ID: 620800
Sample Name: vjfhD2yGrp
Cookbook: default.jbs
Time: 08:59:33
Date: 05/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report vjfhD2yGrp 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Signatures 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
System Summary 5
Malware Analysis System Evasion 5
Anti Debugging 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 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 10
World Map of Contacted IPs 13
Public IPs 14
Private 14
General Information 14
Warnings 15
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASNs 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\2D85F72862B55C4EADD9E66E06947F3D 15
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506 16
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\2D85F72862B55C4EADD9E66E06947F3D 16
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506 16
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vjfhD2yGrp.exe.log 17
Static File Info 17
General 17
File Icon 17
Static PE Info 17
General 18
Entrypoint Preview 18
Data Directories 20
Sections 20
Resources 20
Imports 20
Version Infos 20
Network Behavior 21
TCP Packets 21
UDP Packets 21
DNS Queries 22
DNS Answers 22
SMTP Packets 22
Statistics 22
Behavior 22

System Behavior 22
Analysis Process: vjfhD2yGrp.exePID: 6452, Parent PID: 2300 22
General 22
File Activities 23
File Created 23
File Written 23
File Read 24
Analysis Process: vjfhD2yGrp.exePID: 6788, Parent PID: 6452 24
General 24
File Activities 24
File Created 24
File Read 25
Disassembly 25

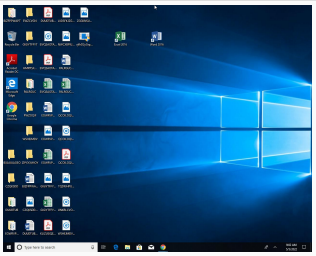
Windows Analysis Report

vjfhD2yGrp

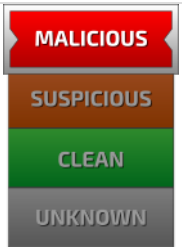
Overview

General Information

Sample Name:	vjfhD2yGrp (renamed file extension from none to exe)
Analysis ID:	620800
MD5:	186652d7ffc900e..
SHA1:	a298ae3f26515b..
SHA256:	372f3ede21d2dc..
Tags:	32 exe
Infos:	



Detection



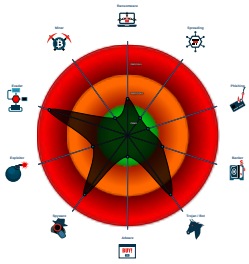
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…
- .NET source code contains very larg…

Classification



Process Tree

- **System is w10x64**
- vjfhD2yGrp.exe (PID: 6452 cmdline: "C:\Users\user\Desktop\vjfhD2yGrp.exe" MD5: 186652D7FFC900EB5BF55E72C7FF07D8)
  - vjfhD2yGrp.exe (PID: 6788 cmdline: C:\Users\user\Desktop\vjfhD2yGrp.exe MD5: 186652D7FFC900EB5BF55E72C7FF07D8)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "home@hardroot.biz",
  "Password": "bigboy247",
  "Host": "mail.hardroot.biz"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000000.298815911.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000000.298815911.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000006.00000000.300624674.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000000.300624674.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000000.298205555.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.0.vjfhD2yGrp.exe.400000.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.0.vjfhD2yGrp.exe.400000.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
6.0.vjfhD2yGrp.exe.400000.6.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32b42:$s10: logins • 0x325a9:$s11: credential • 0x2eba7:$g1: get_Clipboard • 0x2ebb5:$g2: get_Keyboard • 0x2ebc2:$g3: get_Password • 0x2fe9f:$g4: get_CtrlKeyDown • 0x2feaf:$g5: get_ShiftKeyDown • 0x2fec0:$g6: get_AltKeyDown
0.2.vjfhD2yGrp.exe.4488dd0.7.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.vjfhD2yGrp.exe.4488dd0.7.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 30 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Machine Learning detection for sample

System Summary

- Malicious sample detected (through community Yara rule)
- .NET source code contains very large array initializations
- PE file has nameless sections
- PE file contains section with special chars

Malware Analysis System Evasion

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Anti Debugging

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

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

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

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality

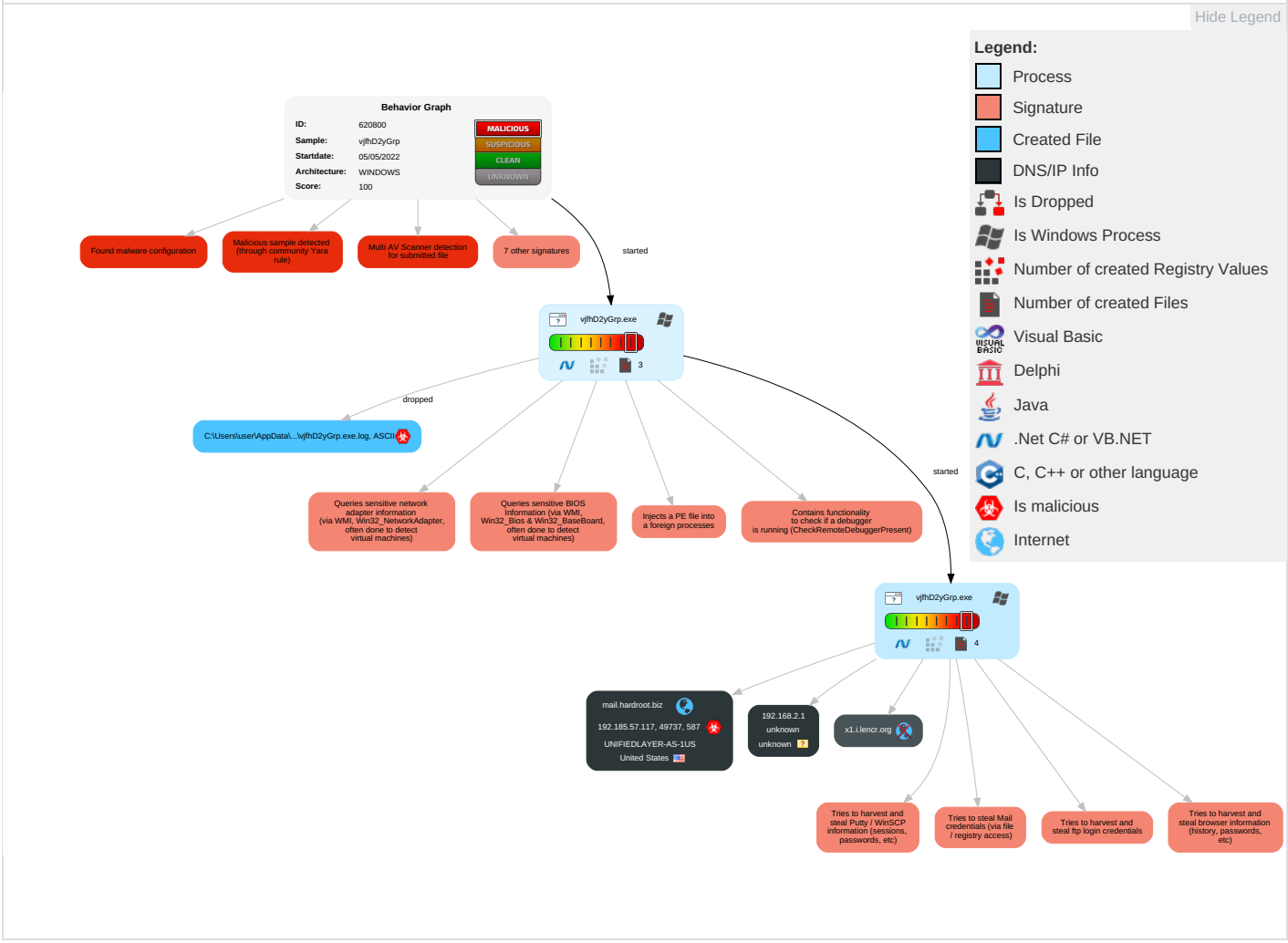
Yara detected AgentTesla

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
Valid Accounts	2 1 1 Windows Management Instrumentation	1 DLL Side-Loading	1 1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	1 Query Registry	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Disable or Modify Tools	1 Credentials in Registry	3 2 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 4 1 Virtualization/Sandbox Evasion	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	1 Application Layer Protocol	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 1 Process Injection	NTDS	1 4 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	4 Software Packing	DCSync	1 1 4 System Information 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	1 Timestomp	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 DLL Side-Loading	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

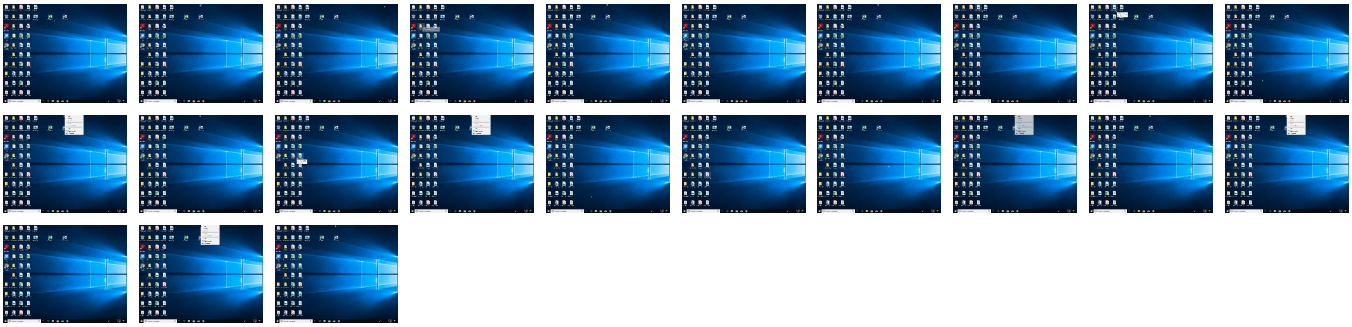
Behavior Graph



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
vjfhD2yGrp.exe	39%	Virustotal		Browse
vjfhD2yGrp.exe	40%	ReversingLabs	Win32.Trojan.Pwsx	
vjfhD2yGrp.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.vjfhD2yGrp.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.vjfhD2yGrp.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.2.vjfhD2yGrp.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.vjfhD2yGrp.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.vjfhD2yGrp.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.vjfhD2yGrp.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
x1.i.lencr.org	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnO	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com2	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://VCKitrOpZNoTw.netpx	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn-u	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://mail.hardroot.biz	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comg	0%	Avira URL Cloud	safe	
http://hdgJLE.com	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comm	0%	Avira URL Cloud	safe	
http://x1.i.lencr.org/	0%	URL Reputation	safe	
http://www.carterandcone.comNDOu	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.founder.com.cn/cnTC	0%	URL Reputation	safe	
http://VCKitrOpZNoTw.net	0%	Avira URL Cloud	safe	
http://www.carterandcone.comraG	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comldTF	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn8	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comm(	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.hardroot.biz	192.185.57.117	true	true		unknown
x1.i.lencr.org	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

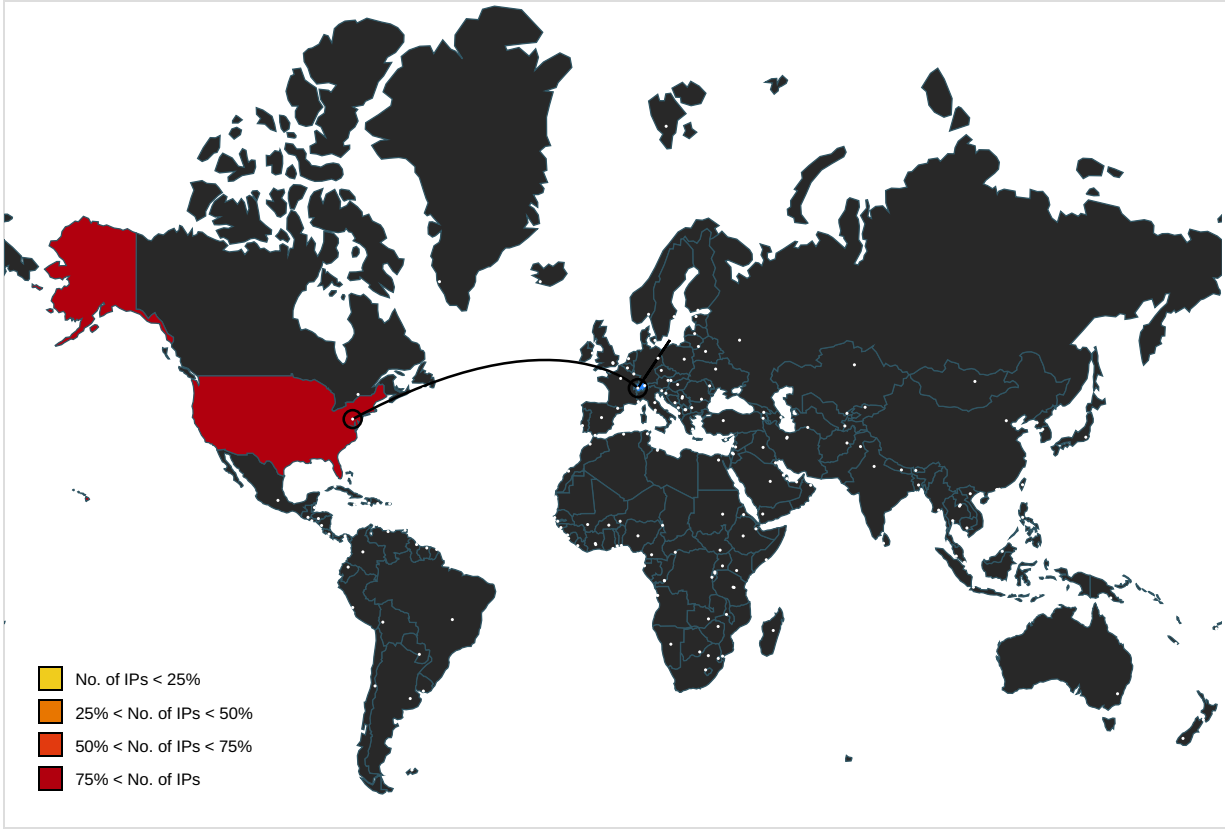
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnO	vjfhD2yGrp.exe, 00000000.00000003.268818336.0000000007CAD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	vjfhD2yGrp.exe, 00000006.00000002.539452466.0000000002C41000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.com2	vjfhD2yGrp.exe, 00000000.00000003.266472729.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.266500675.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.266426109.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://VCKitrOpZNoTw.netpx	vjfhD2yGrp.exe, 00000006.00000002.539452466.0000000002C41000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersC	vjfhD2yGrp.exe, 00000000.00000003.276649117.0000000007CA6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	vjfhD2yGrp.exe, 00000000.00000003.274048570.0000000007CA6000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.274976297.0000000007CA6000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.275561673.0000000007CA6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	vjfhD2yGrp.exe, 00000000.00000003.269484995.0000000007C85000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.270021035.0000000007C75000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://r3.i.lencr.org/0	vjfhD2yGrp.exe, 00000006.00000002.539929236.0000000002F98000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	vjfhD2yGrp.exe, 00000000.00000003.266669316.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.266872142.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.266699957.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.266739881.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.266587139.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.266472729.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.266500675.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.266901941.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.266426109.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cno	vjfhD2yGrp.exe, 00000000.00000003.268747522.0000000007C7C000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.268722975.0000000007C72000.00000004.00000800.00020000.00000000.sdmp	false		unknown
http://www.typography.netD	vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://x1.c.lencr.org/0	vjfhD2yGrp.exe, 00000006.00000002.539929236.0000000002F98000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://x1.i.lencr.org/0	vjfhD2yGrp.exe, 00000006.00000002.539929236.0000000002F98000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	vjfhD2yGrp.exe, 00000006.00000002.539452466.0000000002C41000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersb	vjfhD2yGrp.exe, 00000000.00000003.277383591.0000000007CA6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://r3.o.lencr.org0	vjfhD2yGrp.exe, 00000006.00000002.539929236.0000000002F98000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnn-u	vjfhD2yGrp.exe, 00000000.00000003.268898497.0000000007C7C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	vjfhD2yGrp.exe, 00000000.00000003.269889298.0000000007C7A000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.come	vjfhD2yGrp.exe, 00000000.00000003.266669316.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.266872142.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.266699957.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.266739881.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.266901941.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	vjfhD2yGrp.exe, 00000000.00000002.311516219.000000008E82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://mail.hardroot.biz	vjfhD2yGrp.exe, 00000006.00000002.539929236.0000000002F98000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comg	vjfhD2yGrp.exe, 00000000.00000003.266669316.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.266872142.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.266699957.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.266739881.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.266587139.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.266901941.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://hdgJLE.com	vjfhD2yGrp.exe, 00000006.00000002.539452466.0000000002C41000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comm	vjfhD2yGrp.exe, 00000000.00000003.266872142.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.266901941.0000000007C8B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	vjfhD2yGrp.exe, 00000000.00000002.311516219.000000008E82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	vjfhD2yGrp.exe, 00000000.00000002.311516219.000000008E82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://x1.i.lencr.org/	2D85F72862B55C4EADD9E66E06947F3D.6.dr	false	• URL Reputation: safe	unknown
http://www.carterandcone.comNDOu	vjfhD2yGrp.exe, 00000000.00000003.269889298.0000000007C7A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.letsencrypt.org0	vjfhD2yGrp.exe, 00000006.00000002.539929236.0000000002F98000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.htmls	vjfhD2yGrp.exe, 00000000.00000003.275508617.0000000007C7A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	vjfhD2yGrp.exe, 00000006.00000002.539452466.0000000002C41000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnTC	vjfhD2yGrp.exe, 00000000.00000003.268898497.0000000007C7C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://VCKitrOpZNoTw.net	vjfhD2yGrp.exe, 00000006.00000002.539452466.0000000002C41000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comraG	vjfhD2yGrp.exe, 00000000.00000003.269889298.0000000007C7A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersg:	vjfhD2yGrp.exe, 00000000.00000003.274838284.0000000007CA6000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.274933091.0000000007CA6000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.274714940.0000000007CA6000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.275561673.0000000007CA6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://en.w	vjfhD2yGrp.exe, 00000000.00000003.269889298.0000000007C7A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersM:	vjfhD2yGrp.exe, 00000000.00000003.276649117.0000000007CA6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	vjfhD2yGrp.exe, 00000000.00000003.268747522.0000000007C7C000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.268818336.0000000007CAD000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000003.268722975.0000000007C72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers-	vjfhD2yGrp.exe, 00000000.00000003.274714940.0000000007CA6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/frere-jones.html	vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	vjfhD2yGrp.exe, 00000000.00000003.276562616.0000000007CA6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comldTF	vjfhD2yGrp.exe, 00000000.00000003.302267026.0000000007C70000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000002.311308444.0000000007C70000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn8	vjfhD2yGrp.exe, 00000000.00000003.268898497.0000000007C7C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comm	vjfhD2yGrp.exe, 00000000.00000003.302267026.0000000007C70000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000002.311308444.0000000007C70000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlX	vjfhD2yGrp.exe, 00000000.00000003.276562616.0000000007CA6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers8	vjfhD2yGrp.exe, 00000000.00000002.311516219.0000000008E82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comm(	vjfhD2yGrp.exe, 00000000.00000003.302267026.0000000007C70000.00000004.00000800.00020000.00000000.sdmp, vjfhD2yGrp.exe, 00000000.00000002.311308444.0000000007C70000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.57.117	mail.hardroot.biz	United States		46606	UNIFIEDLAYER-AS-1US	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	620800
Start date and time: 05/05/202208:59:33	2022-05-05 08:59:33 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	vjfhD2yGrp (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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/5@2/2

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1% (good quality ratio 0.4%) • Quality average: 30.3% • Quality standard deviation: 38.5%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.50.97.168, 8.248.115.254, 67.26.139.254, 8.241.126.249, 8.241.126.121, 8.248.149.254, 173.222.108.210, 173.222.108.226
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, fs.microsoft.com, e8652.dscx.akamaiedge.net, settings-win.data.microsoft.com, ctldl.windowsupdate.com, a767.dspw65.akamai.net, arc.msn.com, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net, ris.api.iris.microsoft.com, go.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, crl.root-x1.letsencrypt.org.edgekey.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory 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
09:00:54	API Interceptor	673x Sleep call for process: vjfhD2yGrp.exe modified

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\LocalLow\Microsoft\CryptnetUrlCache\Content\2D85F72862B55C4EADD9E66E06947F3D

Process:	C:\Users\user\Desktop\vjfhD2yGrp.exe
File Type:	data

Category:	dropped
Size (bytes):	1391
Entropy (8bit):	7.705940075877404
Encrypted:	false
SSDEEP:	24:ooVdTH2NMU+I3E0Ulcrgdaf3sWrATrnkC4EmCUkmGMkfQo1fSZotWzD1:ooVguI3Kcx8WIzNeCUkJMmSuMX1
MD5:	0CD2F9E0DA1773E9ED864DA5E370E74E
SHA1:	CABD2A79A1076A31F21D253635CB039D4329A5E8
SHA-256:	96BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C6
SHA-512:	3B40F27E828323F5B91F8909883A78A21C86551761F27B38029FAAEC14AF5B7AA96FB9F9CC93EE201B5EB1D0FEF17B290747E8B839D2E49A8F36C5EBF3C7C910
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..k0..S.....@.YDc.c...0...*.H.....0O1.0...U....US1)0'..U... Internet Security Research Group1.0...U....ISRG Root X10...1506041104 38Z..3506041104 38Z0O1.0...U... .US1)0'..U... Internet Security Research Group1.0...U....ISRG Root X10.."0...*.H.....0.....$s..7.+W(.....8..n<.W.x.u...jn..O(..h.lD...c...k....1.!~.3<.H..y.....!.K...qiJffl.~<p. .)".....K...~....G.|.H#S.8.O.o...IW..t../.8.{.p!.u.0<.....c...O..K~.....w...{J.L.%.p..)..S$.....J.?..aQ.....cq...o[...\4ylv.;.by.../&.....6....7..6u...r.....l.....*.A..v.....5/(.l....dwn G7..Y^h..r...A)>Y>.&.$...Z.L@.F....:Qn.;.}r...xY.>Qx...../..>{J.Ks.....P.|C.t..t.....0.[q6....00\H..;..}`...).....A.....|.;F.H*..v.v..j.=...8.d..+..(.....B.".'].y...p..N..:..'Qn..d.3CO.....B0 @0...U.....0...U.....0....0...U.....y.Y.{....s.....X..n0...*.H.....U.X....P.....i ').au\.n...i/..VK..s.Y.!.~.Lq..`.9....!V..P.Y...Y.....b.E.f..|o..;....'...}~.."....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\Desktop\vjfhD2yGrp.exe
File Type:	Microsoft Cabinet archive data, 61480 bytes, 1 file
Category:	dropped
Size (bytes):	61480
Entropy (8bit):	**7.9951219482618905**
Encrypted:	**true**
SSDEEP:	1536:kmu7iDG/SCACih0/8uIGantJdjFpTE8lTeNjiXKGgUN:CeGf5gKsG4vdjFpjlYeX9gUN
MD5:	B9F21D8DB36E88831E5352BB82C438B3
SHA1:	4A3C330954F9F65A2F5FD7E55800E46CE228A3E2
SHA-256:	998E0209690A48ED33B79AF30FC13851E3E3416BED97E3679B6030C10CAB361E
SHA-512:	D4A2AC7C14227FBAF8B532398FB69053F0A0D913273F6917027C8CADBBA80113FDBEC20C2A7EB31B7BB57C99F9FDECCF8576BE5F39346D8B564FC72FB1699476
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....(.....,.....I.....y.....Tbr .authroot.stl..$..4..CK..<Tk...c_.d....A.K.....Y.f....!.))$7*I.....e..eKT..k....n.3.....S..9.s.....3H.Mh.....qV.=M6.=.4.F.....V:F..]..... B`....Q...c"U.0.n....J.....4.....i7s..:.27...._...+).IE..he.4|.?,...h....7..PA..b.,. .....#1+..o...g.....2n1m...=.....Dp.;..f..ljX.Dx..r<'.1RI3B0<w.D.z..)D|..8<..c+..'XH..K,.Y..d.j.<.A... ....I_lVb[w..rDp...'.....nL....!G.F....f.fX..r.. ?.....v(...L..<.\.Z..g;.>.0v...P .....|...A..(..x...T0.`g...c..7.U?...9.p..a..&..9.....sV..l0..D..fhi..h.F....q...y.....Mq].4..Z.....={L....AS..9.....:'..... ...+..P.N....EAQ.V. sr.....y.B.`.Efe..8../....$...y-.q.J.....nP...2.Q8...O.....M.@\.>=X....V..z.4.=.@...ws.N.M3.S.c?.....C4]?..\.K.9.....^...CU.....O....X.`.....,_.gU...*..V.{V6..m ..D.-|.Q.t.7.....9.~....[...I.<e...~$..>.....s.I.S....~1..IV.2Ri:..]R!8...q...I.X.%.)@.....2.gb,t...}..;...@.Z..<q..y..:...e3..cY.we.$....z..| .#.....I...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\2D85F72862B55C4EADD9E66E06947F3D

Process:	C:\Users\user\Desktop\vjfhD2yGrp.exe
File Type:	data
Category:	dropped
Size (bytes):	192
Entropy (8bit):	2.7633865340992063
Encrypted:	false
SSDEEP:	3:kkFklt1JE/XfllXlE/zMccvNNX8RolJuRdyo1dlUKlGXJlDdt:kKYk81cVNMa8Rdy+UKcXP
MD5:	8A8A662FFB7D99EC5092CC14FD80826D
SHA1:	71829B131F2A17701228332C148E094FAD1F9838
SHA-256:	6054515D09A4804283ED0687CBBD315D6C3C0B66A2439D14D4B408A0177A973B
SHA-512:	D2BC03A21EA3EC15F90FC2BC60BAC2BAE99C764F71E15FF8060731EDF41232B8F6F96F48005C47724A2810792F84EBD25404C83D71E5BB6E60E9E4847000694
Malicious:	false
Reputation:	low
Preview:	p..... .....`..(..... .....~.....o...h.t.t.p.:././.x.1...i...l.e.n.c.r...o.r.g./..."..5.a.6.2.8.1.5.c.-.5.6.f."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\Desktop\vjfhD2yGrp.exe
File Type:	data
Category:	modified
Size (bytes):	330
Entropy (8bit):	3.122093209666636
Encrypted:	false

SSDEEP:	6:kKRdoJN+SkQlPlEGYRMY9z+4KlDA3RUesJ21:LkPlE99SNxAhUesE1
MD5:	A1E4FACDBE0DE7A08F26F2C2692E8409
SHA1:	B57235D96B4E3BF010B3C5014771AACB63EEBB24
SHA-256:	6F40FFD572E87151621DAB8C0AE3852AA6D6CD18DF1896D7F492D56AEF2A2D19
SHA-512:	01C12C9B70C7509B8D06E120D731E1C5D66A7A383BAD08531C7E1033A7D73818A343C9E62255C811C2C39F80496A4979BCAC5EC7580B91B69E76EE022BAAC1 5
Malicious:	false
Reputation:	low
Preview:	p..... ...../.`..(..... .....3k/"[.....(.....(...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".8.0.3.3.6.b.2.f.2.2.5.b.d.8.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vjfhD2yGrp.exe.log

Process:	C:\Users\user\Desktop\vjfhD2yGrp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:ML9E4Ks29E4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MxHKX9HKx1qHiYHKhQnoPtHoxHhAHKzu
MD5:	36C0A7F32E757FCBECED4EB6FC3C922C
SHA1:	939BED45186769E4D878B9A44420CE140445F2CB
SHA-256:	C85B76D06B14DE0D203F30A03BA1D26F17BA9970FE8491AB00A1ED1C0DEC9989
SHA-512:	F0C308E83AE3FB61E9A7AA68E2CA54D9D48027DF1E8D8092C1FA61600555005675063F377C50572C34A39E8CC77FC044EAF2BC31D5C08DC46446C38F4433DF1
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken= b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni .dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\S ystem.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b 77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.917880959694303
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	vjfhD2yGrp.exe
File size:	626176
MD5:	186652d7ffc900eb5bf55e72c7ff07d8
SHA1:	a298ae3f26515bf2795dff5e415f01184e00fee0
SHA256:	372f3ede21d2dc6c7f2ef29b36a29f8473ddb9d069c5a29cab5d26f9b6f3ecda
SHA512:	2f5088b8d7091a1525d49d40c2ece63a684462f552e6cbe617d83da28e2365a0caa7864b556acef1138f2c08c8cdd95053cbd3642afb705c2b7313546223ee84
SSDEEP:	12288:kSatuEQ+PG9gTs8J48y12L2I23fh3jCjsu68jpCr6p9qgBX3:kSa82wfVOsuRjMrIq6X3
TLSH:	2BD4D09C7661B2EFC867D4B2DE980DA4FA55397B931B0243E02316ADD90C49BDF244F2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...TXZ.....0..... ....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x4a000a
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xC05A5854 [Wed Apr 6 05:32:04 2072 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [004A0000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Instruction
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe898	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9c000	0x438	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9e000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xa0000	0x8	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0xe000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
M'M)[6	0x2000	0xbca0	0xbe00	False	1.00043174342	data	7.99597055972	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0xe000	0x8c1a8	0x8c200	False	0.922706079951	data	7.91525345421	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x9c000	0x438	0x600	False	0.2890625	data	2.47024216681	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9e000	0xc	0x200	False	0.044921875	data	0.0776331623432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
	0xa0000	0x10	0x200	False	0.04296875	data	0.101910425663	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x9c058	0x3dc	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020-2021 by David Xanatos (xanasoft.com)
Assembly Version	1.0.0.0
InternalName	AssemblyDescriptionAttrib.exe
FileVersion	1.0.0.0
CompanyName	sandboxie-plus.com
LegalTrademarks	
Comments	
ProductName	Sandboxie
ProductVersion	1.0.0.0

Description	Data
FileDescription	Sandboxie Installer
OriginalFilename	AssemblyDescriptionAttrib.exe

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2022 09:01:12.000746012 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:01:12.137536049 CEST	587	49737	192.185.57.117	192.168.2.3
May 5, 2022 09:01:12.137695074 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:01:14.156817913 CEST	587	49737	192.185.57.117	192.168.2.3
May 5, 2022 09:01:14.245843887 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:01:14.383192062 CEST	587	49737	192.185.57.117	192.168.2.3
May 5, 2022 09:01:14.383460999 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:01:14.527405024 CEST	587	49737	192.185.57.117	192.168.2.3
May 5, 2022 09:01:14.605276108 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:01:14.762491941 CEST	587	49737	192.185.57.117	192.168.2.3
May 5, 2022 09:01:14.762525082 CEST	587	49737	192.185.57.117	192.168.2.3
May 5, 2022 09:01:14.762547970 CEST	587	49737	192.185.57.117	192.168.2.3
May 5, 2022 09:01:14.762756109 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:01:16.645154953 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:01:16.793016911 CEST	587	49737	192.185.57.117	192.168.2.3
May 5, 2022 09:01:16.874833107 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:01:21.267862082 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:01:21.404855013 CEST	587	49737	192.185.57.117	192.168.2.3
May 5, 2022 09:01:21.411225080 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:01:21.550159931 CEST	587	49737	192.185.57.117	192.168.2.3
May 5, 2022 09:01:21.550985098 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:01:21.709300041 CEST	587	49737	192.185.57.117	192.168.2.3
May 5, 2022 09:01:21.714469910 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:01:21.851115942 CEST	587	49737	192.185.57.117	192.168.2.3
May 5, 2022 09:01:21.851669073 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:01:22.009010077 CEST	587	49737	192.185.57.117	192.168.2.3
May 5, 2022 09:01:22.010184050 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:01:22.153417110 CEST	587	49737	192.185.57.117	192.168.2.3
May 5, 2022 09:01:22.157120943 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:01:22.157319069 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:01:22.165695906 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:01:22.165859938 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:01:22.293642044 CEST	587	49737	192.185.57.117	192.168.2.3
May 5, 2022 09:01:22.293667078 CEST	587	49737	192.185.57.117	192.168.2.3
May 5, 2022 09:01:22.302448034 CEST	587	49737	192.185.57.117	192.168.2.3
May 5, 2022 09:01:22.302472115 CEST	587	49737	192.185.57.117	192.168.2.3
May 5, 2022 09:01:22.311942101 CEST	587	49737	192.185.57.117	192.168.2.3
May 5, 2022 09:01:22.371309996 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:02:51.796515942 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:02:51.934453964 CEST	587	49737	192.185.57.117	192.168.2.3
May 5, 2022 09:02:51.934662104 CEST	49737	587	192.168.2.3	192.185.57.117
May 5, 2022 09:02:51.948575974 CEST	49737	587	192.168.2.3	192.185.57.117

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2022 09:01:11.833470106 CEST	58204	53	192.168.2.3	8.8.8.8
May 5, 2022 09:01:11.975197077 CEST	53	58204	8.8.8.8	192.168.2.3
May 5, 2022 09:01:17.411793947 CEST	57851	53	192.168.2.3	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 5, 2022 09:01:11.833470106 CEST	192.168.2.3	8.8.8.8	0xd70a	Standard query (0)	mail.hardroot.biz	A (IP address)	IN (0x0001)
May 5, 2022 09:01:17.411793947 CEST	192.168.2.3	8.8.8.8	0xb7d2	Standard query (0)	x1.i.lencr.org	A (IP address)	IN (0x0001)

DNS Answers

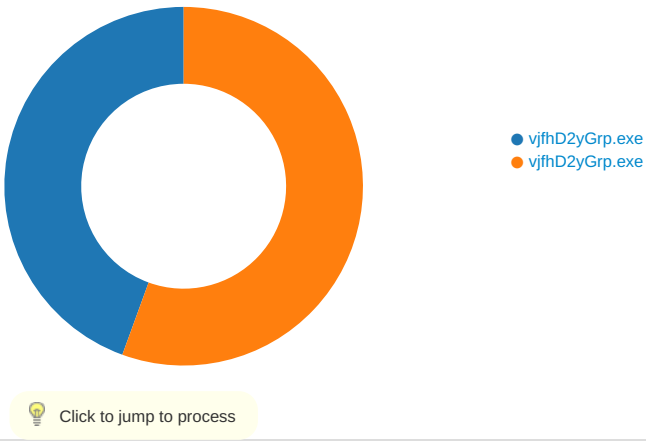
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 5, 2022 09:01:11.975197077 CEST	8.8.8.8	192.168.2.3	0xd70a	No error (0)	mail.hardroot.biz		192.185.57.117	A (IP address)	IN (0x0001)
May 5, 2022 09:01:17.436686993 CEST	8.8.8.8	192.168.2.3	0xb7d2	No error (0)	x1.i.lencr.org	crl.root-x1.letsencrypt.org.edgekey.net		CNAME (Canonical name)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 5, 2022 09:01:14.156817913 CEST	587	49737	192.185.57.117	192.168.2.3	220-paseo.websitewelcome.com ESMTP Exim 4.94.2 #2 Thu, 05 May 2022 02:01:14 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 5, 2022 09:01:14.245843887 CEST	49737	587	192.168.2.3	192.185.57.117	EHLO 506013
May 5, 2022 09:01:14.383192062 CEST	587	49737	192.185.57.117	192.168.2.3	250-paseo.websitewelcome.com Hello 506013 [102.129.143.40] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 5, 2022 09:01:14.383460999 CEST	49737	587	192.168.2.3	192.185.57.117	STARTTLS
May 5, 2022 09:01:14.527405024 CEST	587	49737	192.185.57.117	192.168.2.3	220 TLS go ahead

Statistics

Behavior



System Behavior

Analysis Process: vjfhD2yGrp.exe PID: 6452, Parent PID: 2300

General

Target ID:	0
Start time:	09:00:42
Start date:	05/05/2022
Path:	C:\Users\user\Desktop\vjfhD2yGrp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\vjfhD2yGrp.exe"
Imagebase:	0x550000
File size:	626176 bytes
MD5 hash:	186652D7FFC900EB5BF55E72C7FF07D8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.303740735.0000000002881000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.309529169.000000000441E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.309529169.000000000441E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.304185934.0000000002AAA000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
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	6D67CF06	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	6D67CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vjfhD2yGrp.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D98C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vjfhD2yGrp.exe.log	0	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",02,"System.Windows.Forms, Vers	success or wait	1	6D98C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D655705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D655705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D65CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D655705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D655705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	68F71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	68F71B4F	ReadFile

Analysis Process: vjfhD2yGrp.exe PID: **6788**, Parent PID: **6452**

General

Target ID:	6
Start time:	09:00:58
Start date:	05/05/2022
Path:	C:\Users\user\Desktop\vjfhD2yGrp.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\vjfhD2yGrp.exe
Imagebase:	0x7b0000
File size:	626176 bytes
MD5 hash:	186652D7FFC900EB5BF55E72C7FF07D8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000000.298815911.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.298815911.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000000.300624674.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.300624674.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000000.298205555.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.298205555.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000000.299591532.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.299591532.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.531340327.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.531340327.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.539452466.0000000002C41000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.539452466.0000000002C41000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D67CF06	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	6D67CF06	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D655705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D655705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D65CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D655705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D655705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	68F71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	68F71B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	68F71B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	68F71B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	68F71B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	68F71B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\05b98e77-fe4c-4961-9081-bc8c3f45dec3	unknown	4096	success or wait	1	68F71B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	68F71B4F	ReadFile

Disassembly

No disassembly