 44 6e 48 66 4a 63 48 41 4c 67 61 33 38 77 36 37 32 75 45 32 54 57 54 49 36 52 52 42 51 44 35 2b 76 38 78 51 53 47 75 74 48 70 4e 36 36 5a 62 52 41 4b 4a 45 4f 70 70 4a 34 37 59 4f 34 6b 6b 4e 73 57 47 44 4b 6a 4b 59 61 73 47 7a 57 7a 34 77 38 63 Data Ascii: kM7aKuX01zAejO0iBOPAIWXdcrcqcsNRNPbhv8WX42ekILAuC4V/01s+a+qqSoIYBBgCunO7yrROpf 2vVhP8Edc6SfCp662FGp/xrXAQ01pURlmH8kal/vliQPiyBUPsJ+DeSkAidkqjuh4q/5ja+jgWEvaDZI4euDI7nY8o5af90DnHfJ cHALga38w672uE2TWTI6RRBQD5+v8xQSGutHpN66ZbRAKJEOppJ47YO4kkNsWGDKjKYasGzWz4w8c
2022-03-26 06:59:51 UTC	9	IN	Data Raw: 6c 65 61 73 65 20 74 75 72 6e 20 4a 61 76 61 53 63 72 69 70 74 20 6f 6e 20 61 6e 64 20 72 65 6c 6f 61 64 20 74 68 65 20 70 61 67 65 2e 3c 2f 68 31 3e 0a 20 20 3c 2f 6e 6f 73 63 72 69 70 74 3e 0a 20 20 20 20 3c 64 69 76 20 69 64 3d 22 6e 6f 2d 63 6f 6f 6b 69 65 2d 77 61 72 6e 69 6e 67 22 20 63 6c 61 73 73 3d 22 63 6f 6f 6b 69 65 2d 77 61 72 6e 69 6e 67 22 20 64 61 74 61 2d 74 72 61 6e 73 6c 61 74 65 3d 22 74 75 72 6e 5f 6f 6e 5f 63 6f 6f 6b 69 65 73 22 20 73 74 79 6c 65 3d 22 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 22 3e 0a 20 20 20 20 20 20 3c 70 20 64 61 74 61 2d 74 72 61 6e 73 6c 61 74 65 3d 22 74 75 72 6e 5f 6f 6e 5f 63 6f 6f 6b 69 65 73 22 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 62 64 32 34 32 36 3b 22 3e 50 6c 65 61 73 65 20 65 6e 61 62 6c 65 20 43 Data Ascii: lease turn JavaScript on and reload the page.</h1> </noscript> <p data-translate="turn_on_cookies" style="color:#bd2426;">Please enable C
2022-03-26 06:59:51 UTC	10	IN	Data Raw: 20 20 20 20 20 20 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 74 72 6b 6a 73 29 3b 0a 20 20 20 20 20 20 20 20 76 61 72 20 63 70 6f 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 3b 0a 20 20 20 20 20 20 20 20 63 70 6f 2e 74 79 70 65 3d 27 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 27 3b 0a 20 20 20 20 20 20 20 20 63 70 6f 2e 73 72 63 3d 22 2f 63 64 6e 2d 63 67 69 2f 63 68 61 6c 6c 65 6e 67 65 2d 70 6c 61 74 66 6f 72 6d 2f 68 2f 62 2f 6f 72 63 68 65 73 74 72 61 74 65 2f 6d 61 6e 61 67 65 64 2f 76 31 3f 72 61 79 3d 36 66 31 65 30 31 38 35 63 38 37 38 38 66 66 61 22 3b 0a 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 77 69 6e 64 6f 77 2e 5f 63 66 5f 63 68 6c 5f 6f 70 Data Ascii: document.body.appendChild(trkjs); var cpo=document.createElement('script'); cpo.type='text/javascript'; cpo.src="/cdn-cgi/challenge-platform/h/b/orchestrate/managed/v1?ray=6f1e0185c8788ffa"; window._cf_chl_op
2022-03-26 06:59:51 UTC	12	IN	Data Raw: 3d 22 63 66 2d 73 65 63 74 69 6f 6e 20 63 66 2d 77 72 61 70 70 65 72 22 3e 0a 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 66 2d 63 6f 6c 75 6d 6e 73 20 74 77 6f 22 3e 0a 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 66 2d 63 6f 6c 75 6d 6e 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 68 32 20 64 61 74 61 2d 74 72 61 6e 73 6c 61 74 65 3d 22 77 68 79 5f 63 61 70 74 63 68 61 5f 68 65 61 64 6c 69 6e 65 22 3e 57 68 79 20 64 6f 20 49 20 68 61 76 65 20 74 6f 20 63 6f 6d 70 6c 65 74 65 20 61 20 43 41 50 54 43 48 41 3f 3c 2f 68 32 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 70 20 64 61 74 61 2d 74 72 61 6e 73 6c 61 74 65 3d 22 77 68 79 5f 63 61 70 74 63 68 61 5f 64 65 74 61 69 6c Data Ascii: ="cf-section cf-wrapper"> <h2 data-translate="why_captcha_headline">Why do I have to complete a CAPTCHA?</h2> <p data-translate="why_captcha_detail
2022-03-26 06:59:51 UTC	13	IN	Data Raw: 61 6e 3e 0a 20 20 20 20 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 63 66 2d 66 6f 6f 74 65 72 2d 73 65 70 61 72 61 74 6f 72 20 73 6d 3a 68 69 64 64 65 6e 22 3e 26 62 75 6c 6c 3b 3c 2f 73 70 61 6e 3e 0a 20 20 20 20 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 63 66 2d 66 6f 6f 74 65 72 2d 69 74 65 6d 20 73 6d 3a 62 6c 6f 63 6b 20 73 6d 3a 6d 62 2d 31 22 3e 3c 73 70 61 6e 3e 59 6f 75 72 20 49 50 3c 2f 73 70 61 6e 3e 3a 20 38 34 2e 31 37 2e 35 32 2e 37 35 3c 2f 73 70 61 6e 3e 0a 20 20 20 20 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 63 66 2d 66 6f 6f 74 65 72 2d 73 65 70 61 72 61 74 6f 72 20 73 6d 3a 68 69 64 64 65 6e 22 3e 26 62 75 6c 6c 3b 3c 2f 73 70 61 6e 3e 0a 20 20 20 20 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 63 66 2d 66 6f 6f 74 65 72 2d 69 74 65 6d 20 73 6d 3a 62 Data Ascii: an> • Your IP: 84.17.52.75 • <span class="cf-footer-item sm:b
2022-03-26 06:59:51 UTC	14	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

FTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Mar 26, 2022 08:00:23.518426895 CET	21	49792	145.14.144.149	192.168.2.4	220 ProFTPD Server (000webhost.com) [::ffff:145.14.144.149]
Mar 26, 2022 08:00:23.523405075 CET	49792	21	192.168.2.4	145.14.144.149	USER fcb-aws-host-4
Mar 26, 2022 08:00:24.476912975 CET	21	49792	145.14.144.149	192.168.2.4	500 USER: Operation not permitted

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: 7.exe PID: **6464**, Parent PID: **5500**

General

Target ID:	0
Start time:	07:59:33
Start date:	26/03/2022
Path:	C:\Users\user\Desktop\7.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\7.exe"
Imagebase:	0x140000
File size:	913920 bytes
MD5 hash:	ED666BF7F4A0766FCEC0E9C8074B089B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.515370288.0000000000142000.00000002.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.515370288.0000000000142000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.515370288.0000000000142000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.515370288.0000000000142000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.515370288.0000000000142000.00000002.00000001.01000000.00000003.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.518144940.0000000003771000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.518144940.0000000003771000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000000.00000002.521204607.0000000007650000.00000004.08000000.00040000.00000000.sdmp, Author: Arnim Rupp • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000000.00000002.521214363.0000000007660000.00000004.08000000.00040000.00000000.sdmp, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000000.244290044.0000000000142000.00000002.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000000.244290044.0000000000142000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000000.244290044.0000000000142000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000000.244290044.0000000000142000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000000.244290044.0000000000142000.00000002.00000001.01000000.00000003.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.516506794.0000000002771000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.516506794.0000000002771000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	726960AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	726960AC	unknown
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	726960AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	726960AC	unknown
C:\Users\user\AppData\Roaming\pid.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	ABBCAB	CreateFileW
C:\Users\user\AppData\Roaming\pidloc.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	ABBCAB	CreateFileW
C:\Users\user\AppData\Roaming\WindowsUpdate.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	4A061AC	CopyFileW
C:\Users\user\AppData\Roaming\WindowsUpdate.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	4A061AC	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holdermail.txt	success or wait	1	4A06A9A	DeleteFileW
C:\Users\user\AppData\Local\Temp\holderwb.txt	success or wait	1	4A06A9A	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	0	4	36 34 36 34	6464	success or wait	1	4A00093	WriteFile
C:\Users\user\AppData\Roaming\pidloc.txt	0	28	43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 5c 37 2e 65 78 65	C:\Users\user\Desktop\7.exe	success or wait	1	4A00093	WriteFile
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 43 fd 61 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 08 00 00 fd 07 00 00 34 00 00 00 00 00 00 fd 0b 08 00 00 20 00 00 00 00 00 00 00 00 40 00 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 fd 08 00 00 02 00 00 00 00 00 00 02 00 40 fd 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.$PELCa4 @ @	success or wait	4	4A061AC	CopyFileW
C:\Users\user\AppData\Roaming\WindowsUpdate.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	4A061AC	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	726C5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	726C5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	726C8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	726C5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	726C5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	4A00093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4A00093	ReadFile
C:\Users\user\AppData\Local\Temp\holdermail.txt	unknown	4096	end of file	1	4A00093	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7276BF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7276BF06	unknown
C:\Windows\assembly\GAC_MSIL\System.Runtime.Remoting\2.0.0.0__b77a5c561934e089\System.Runtime.Remoting.dll	unknown	4096	success or wait	1	7276BF06	unknown
C:\Windows\assembly\GAC_MSIL\System.Runtime.Remoting\2.0.0.0__b77a5c561934e089\System.Runtime.Remoting.dll	unknown	512	success or wait	1	7276BF06	unknown
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	success or wait	1	4A00093	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	end of file	1	4A00093	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Windows Update	unicode	C:\Users\user\AppData\Roaming\WindowsUpdate.exe	success or wait	1	4A0629E	RegSetValueExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Hidden	dword	2	1	success or wait	1	4A05E92	RegSetValueExW

Analysis Process: vbc.exe PID: **7048**, Parent PID: **6464**

General

Target ID:	6
Start time:	07:59:54
Start date:	26/03/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext "C:\Users\user\AppData\Local\Temp\holdermail.txt"
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000006.00000000.294953383.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000006.00000000.294308364.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000006.00000000.293577766.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000006.00000002.298222590.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holdermail.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405EFC	CreateFileA

Analysis Process: vbc.exe PID: **7064**, Parent PID: **6464**

General

Target ID:	7
Start time:	07:59:54
Start date:	26/03/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext "C:\Users\user\AppData\Local\Temp\holderwb.txt"
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000000.295698908.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000002.336555805.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000000.294642291.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000000.295228513.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bhv4267.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40750C	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\holderwb.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	407175	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bhv4267.tmp	success or wait	1	40909B	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bhv4267.tmp	0	29884416	fd 6b fd 0f fd 6b fd 20 06 00 00 00 00 00 00 fd 3f 00 00 00 00 00 00 5f 65 fd fd 2a 0c 12 1b 06 77 fd 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 3d 00 0f 00 00 00 14 2b 09 08 03 7a 1b 0c 10 3b 06 1a 03 7a 23 0a 68 02 3f 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 62 fd fd fd 2a 0c 12 1b 06 77 fd 0c 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 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 00 00 00 00 00 00 00 00 00 00 00 00 7b 00 00 00 0a 00 00 00 00 00 00 00 fd 42 00 00 00 00 00 00 14 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	k ?_e*w=+z;z#h?b*w{B	success or wait	1	408C26	WriteFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	0	2	fd fd		success or wait	1	407BCF	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bhv4267.tmp	unknown	1024	success or wait	1	407BB0	ReadFile
C:\Users\user\AppData\Local\Temp\bhv4267.tmp	unknown	32768	success or wait	2	407BB0	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bhv4267.tmp	unknown	32768	success or wait	3	407BB0	ReadFile
C:\Users\user\AppData\Local\Temp\bhv4267.tmp	unknown	32768	success or wait	1	407BB0	ReadFile
C:\Users\user\AppData\Local\Temp\bhv4267.tmp	unknown	32768	success or wait	6	407BB0	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	100	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	100	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	2048	success or wait	1	414E52	ReadFile

Analysis Process: WindowsUpdate.exe PID: **5692**, Parent PID: **3616**

General

Target ID:	11
Start time:	08:00:03
Start date:	26/03/2022
Path:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\WindowsUpdate.exe"
Imagebase:	0x4a0000
File size:	913920 bytes
MD5 hash:	ED666BF7F4A0766FCEC0E9C8074B089B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000B.00000002.319064303.00000000004A2000.00000002.00000001.01000000.00000008.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000002.319064303.00000000004A2000.00000002.00000001.01000000.00000008.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000B.00000002.319064303.00000000004A2000.00000002.00000001.01000000.00000008.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000B.00000002.319064303.00000000004A2000.00000002.00000001.01000000.00000008.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000B.00000002.319064303.00000000004A2000.00000002.00000001.01000000.00000008.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000B.00000000.311517267.00000000004A2000.00000002.00000001.01000000.00000008.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000000.311517267.00000000004A2000.00000002.00000001.01000000.00000008.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000B.00000000.311517267.00000000004A2000.00000002.00000001.01000000.00000008.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000B.00000000.311517267.00000000004A2000.00000002.00000001.01000000.00000008.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000B.00000000.311517267.00000000004A2000.00000002.00000001.01000000.00000008.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\Users\user\AppData\Roaming\WindowsUpdate.exe, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 69%, Metadefender, Browse • Detection: 95%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	726960AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	726960AC	unknown
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	726960AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	726960AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\WindowsUpdate.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	726834A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\WindowsUpdate.exe.log	0	916	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e 6e	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7296A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	726C5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	726C5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	726C8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	726C5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	726C5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	29C0093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	29C0093	ReadFile

Analysis Process: WindowsUpdate.exe PID: **2372**, Parent PID: **3616**

General

Target ID:	13
Start time:	08:00:14
Start date:	26/03/2022
Path:	C:\Users\user\AppData\Roaming\WindowsUpdate.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\WindowsUpdate.exe"
Imagebase:	0xc90000
File size:	913920 bytes
MD5 hash:	ED666BF7F4A0766FCEC0E9C8074B089B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000D.00000002.336007062.0000000000C92000.00000002.00000001.01000000.00000008.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000D.00000002.336007062.0000000000C92000.00000002.00000001.01000000.00000008.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000D.00000002.336007062.0000000000C92000.00000002.00000001.01000000.00000008.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000D.00000002.336007062.0000000000C92000.00000002.00000001.01000000.00000008.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000D.00000002.336007062.0000000000C92000.00000002.00000001.01000000.00000008.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000D.00000000.331712368.0000000000C92000.00000002.00000001.01000000.00000008.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000D.00000000.331712368.0000000000C92000.00000002.00000001.01000000.00000008.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000D.00000000.331712368.0000000000C92000.00000002.00000001.01000000.00000008.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000D.00000000.331712368.0000000000C92000.00000002.00000001.01000000.00000008.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000D.00000000.331712368.0000000000C92000.00000002.00000001.01000000.00000008.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	726960AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	726960AC	unknown
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	726960AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	726960AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	726C5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	726C5544	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	726C8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	726C5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	726C5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	5920093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5920093	ReadFile

Disassembly

No disassembly