

ID: 626545
Sample Name:
2C01EPgbbjrSPr7.exe
Cookbook: default.jbs
Time: 12:06:20
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 2C01EPgbbjrSPr7.exe 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
Networking 5
Spam, unwanted Advertisements and Ransom Demands 5
System Summary 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Lowering of HIPS / PFW / Operating System Security Settings 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 10
Contacted Domains 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 14
Public IPs 15
General Information 15
Warnings 16
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 16
ASNs 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\2D85F72862B55C4EADD9E66E06947F3D 16
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\2D85F72862B55C4EADD9E66E06947F3D 17
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\2C01EPgbbjrSPr7.exe.log 17
C:\Windows\System32\drivers\etc\hosts 17
Static File Info 18
General 18
File Icon 18
Static PE Info 18
General 18
Entrypoint Preview 19
Data Directories 20
Sections 21
Resources 21
Imports 21
Version Infos 21
Network Behavior 21
TCP Packets 21
UDP Packets 22
DNS Queries 22
DNS Answers 22
SMTP Packets 22
Statistics 23
Behavior 23

System Behavior 23
Analysis Process: 2C01EPgbbjrSPr7.exePID: 6992, Parent PID: 2232 23
General 23
File Activities 24
File Created 24
File Written 24
File Read 24
Analysis Process: RegSvcs.exePID: 6108, Parent PID: 6992 25
General 25
File Activities 25
File Created 25
File Written 25
File Read 25
Disassembly 26

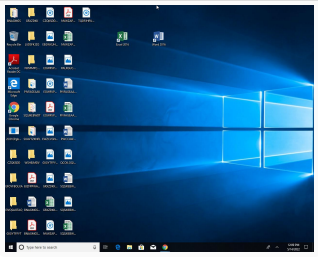
Windows Analysis Report

2C01EPgbbjrSPr7.exe

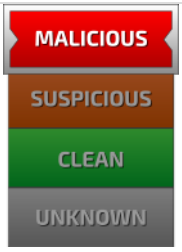
Overview

General Information

Sample Name:	2C01EPgbbjrSPr7.exe
Analysis ID:	626545
MD5:	dc6c55fee2366d…
SHA1:	609b99bc51ea6e..
SHA256:	99c52b9d5bcaa8..
Tags:	agenttesla exe
Infos:	



Detection



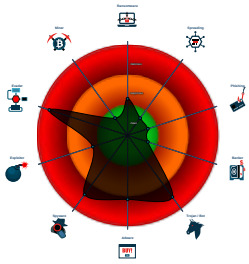
AgentTesla

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…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Modifies the hosts file
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- 2C01EPgbbjrSPr7.exe (PID: 6992 cmdline: "C:\Users\user\Desktop\2C01EPgbbjrSPr7.exe" MD5: DC6C55FEE2366DEE1D9C502BF061A8DC)
  - RegSvcs.exe (PID: 6108 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "leakkim@dtvcambodia.com",
  "Password": "@DTVcambodia2017",
  "Host": "mail.dtvcambodia.com"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.507717756.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.507717756.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000004.00000000.279997636.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000000.279997636.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000004.00000000.279367854.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
4.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
4.2.RegSvcs.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30dc2:$s1: get_kbok • 0x316f6:$s2: get_CHoo • 0x32369:$s3: set_passwordIsSet • 0x30bc6:$s4: get_enableLog • 0x3529a:$s8: torbrowser • 0x33c76:$s10: logins • 0x335f5:$s11: credential • 0x2ffbb:$g1: get_Clipboard • 0x2ffc9:$g2: get_Keyboard • 0x2ffd6:$g3: get_Password • 0x315a4:$g4: get_CtrlKeyDown • 0x315b4:$g5: get_ShiftKeyDown • 0x315c5:$g6: get_AltKeyDown
4.0.RegSvcs.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 26 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

Networking



Yara detected Generic Downloader

Spam, unwanted Advertisements and Ransom Demands



Modifies the hosts file

Copyright Joe Security LLC 2022

System Summary



Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

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)

HIPS / PFW / Operating System Protection Evasion



Writes to foreign memory regions

Modifies the hosts file

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings



Modifies the hosts file

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

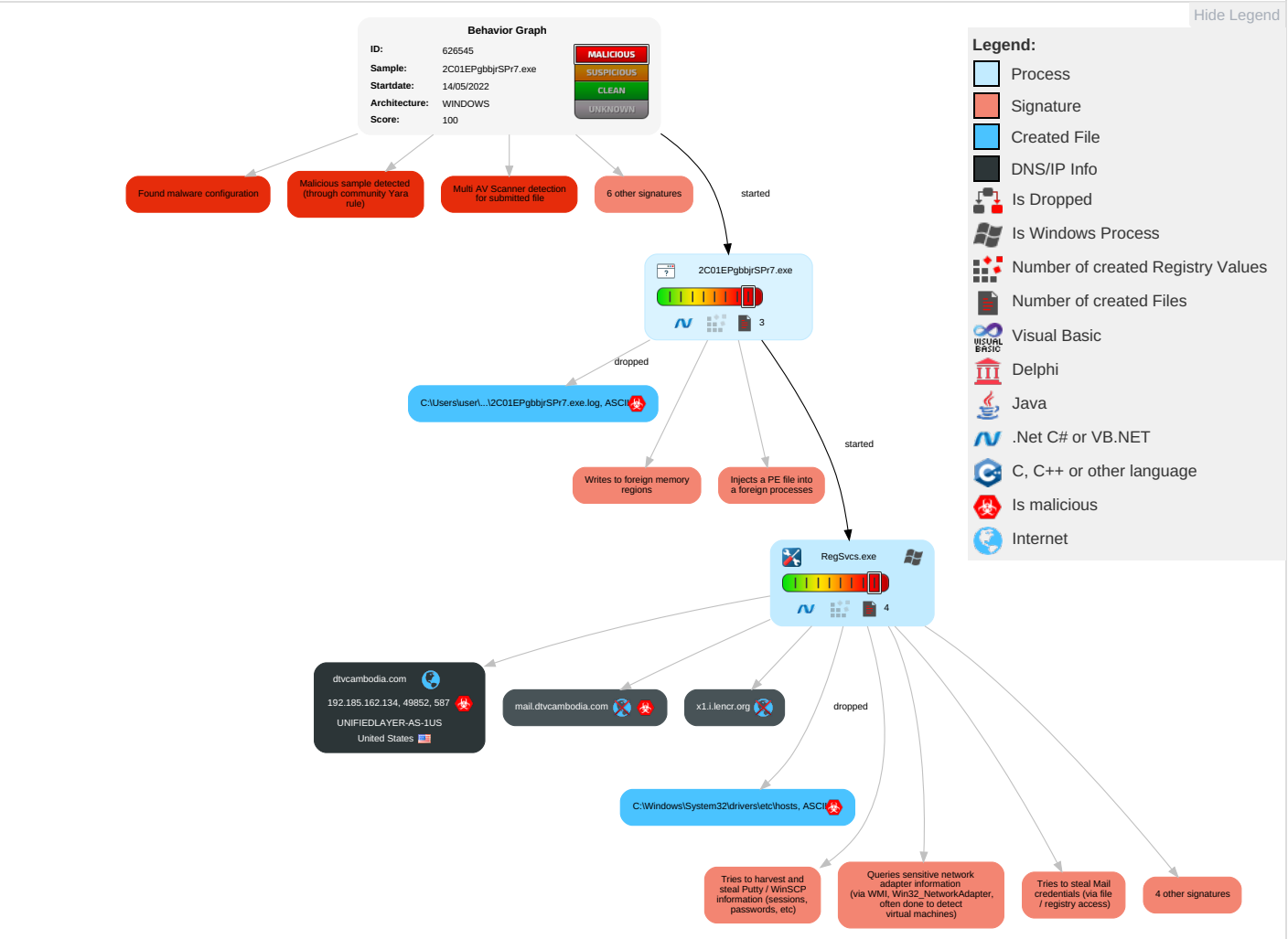
Mitre Att&ck Matrix

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	Path Interception	2 1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	2 1 1 Security Software Discovery	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	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 File and Directory Permissions Modification	1 Credentials in Registry	1 4 1 Virtualization/Sandbox Evasion	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 Disable or Modify Tools	Security Account Manager	1 Application Window 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 4 1 Virtualization/Sandbox Evasion	NTDS	1 Account Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

Copyright Joe Security LLC 2022

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 1 1 Process Injection	LSA Secrets	1 System Owner/User 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	1 1 Deobfuscate/Decode 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 Obfuscated Files or Information	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	3 Software Packing	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

Behavior Graph



Screenshots

Thumbnails

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

Copyright Joe Security LLC 2022





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
2C01EPgbbjrSPr7.exe	32%	Virustotal		Browse
2C01EPgbbjrSPr7.exe	62%	ReversingLabs	ByteCode-MSIL.Trojan.Injuke	
2C01EPgbbjrSPr7.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
4.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
dtvcambodia.com	0%	Virustotal		Browse
x1.i.lencr.org	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comsiv	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.founder.c	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comcomI)	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fonts.comcI	0%	Avira URL Cloud	safe	
http://www.fontbureau.comceTF	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcom7	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/0F	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnicre2	0%	Avira URL Cloud	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://https://drm1JEWaqqI1.net	0%	Avira URL Cloud	safe	
http://www.fontbureau.comtud	0%	Avira URL Cloud	safe	
http://www.fontbureau.comgreta	0%	URL Reputation	safe	
http://www.fontbureau.comkP)	0%	Avira URL Cloud	safe	
http://www.urwpp.dephy	0%	Avira URL Cloud	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.fontbureau.com7	0%	Avira URL Cloud	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sandoll.co.krC	0%	Avira URL Cloud	safe	
http://www.fonts.comx	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://x1.i.lencr.org/	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/:	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	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.zip%tordir%%ha	0%	URL Reputation	safe	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://www.tiro.comr	0%	Avira URL Cloud	safe	
http://www.fontbureau.comal)	0%	Avira URL Cloud	safe	
http://eolgGu.com	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kre	0%	URL Reputation	safe	
http://dtvcambodia.com	0%	Avira URL Cloud	safe	
http://www.fonts.comW	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn7	0%	URL Reputation	safe	
http://mail.dtvcambodia.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.founder.com.cn/cn4	0%	URL Reputation	safe	
http://x1.i.lencr.org/d	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dtvcambodia.com	192.185.162.134	true	true	• 0%, Virustotal, Browse	unknown
x1.i.lencr.org	unknown	unknown	false	• 1%, Virustotal, Browse	unknown
mail.dtvcambodia.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegSvcs.exe, 00000004.00000002.509894637.0000000002BA1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comsiv	2C01EPgbbjrSPr7.exe, 00000000.00000003.254284053.0000000005E79000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.244443790.0000000005E8B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.c	2C01EPgbbjrSPr7.exe, 00000000.00000003.246407275.0000000005E74000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.246653744.0000000005E74000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

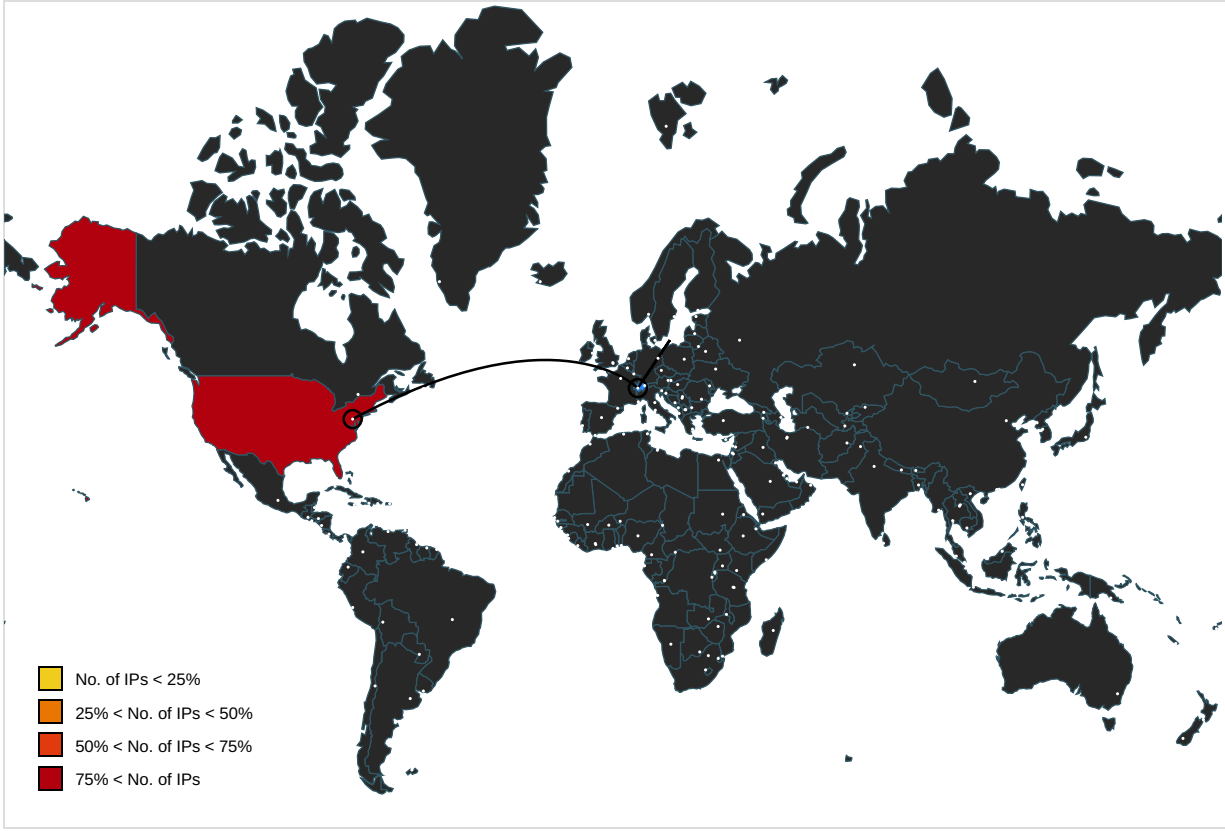
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comessed	2C01EPgbbjrSPr7.exe, 00000000.00000003.253560396.0000000005E7A000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.253090300.0000000005E79000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comcomI)	2C01EPgbbjrSPr7.exe, 00000000.00000003.254284053.0000000005E79000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.goodfont.co.kr	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comcI	2C01EPgbbjrSPr7.exe, 00000000.00000003.243999766.0000000005E8B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comceTF	2C01EPgbbjrSPr7.exe, 00000000.00000002.288273378.0000000005E70000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.281259255.0000000005E70000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comcom7	2C01EPgbbjrSPr7.exe, 00000000.00000003.253560396.0000000005E7A000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.253090300.0000000005E79000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.i.lencr.org/0F	RegSvcs.exe, 00000004.00000002.512946550.0000000005BE8000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000004.00000002.511389823.0000000002F03000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnicre2	2C01EPgbbjrSPr7.exe, 00000000.00000003.246653744.0000000005E74000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	2C01EPgbbjrSPr7.exe, 00000000.00000003.243716394.0000000005E8B000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.243840965.0000000005E8B000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.243824653.0000000005E8B000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.243882011.0000000005E8B000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.243743765.0000000005E8B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://drm1JEWaqqI1.net	RegSvcs.exe, 00000004.00000002.511188968.0000000002ECB000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000004.00000002.509894637.0000000002BA1000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000004.00000002.511337884.0000000002EFD000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000004.00000002.511295523.0000000002EF9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comtud	2C01EPgbbjrSPr7.exe, 00000000.00000003.254284053.0000000005E79000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comgreta	2C01EPgbbjrSPr7.exe, 00000000.00000002.288273378.0000000005E70000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.281259255.0000000005E70000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comkP)	2C01EPgbbjrSPr7.exe, 00000000.00000003.253560396.0000000005E7A000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.252302756.0000000005E78000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.253090300.0000000005E7900.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.urwpp.dephy	2C01EPgbbjrSPr7.exe, 00000000.00000003.254284053.0000000005E79000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://x1.c.lencr.org/0	RegSvcs.exe, 00000004.00000002.512946550.0000000005BE8000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000004.00000002.513029654.0000000005C2C000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000004.00000002.511389823.0000000002F03000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://x1.i.lencr.org/0	RegSvcs.exe, 00000004.00000002.512946550.0000000005BE8000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000004.00000002.513029654.0000000005C2C000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000004.00000002.511389823.0000000002F03000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://r3.o.lencr.org0	RegSvcs.exe, 00000004.00000002.512946550.0000000005BE8000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000004.00000002.511389823.0000000002F03000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	RegSvcs.exe, 00000004.00000002.509894637.0000000002BA1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.fonts.com	2C01EPgbbjrSPr7.exe, 00000000.00000003.243999766.0000000005E8B000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.244124001.0000000005E8B000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.243951668.0000000005E8B000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.244065913.0000000005E8B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com7	2C01EPgbbjrSPr7.exe, 00000000.00000003.254284053.0000000005E79000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de	2C01EPgbbjrSPr7.exe, 00000000.00000003.254284053.0000000005E79000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krC	2C01EPgbbjrSPr7.exe, 00000000.00000003.245662763.0000000005E76000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.comx	2C01EPgbbjrSPr7.exe, 00000000.00000003.243999766.0000000005E8B000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.243951668.0000000005E8B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	2C01EPgbbjrSPr7.exe, 00000000.00000002.286333778.000000000403F000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000004.00000002.507717756.0000000000402000.00000040.00000400.00020000.00000000.sdmp, RegSvcs.exe, 00000004.00000000.279367854.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.254284053.0000000005E79000.00000004.00000800.00020000.00000000.sdmp	false		high
http://x1.i.lencr.org/	RegSvcs.exe, 00000004.00000002.512946550.0000000005BE8000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000004.00000002.513029654.0000000005C2C000.00000004.00000800.00020000.00000000.sdmp, 2D85F72862B55C4EADD9E66E06947F3D0.4.dr	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNS	RegSvcs.exe, 00000004.00000002.509894637.0000000002BA1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/:	2C01EPgbbjrSPr7.exe, 00000000.00000003.246653744.0000000005E74000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comF	2C01EPgbbjrSPr7.exe, 00000000.00000003.254284053.0000000005E79000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://cps.letsencrypt.org0	RegSvcs.exe, 00000004.00000002.512946550.0000000005BE8000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000004.00000002.511389823.0000000002F03000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegSvcs.exe, 00000004.00000002.509894637.0000000002BA1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comr	2C01EPgbbjrSPr7.exe, 00000000.00000003.244414864.0000000005E8B000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.244443790.0000000005E8B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comal)	2C01EPgbbjrSPr7.exe, 00000000.00000002.288273378.0000000005E70000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.281259255.0000000005E70000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://eolgGu.com	RegSvcs.exe, 00000004.00000002.509894637.0000000002BA1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kre	2C01EPgbbjrSPr7.exe, 00000000.00000003.245662763.0000000005E76000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://dtvcambodia.com	RegSvcs.exe, 00000004.00000002.511389823.0000000002F03000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comW	2C01EPgbbjrSPr7.exe, 00000000.00000003.243999766.0000000005E8B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	2C01EPgbbjrSPr7.exe, 00000000.00000003.253560396.0000000005E7A000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.253090300.0000000005E79000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.254284053.0000000005E79000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://en.w	2C01EPgbbjrSPr7.exe, 00000000.00000003.243510111.00000000015ED000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%$	RegSvcs.exe, 00000004.00000002.509894637.0000000002BA1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coml	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	2C01EPgbbjrSPr7.exe, 00000000.00000003.246653744.0000000005E74000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	2C01EPgbbjrSPr7.exe, 00000000.00000003.246378606.0000000005EAD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	2C01EPgbbjrSPr7.exe, 00000000.00000003.253625429.0000000005EA5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn7	2C01EPgbbjrSPr7.exe, 00000000.00000003.246407275.0000000005E74000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.246653744.0000000005E74000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://mail.dtvcambodia.com	RegSvcs.exe, 00000004.00000002.511389823.0000000002F03000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.como	2C01EPgbbjrSPr7.exe, 00000000.00000002.288273378.0000000005E70000.00000004.00000800.00020000.00000000.sdmp, 2C01EPgbbjrSPr7.exe, 00000000.00000003.281259255.0000000005E70000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn4	2C01EPgbbjrSPr7.exe, 00000000.00000003.246407275.0000000005E74000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	2C01EPgbbjrSPr7.exe, 00000000.00000002.288950173.0000000007082000.00000004.00000800.00020000.00000000.sdmp	false		high
http://x1.i.lencr.org/d	RegSvcs.exe, 00000004.00000002.512946550.0000000005BE8000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.162.134	dtvcambodia.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626545
Start date and time: 14/05/202212:06:20	2022-05-14 12:06:20 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2C01EPgbbjrSPr7.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.adwa.spyw.evad.winEXE@3/4@3/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%

Copyright Joe Security LLC 2022

HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.50.97.168
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, e8652.dscx.akamaiedge.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, 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
12:07:31	API Interceptor	1x Sleep call for process: 2C01EPgbbjrSPr7.exe modified
12:07:49	API Interceptor	632x Sleep call for process: RegSvcs.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:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.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...150604110438Z..350604110438Z0O1.0...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.....I.....*.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\MetaData\2D85F72862B55C4EADD9E66E06947F3D

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	modified
Size (bytes):	192
Entropy (8bit):	2.795995823915415
Encrypted:	false
SSDEEP:	3:kkFkle0gPQXfllXlE/zMcyzXNNX8RolJuRdyo1dlUKlGXJlDdt:kKHr1yzdNMa8Rdy+UKcXP
MD5:	D5EA50AB6E2D47C57A613BC60522B9A0
SHA1:	1E199675C0C52DE3FDCCCD2415826C7904191969
SHA-256:	11E594484545FF0179379C437CDA5608367775449551 44E2DBC50BDD676ED282
SHA-512:	4312819708CD78D76DF4F374ACFCC8BCFE6B8408A1D98CD47927FA3E7772BDFB24BB4B22D0450BBBDF83C689868EF399BFA37DA20A1E69725AF3C6BA5304A0C
Malicious:	false
Reputation:	low
Preview:	p..... .....mQ...g..(..... .....~.....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\Local\Microsoft\CLR_v4.0_32\UsageLogs\2C01EPgbbjrSPr7.exe.log

Process:	C:\Users\user\Desktop\2C01EPgbbjrSPr7.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Windows\System32\drivers\etc\hosts

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP

MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA F
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.8493365780126645
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	2C01EPgbbjrSPr7.exe
File size:	833536
MD5:	dc6c55fee2366dee1d9c502bf061a8dc
SHA1:	609b99bc51ea6e1512d4aa1636a4586d2f6b29d6
SHA256:	99c52b9d5bcaa8af4bae268f70a39b94c0b2879dfed2cbdabd25c6fef5ff2258
SHA512:	8ca56693aabeeec0e59c1638d9097052bff8363a8f4629c3d523e46f970b4fac8e7a97b6c6c5f504c7eb63c8eb10e1b5785a5cd26b66fba562b1d1cd428e9956
SSDEEP:	12288:KaufL3YRRhPziuVIf5EKgZU4iFrqSwkVwQjylXPZmQJPEI5xnCIzjLjvllg+WKG:Kzf0H7iuVIRE9ZHo8VQ8N57dlW
TLSH:	250501153B5D3E62D5ABCB345152C00881B5FC9FBD33E12B7EA73D8E6818B5193A0AB1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...$>~b.....P.....F.... .....@.. ....@.....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4ccc46
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x627E3E24 [Fri May 13 11:16:52 2022 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 [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
or al, byte ptr [eax+00h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [esi], cl
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
adc byte ptr [eax+00h], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax+eax*2], cl
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
adc dword ptr [eax+00h], eax
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xccbf4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xce000	0x5a4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Copyright Joe Security LLC 2022

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xcac74	0xcae00	False	0.900544660736	data	7.85472323726	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xce000	0x5a4	0x600	False	0.422526041667	data	4.0893027472	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd0000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xce090	0x314	data		
RT_MANIFEST	0xce3b4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	g863j.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Coffee Shop
ProductVersion	1.0.0.0
FileDescription	Coffee Shop
OriginalFilename	g863j.exe

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 12:09:18.696096897 CEST	49852	587	192.168.2.3	192.185.162.134
May 14, 2022 12:09:18.837666988 CEST	587	49852	192.185.162.134	192.168.2.3
May 14, 2022 12:09:18.837800026 CEST	49852	587	192.168.2.3	192.185.162.134
May 14, 2022 12:09:19.225521088 CEST	587	49852	192.185.162.134	192.168.2.3
May 14, 2022 12:09:19.226907015 CEST	49852	587	192.168.2.3	192.185.162.134
May 14, 2022 12:09:19.368829966 CEST	587	49852	192.185.162.134	192.168.2.3
May 14, 2022 12:09:19.369097948 CEST	49852	587	192.168.2.3	192.185.162.134
May 14, 2022 12:09:19.513761997 CEST	587	49852	192.185.162.134	192.168.2.3
May 14, 2022 12:09:19.566498995 CEST	49852	587	192.168.2.3	192.185.162.134
May 14, 2022 12:09:19.643241882 CEST	49852	587	192.168.2.3	192.185.162.134
May 14, 2022 12:09:19.797015905 CEST	587	49852	192.185.162.134	192.168.2.3
May 14, 2022 12:09:19.797054052 CEST	587	49852	192.185.162.134	192.168.2.3
May 14, 2022 12:09:19.797072887 CEST	587	49852	192.185.162.134	192.168.2.3
May 14, 2022 12:09:19.797126055 CEST	49852	587	192.168.2.3	192.185.162.134
May 14, 2022 12:09:19.816838980 CEST	49852	587	192.168.2.3	192.185.162.134
May 14, 2022 12:09:19.959172964 CEST	587	49852	192.185.162.134	192.168.2.3
May 14, 2022 12:09:20.003353119 CEST	49852	587	192.168.2.3	192.185.162.134

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 12:09:39.908737898 CEST	49852	587	192.168.2.3	192.185.162.134
May 14, 2022 12:09:40.050744057 CEST	587	49852	192.185.162.134	192.168.2.3
May 14, 2022 12:09:40.052113056 CEST	49852	587	192.168.2.3	192.185.162.134
May 14, 2022 12:09:40.194169044 CEST	587	49852	192.185.162.134	192.168.2.3
May 14, 2022 12:09:40.194650888 CEST	49852	587	192.168.2.3	192.185.162.134
May 14, 2022 12:09:40.347683907 CEST	587	49852	192.185.162.134	192.168.2.3
May 14, 2022 12:09:40.348759890 CEST	49852	587	192.168.2.3	192.185.162.134
May 14, 2022 12:09:40.490468025 CEST	587	49852	192.185.162.134	192.168.2.3
May 14, 2022 12:09:40.490757942 CEST	49852	587	192.168.2.3	192.185.162.134
May 14, 2022 12:09:40.647701979 CEST	587	49852	192.185.162.134	192.168.2.3
May 14, 2022 12:09:40.647914886 CEST	49852	587	192.168.2.3	192.185.162.134
May 14, 2022 12:09:40.789446115 CEST	587	49852	192.185.162.134	192.168.2.3
May 14, 2022 12:09:40.790183067 CEST	49852	587	192.168.2.3	192.185.162.134
May 14, 2022 12:09:40.790239096 CEST	49852	587	192.168.2.3	192.185.162.134
May 14, 2022 12:09:40.791019917 CEST	49852	587	192.168.2.3	192.185.162.134
May 14, 2022 12:09:40.791034937 CEST	49852	587	192.168.2.3	192.185.162.134
May 14, 2022 12:09:40.931632042 CEST	587	49852	192.185.162.134	192.168.2.3
May 14, 2022 12:09:40.931677103 CEST	587	49852	192.185.162.134	192.168.2.3
May 14, 2022 12:09:40.932300091 CEST	587	49852	192.185.162.134	192.168.2.3
May 14, 2022 12:09:40.932327032 CEST	587	49852	192.185.162.134	192.168.2.3
May 14, 2022 12:09:40.932929993 CEST	587	49852	192.185.162.134	192.168.2.3
May 14, 2022 12:09:40.973928928 CEST	49852	587	192.168.2.3	192.185.162.134

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 12:09:18.372874975 CEST	54205	53	192.168.2.3	8.8.8.8
May 14, 2022 12:09:18.523155928 CEST	53	54205	8.8.8.8	192.168.2.3
May 14, 2022 12:09:18.532202959 CEST	62756	53	192.168.2.3	8.8.8.8
May 14, 2022 12:09:18.673108101 CEST	53	62756	8.8.8.8	192.168.2.3
May 14, 2022 12:09:24.027848959 CEST	58497	53	192.168.2.3	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 12:09:18.372874975 CEST	192.168.2.3	8.8.8.8	0xc04d	Standard query (0)	mail.dtvcambodia.com	A (IP address)	IN (0x0001)
May 14, 2022 12:09:18.532202959 CEST	192.168.2.3	8.8.8.8	0xc312	Standard query (0)	mail.dtvcambodia.com	A (IP address)	IN (0x0001)
May 14, 2022 12:09:24.027848959 CEST	192.168.2.3	8.8.8.8	0xe66d	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 14, 2022 12:09:18.523155928 CEST	8.8.8.8	192.168.2.3	0xc04d	No error (0)	mail.dtvcambodia.com	dtvcambodia.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 12:09:18.523155928 CEST	8.8.8.8	192.168.2.3	0xc04d	No error (0)	dtvcambodia.com		192.185.162.134	A (IP address)	IN (0x0001)
May 14, 2022 12:09:18.673108101 CEST	8.8.8.8	192.168.2.3	0xc312	No error (0)	mail.dtvcambodia.com	dtvcambodia.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 12:09:18.673108101 CEST	8.8.8.8	192.168.2.3	0xc312	No error (0)	dtvcambodia.com		192.185.162.134	A (IP address)	IN (0x0001)
May 14, 2022 12:09:24.049050093 CEST	8.8.8.8	192.168.2.3	0xe66d	No error (0)	x1.i.lencr.org	crl.root-x1.letsencrypt.org.edgekey.net		CNAME (Canonical name)	IN (0x0001)

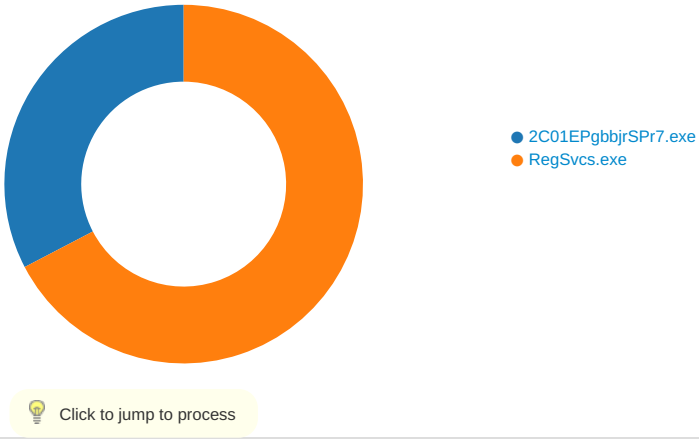
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 14, 2022 12:09:19.225521088 CEST	587	49852	192.185.162.134	192.168.2.3	220-jimmy.websitewelcome.com ESMTP Exim 4.94.2 #2 Sat, 14 May 2022 05:09:19 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 14, 2022 12:09:19.226907015 CEST	49852	587	192.168.2.3	192.185.162.134	EHLO 704672
May 14, 2022 12:09:19.368829966 CEST	587	49852	192.185.162.134	192.168.2.3	250-jimmy.websitewelcome.com Hello 704672 [102.129.143.55] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 14, 2022 12:09:19.369097948 CEST	49852	587	192.168.2.3	192.185.162.134	STARTTLS
May 14, 2022 12:09:19.513761997 CEST	587	49852	192.185.162.134	192.168.2.3	220 TLS go ahead

Statistics

Behavior



System Behavior

Analysis Process: 2C01EPgbbjrSPr7.exe PID: 6992, Parent PID: 2232

General

Target ID:	0
Start time:	12:07:20
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\2C01EPgbbjrSPr7.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\2C01EPgbbjrSPr7.exe"
Imagebase:	0xb50000
File size:	833536 bytes
MD5 hash:	DC6C55FEE2366DEE1D9C502BF061A8DC
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: 00000000.00000002.286333778.000000000403F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.286333778.000000000403F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Copyright Joe Security LLC 2022

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	6DC7CF06	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	6DC7CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\2C01EPgbbjrSPr7.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF8C78D	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\2C01EPgbbjrSPr7.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 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 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 30 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	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DF8C907	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	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C2C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C2C1B4F	ReadFile

Copyright Joe Security LLC 2022

Analysis Process: RegSvcs.exe PID: **6108**, Parent PID: **6992**

General

Target ID:	4
Start time:	12:07:36
Start date:	14/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x700000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000004.00000002.507717756.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.507717756.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.279997636.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.279997636.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.279367854.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.279367854.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.280271675.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.280271675.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.279715834.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.279715834.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.509894637.0000000002BA1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.509894637.0000000002BA1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000004.00000002.509894637.0000000002BA1000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	high

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	6DC7CF06	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	6DC7CF06	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\etc\hosts	824	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	127.0.0.1	success or wait	1	6C2C1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC55705	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DC5CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DC5CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuratio n.ni.dll.aux	unknown	864	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C2C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C2C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6C2C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6C2C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C2C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C2C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6C2C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6C2C1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C2C1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C2C1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5 CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C2C1B4F	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	6C2C1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5 CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C2C1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C2C1B4F	ReadFile

Disassembly

No disassembly