ID: 830558
Sample Name: PO.exe
Cookbook: default.jbs
Time: 13:54:26
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

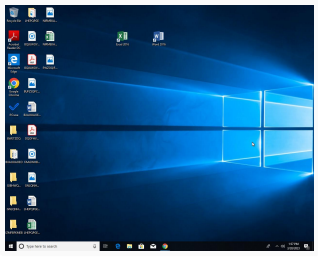
Windows Analysis Report

PO.exe

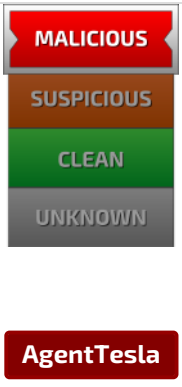
Overview

General Information

Sample Name:	PO.exe
Analysis ID:	830558
MD5:	03d90e26c8a6…
SHA1:	68b83832a442…
SHA256:	eb2ad014aa49…
Tags:	exe
Infos:	



Detection

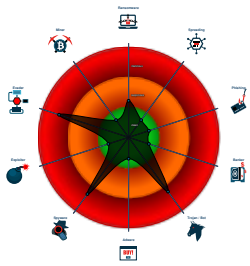


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Multi AV Scanner detection for drop…
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…
- Machine Learning detection for drop…
- Hides that the sample has been dow…
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…
- Queries sensitive BIOS Information…

Classification



Process Tree

- **System is w10x64**
- PO.exe (PID: 5176 cmdline: C:\Users\user\Desktop\PO.exe MD5: 03D90E26C8A6FBBEB284359B0F90EE91)
  - PO.exe (PID: 1116 cmdline: C:\Users\user\Desktop\PO.exe MD5: 03D90E26C8A6FBBEB284359B0F90EE91)
- keWKhH.exe (PID: 5144 cmdline: "C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe" MD5: 03D90E26C8A6FBBEB284359B0F90EE91)
  - keWKhH.exe (PID: 2888 cmdline: C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe MD5: 03D90E26C8A6FBBEB284359B0F90EE91)
  - keWKhH.exe (PID: 4980 cmdline: C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe MD5: 03D90E26C8A6FBBEB284359B0F90EE91)
- keWKhH.exe (PID: 6084 cmdline: "C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe" MD5: 03D90E26C8A6FBBEB284359B0F90EE91)
  - keWKhH.exe (PID: 3932 cmdline: C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe MD5: 03D90E26C8A6FBBEB284359B0F90EE91)
  - keWKhH.exe (PID: 3180 cmdline: C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe MD5: 03D90E26C8A6FBBEB284359B0F90EE91)
- **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

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Host": "us2.smtp.mailhostbox.com",
  "Username": "sudeni@dalwabo-jp.com",
  "Password": "     dLm)Xyz9     "
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.536082591.0000000002E81000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.536082591.0000000002E81000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000010.00000002.536562013.0000000002AA1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000010.00000002.536562013.0000000002AA1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000D.00000002.536833086.000000000311C000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 7 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

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

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

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

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

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

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

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

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

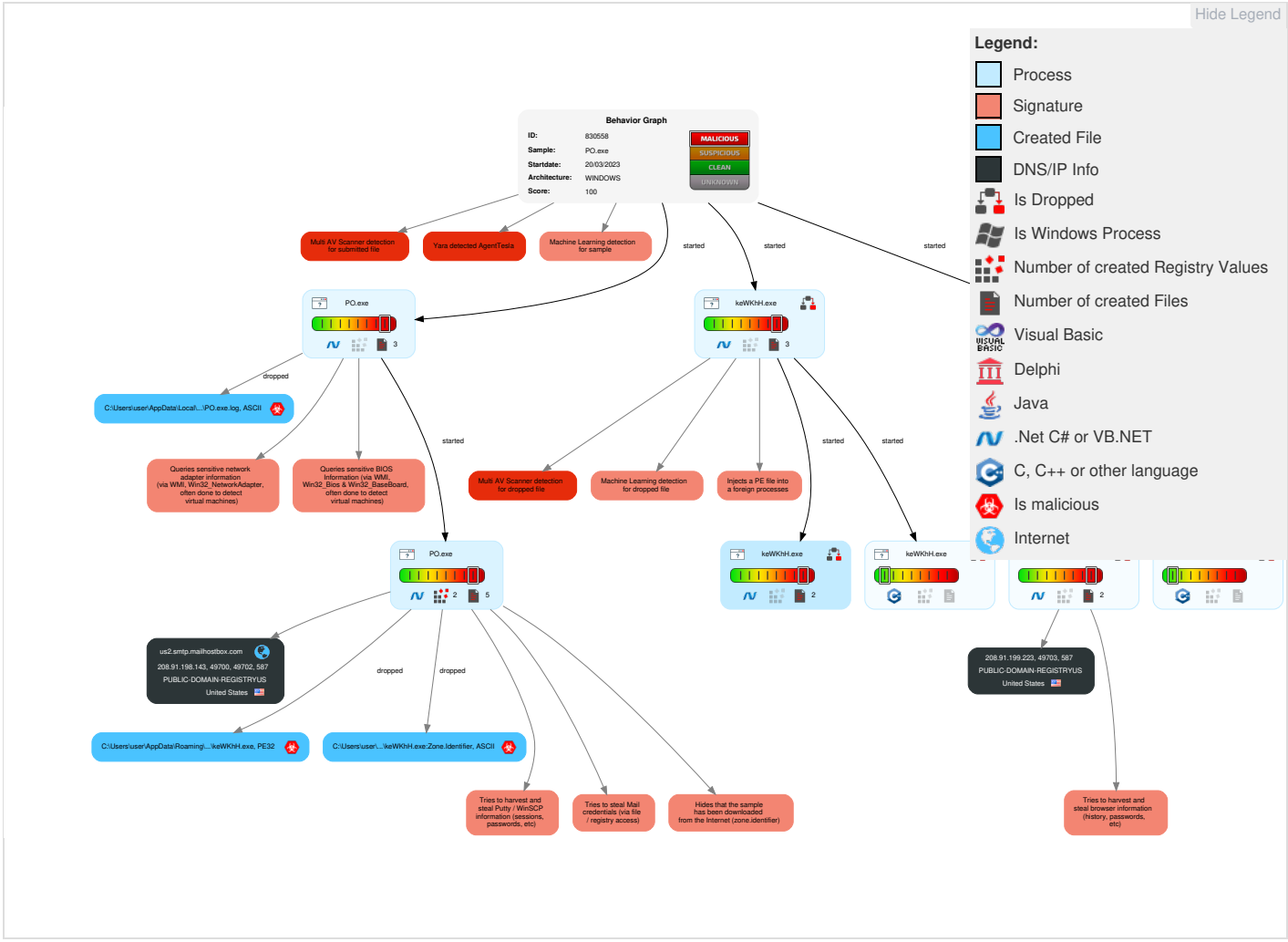
Remote Access Functionality

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	1 1 1 Process Injection	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	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	2 Obfuscated Files or Information	1 Input Capture	1 1 4 System Information 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)	2 Software Packing	1 Credentials in Registry	2 1 1 Security Software 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	1 Process 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 3 1 Virtualization/Sandbox Evasion	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 1 Process Injection	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Hidden Files and Directories	DCSync	1 System Owner/User 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 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

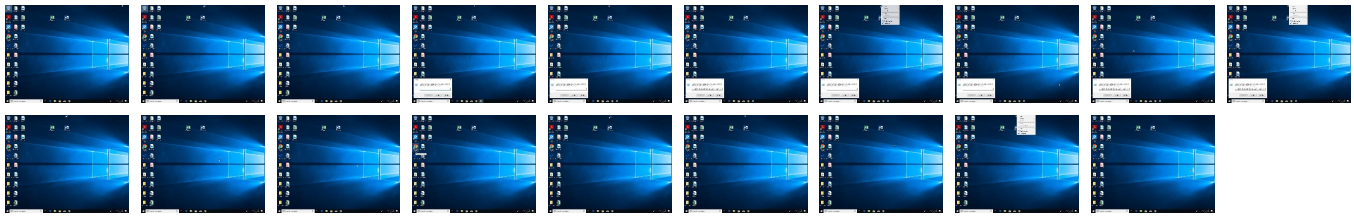
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PO.exe	38%	ReversingLabs	Win32.Trojan.Generic	
PO.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe	38%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
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.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	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.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.198.143	true	false		high

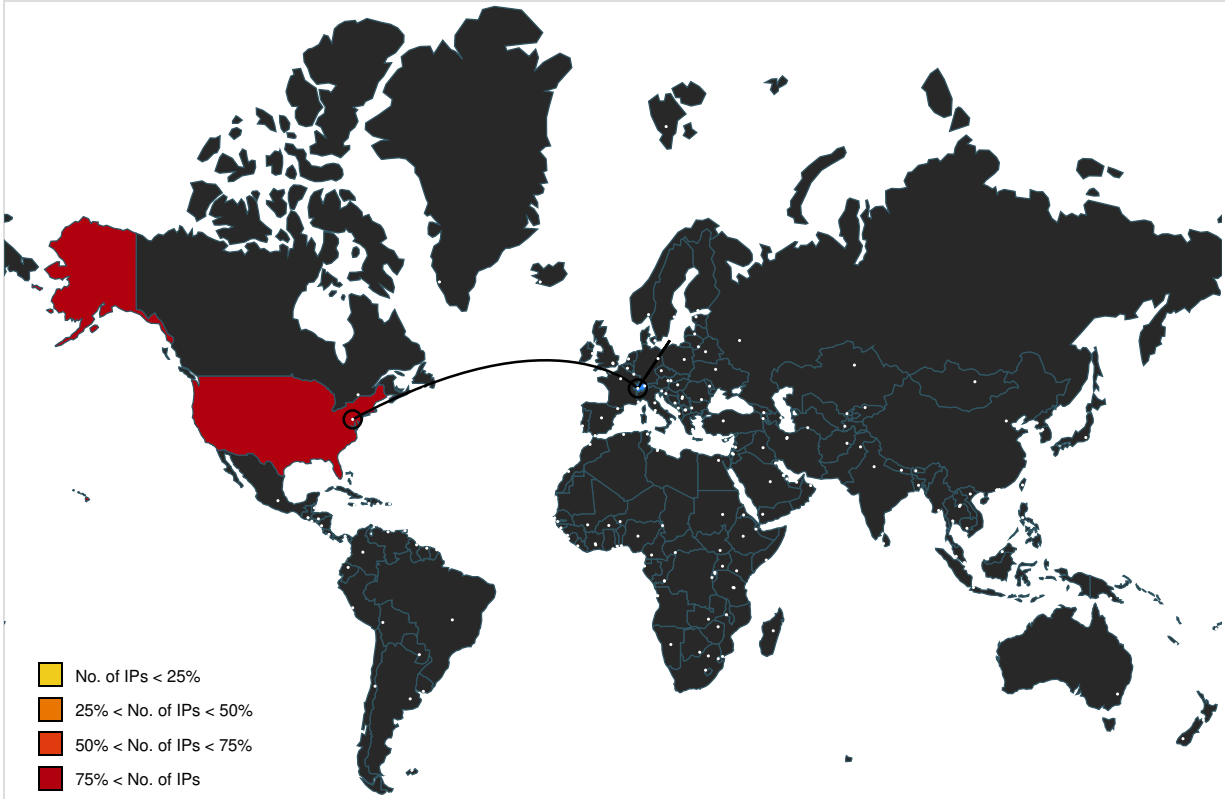
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	PO.exe, 00000006.00000002.533158671.000000001258000.00000004.00000020.00020000.00000000.sdmp, PO.exe, 00000006.00000002.536082591.0000000002ED9000.00000004.00000800.00020000.00000000.sdmp, PO.exe, 00000006.00000002.533158671.000000000129D000.00000004.00000020.00020000.00000000.sdmp, keWKhH.exe, 0000000D.00000002.536833086.00000003169000.00000004.00000800.00020000.00000000.sdmp, keWKhH.exe, 00000010.00000002.536562013.0000000002AF9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	PO.exe, 00000000.00000002.309764794.000000006B82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	PO.exe, 00000000.00000002.309764794.000000006B82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	PO.exe, 00000000.00000002.309764794.000000006B82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://sectigo.com/CPS0	PO.exe, 00000006.00000002.533158671.000000001258000.00000004.00000020.00020000.00000000.sdmp, PO.exe, 00000006.00000002.536082591.0000000002ED9000.00000004.00000800.00020000.00000000.sdmp, PO.exe, 00000006.00000002.533158671.000000000129D000.00000004.00000020.00020000.00000000.sdmp, keWKhH.exe, 0000000D.00000002.536833086.00000003169000.00000004.00000800.00020000.00000000.sdmp, keWKhH.exe, 00000010.00000002.536562013.0000000002AF9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	PO.exe, 00000000.00000002.309764794.000000006B82000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://us2.smtp.mailhostbox.com	PO.exe, 00000006.00000002.536082591.000000002ED9000.00000004.00000800.00020000.00000000.sdmp, keWKhH.exe, 0000000D.00000002.536833086.0000000003169000.00000004.00000800.00020000.00000000.sdmp, keWKhH.exe, 00000010.00000002.536562013.0000000002AF9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ocsp.sectigo.com0A	PO.exe, 00000006.00000002.533158671.000001258000.00000004.00000020.00020000.00000000.sdmp, PO.exe, 00000006.00000002.536082591.0000000002ED9000.00000004.00000800.00020000.00000000.sdmp, PO.exe, 00000006.00000002.533158671.000000000129D000.00000004.00000020.00020000.00000000.sdmp, keWKhH.exe, 0000000D.00000002.536833086.0000000003169000.00000004.00000800.00020000.00000000.sdmp, keWKhH.exe, 00000010.00000002.536562013.0000000002AF9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	PO.exe, 00000000.00000002.309764794.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.198.143	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
208.91.199.223	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830558
Start date and time:	2023-03-20 13:54:26 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 30s
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:	19
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:	PO.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@13/4@4/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com
- 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 NtQueryValueKey calls found.
- VT rate limit hit for: PO.exe

Simulations

Behavior and APIs

Time	Type	Description
13:55:36	API Interceptor	28x Sleep call for process: PO.exe modified
13:55:43	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run keWKhH C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe
13:55:52	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run keWKhH C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe
13:55:56	API Interceptor	63x Sleep call for process: keWKhH.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\PO.exe.log

Process:	C:\Users\user\Desktop\PO.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:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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\keWKhH.exe.log

Process:	C:\Users\user\AppData\Roaming\keWKhH\keWKhH.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
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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\Roaming\keWKhH\keWKhH.exe

Process:	C:\Users\user\Desktop\PO.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	744960
Entropy (8bit):	7.861489987265584
Encrypted:	false
SSDEEP:	12288:chmmYMUnFW/NQbwf4i9aXFc4fUDC/MbGh+796B5PthWxnr569lgx/0PHSHFfG2Sc:chmUWPWa75EbGhK92Vcnr8Q90PQY2ShW
MD5:	03D90E26C8A6FBBEB284359B0F90EE91
SHA1:	68B83832A4423003564A8DF9AF2CDA29622190A0
SHA-256:	EB2AD014AA499FD10C8EC16353295ACE996E28A7D822097CAF7BD11929C0B558
SHA-512:	2D36BF943AC0B78940780209273C400F6B99344CAECEF2351A7EAE639A62B1B93DF8FF796215D75380B61CA2906DB1DB0A2A620BC7CB596B31806A2333CFE18

Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....d.....0..H.....f... .....@.. ....@.....mf..O.....XR..T..... ....H.....text....F... ...H..... ..`.rsrc.....J.....@..@.rel oc.....\.....@..B.....f.....H.....@V...1....."....H.....0..R.....4...%..{....{L....%.r...p.%..|....(.....%.r...p.%..{.....X...(.....(.....+..*...0 ..&.....{.....,...{.....+....{....Z.+..*".(.....*..0..z.....}.....}.....}.....(.....(.....{.....s!...%.d}M...%r!..p}L...%.{....}P...%.{....}O.....{.....s!...%.d}M...%r)..p}L...%.{....}P...%.{.. ..}O.....{.....s!...%.d}M...%r1..p}L...%.{....}P...%.{....}O.....{.....+.....o....&.

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

Process:	C:\Users\user\Desktop\PO.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.861489987265584
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	PO.exe
File size:	744960
MD5:	03d90e26c8a6fbbeb284359b0f90ee91
SHA1:	68b83832a4423003564a8df9af2cda29622190a0
SHA256:	eb2ad014aa499fd10c8ec16353295ace996e28a7d822097caf7bd11929c0b558
SHA512:	2d36bf943ac0b78940780209273c400f6b99344caecef2351a7eae639a62b1b93df8ff796215d75380b61ca2906db1db0a2a620bc7cb596b31806a2333cfe180
SSDEEP:	12288:chmmYMUnFW/NQbwf4i9aXFc4fUDC/MbGh+796B5PthWxnr569lgx/0PHSHFfG2Sc:chmUWPWa75EbGhK92Vcnr8Q90PQY2ShW
TLSH:	B2F401392BAA5238F83657BD85E42290577D77A32B17C58D14F121CE5B73B038AD0A3B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....d.....0..H.....f... .....@.. .....@.....

File Icon

Icon Hash:	209480e66eb84902

Static PE Info

General

Entrypoint:	0x4b66c2
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:	0x6417B6B1 [Mon Mar 20 01:28:17 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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb666d	0x4f	.text

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb8000	0x1110	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xba000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xb5258	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	0xb46c8	0xb4800	False	0.926453482081025	data	7.870304849303137	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xb8000	0x1110	0x1200	False	0.7298177083333334	data	6.6330181066106375	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xba000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

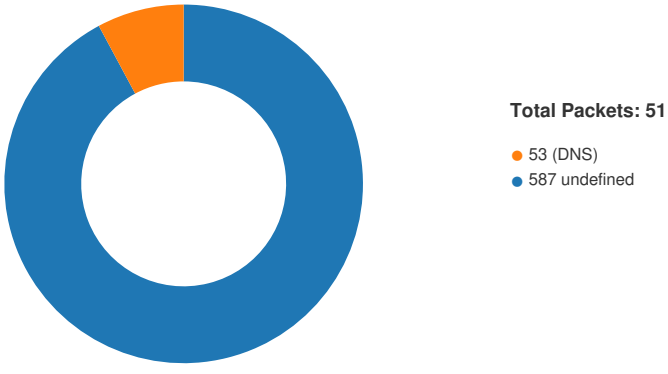
Name	RVA	Size	Type	Language	Country
RT_ICON	0xb8100	0xa79	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xb8b8c	0x14	data		
RT_VERSION	0xb8bb0	0x360	data		
RT_MANIFEST	0xb8f20	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 13:55:51.379208088 CET	49700	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:55:51.561971903 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:51.568327904 CET	49700	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:55:51.822913885 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:51.823677063 CET	49700	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:55:52.006165981 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:52.007561922 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:52.022155046 CET	49700	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:55:52.204807043 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:52.277923107 CET	49700	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:55:52.469763041 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:52.469798088 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:52.469816923 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:52.469832897 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:52.469852924 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:52.469980001 CET	49700	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:55:52.652877092 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:52.694524050 CET	49700	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:55:52.722714901 CET	49700	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:55:52.906130075 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:53.065079927 CET	49700	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:55:53.248606920 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:53.249872923 CET	49700	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:55:53.435743093 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:53.436301947 CET	49700	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:55:53.630464077 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:53.631983042 CET	49700	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:55:53.817394018 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:53.817768097 CET	49700	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:55:54.025801897 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:54.051700115 CET	49700	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:55:54.235774040 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:54.238713026 CET	49700	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:55:54.238836050 CET	49700	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:55:54.238903046 CET	49700	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:55:54.238959074 CET	49700	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:55:54.421613932 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:54.421794891 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:54.549983978 CET	587	49700	208.91.198.143	192.168.2.3
Mar 20, 2023 13:55:54.694654942 CET	49700	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:56:19.372095108 CET	49702	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:56:19.556463957 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:19.558954954 CET	49702	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:56:19.747483969 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:19.750802994 CET	49702	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:56:19.933517933 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:19.933639050 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:19.934598923 CET	49702	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:56:20.118187904 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:20.132863045 CET	49702	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:56:20.316102028 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:20.316154957 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:20.316188097 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:20.316232920 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:20.316243887 CET	49702	587	192.168.2.3	208.91.198.143

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 13:56:20.316360950 CET	49702	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:56:20.319158077 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:20.400011063 CET	49702	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:56:20.499293089 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:20.507908106 CET	49702	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:56:20.691613913 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:20.766664982 CET	49702	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:56:20.949820995 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:20.950285912 CET	49702	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:56:21.136104107 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:21.136550903 CET	49702	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:56:21.325586081 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:21.325930119 CET	49702	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:56:21.512427092 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:21.512749910 CET	49702	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:56:21.726322889 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:21.753025055 CET	49702	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:56:21.937357903 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:21.938667059 CET	49702	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:56:21.938776016 CET	49702	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:56:21.938776016 CET	49702	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:56:21.938776016 CET	49702	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:56:22.121570110 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:22.121669054 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:22.253518105 CET	587	49702	208.91.198.143	192.168.2.3
Mar 20, 2023 13:56:22.400196075 CET	49702	587	192.168.2.3	208.91.198.143
Mar 20, 2023 13:56:29.827996016 CET	49703	587	192.168.2.3	208.91.199.223
Mar 20, 2023 13:56:30.011459112 CET	587	49703	208.91.199.223	192.168.2.3
Mar 20, 2023 13:56:30.014067888 CET	49703	587	192.168.2.3	208.91.199.223
Mar 20, 2023 13:56:30.268151045 CET	587	49703	208.91.199.223	192.168.2.3
Mar 20, 2023 13:56:30.269398928 CET	49703	587	192.168.2.3	208.91.199.223
Mar 20, 2023 13:56:30.452392101 CET	587	49703	208.91.199.223	192.168.2.3
Mar 20, 2023 13:56:30.452708006 CET	587	49703	208.91.199.223	192.168.2.3
Mar 20, 2023 13:56:30.453392982 CET	49703	587	192.168.2.3	208.91.199.223
Mar 20, 2023 13:56:30.636518955 CET	587	49703	208.91.199.223	192.168.2.3
Mar 20, 2023 13:56:30.647614002 CET	49703	587	192.168.2.3	208.91.199.223
Mar 20, 2023 13:56:30.832444906 CET	587	49703	208.91.199.223	192.168.2.3
Mar 20, 2023 13:56:30.832494020 CET	587	49703	208.91.199.223	192.168.2.3
Mar 20, 2023 13:56:30.832515955 CET	587	49703	208.91.199.223	192.168.2.3
Mar 20, 2023 13:56:30.832532883 CET	587	49703	208.91.199.223	192.168.2.3
Mar 20, 2023 13:56:30.832700968 CET	49703	587	192.168.2.3	208.91.199.223
Mar 20, 2023 13:56:30.832743883 CET	49703	587	192.168.2.3	208.91.199.223
Mar 20, 2023 13:56:30.833830118 CET	587	49703	208.91.199.223	192.168.2.3
Mar 20, 2023 13:56:30.901175022 CET	49703	587	192.168.2.3	208.91.199.223
Mar 20, 2023 13:56:31.015933990 CET	587	49703	208.91.199.223	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 13:55:51.338753939 CET	49977	53	192.168.2.3	8.8.8.8
Mar 20, 2023 13:55:51.360728979 CET	53	49977	8.8.8.8	192.168.2.3
Mar 20, 2023 13:56:19.286415100 CET	57990	53	192.168.2.3	8.8.8.8
Mar 20, 2023 13:56:19.307167053 CET	53	57990	8.8.8.8	192.168.2.3
Mar 20, 2023 13:56:28.777345896 CET	52387	53	192.168.2.3	8.8.8.8
Mar 20, 2023 13:56:29.781128883 CET	52387	53	192.168.2.3	8.8.8.8
Mar 20, 2023 13:56:29.801374912 CET	53	52387	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
Mar 20, 2023 13:55:51.338753939 CET	192.168.2.3	8.8.8.8	0x12ed	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 13:56:19.286415100 CET	192.168.2.3	8.8.8.8	0x4bac	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 13:56:28.777345896 CET	192.168.2.3	8.8.8.8	0x2cd4	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 13:56:29.781128883 CET	192.168.2.3	8.8.8.8	0x2cd4	Standard query (0)	us2.smtp.mailhostbox.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
Mar 20, 2023 13:55:51.360728979 CET	8.8.8.8	192.168.2.3	0x12ed	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)	false
Mar 20, 2023 13:55:51.360728979 CET	8.8.8.8	192.168.2.3	0x12ed	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)	false
Mar 20, 2023 13:55:51.360728979 CET	8.8.8.8	192.168.2.3	0x12ed	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)	false
Mar 20, 2023 13:55:51.360728979 CET	8.8.8.8	192.168.2.3	0x12ed	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)	false
Mar 20, 2023 13:56:19.307167053 CET	8.8.8.8	192.168.2.3	0x4bac	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)	false
Mar 20, 2023 13:56:19.307167053 CET	8.8.8.8	192.168.2.3	0x4bac	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)	false
Mar 20, 2023 13:56:19.307167053 CET	8.8.8.8	192.168.2.3	0x4bac	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)	false
Mar 20, 2023 13:56:19.307167053 CET	8.8.8.8	192.168.2.3	0x4bac	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)	false
Mar 20, 2023 13:56:29.801374912 CET	8.8.8.8	192.168.2.3	0x2cd4	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)	false
Mar 20, 2023 13:56:29.801374912 CET	8.8.8.8	192.168.2.3	0x2cd4	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)	false
Mar 20, 2023 13:56:29.801374912 CET	8.8.8.8	192.168.2.3	0x2cd4	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)	false
Mar 20, 2023 13:56:29.801374912 CET	8.8.8.8	192.168.2.3	0x2cd4	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)	false

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Mar 20, 2023 13:55:51.822913885 CET	587	49700	208.91.198.143	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Mar 20, 2023 13:55:51.823677063 CET	49700	587	192.168.2.3	208.91.198.143	EHLO 494126
Mar 20, 2023 13:55:52.007561922 CET	587	49700	208.91.198.143	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Mar 20, 2023 13:55:52.022155046 CET	49700	587	192.168.2.3	208.91.198.143	STARTTLS
Mar 20, 2023 13:55:52.204807043 CET	587	49700	208.91.198.143	192.168.2.3	220 2.0.0 Ready to start TLS
Mar 20, 2023 13:56:19.747483969 CET	587	49702	208.91.198.143	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Mar 20, 2023 13:56:19.750802994 CET	49702	587	192.168.2.3	208.91.198.143	EHLO 494126

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Mar 20, 2023 13:56:19.933639050 CET	587	49702	208.91.198.143	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Mar 20, 2023 13:56:19.934598923 CET	49702	587	192.168.2.3	208.91.198.143	STARTTLS
Mar 20, 2023 13:56:20.118187904 CET	587	49702	208.91.198.143	192.168.2.3	220 2.0.0 Ready to start TLS
Mar 20, 2023 13:56:30.268151045 CET	587	49703	208.91.199.223	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Mar 20, 2023 13:56:30.269398928 CET	49703	587	192.168.2.3	208.91.199.223	EHLO 494126
Mar 20, 2023 13:56:30.452708006 CET	587	49703	208.91.199.223	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Mar 20, 2023 13:56:30.453392982 CET	49703	587	192.168.2.3	208.91.199.223	STARTTLS
Mar 20, 2023 13:56:30.636518955 CET	587	49703	208.91.199.223	192.168.2.3	220 2.0.0 Ready to start TLS

Statistics

Behavior

System Behavior

Analysis Process: PO.exe PID: **5176**, Parent PID: **3452**

General

Target ID:	0
Start time:	13:55:28
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\PO.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\Desktop\PO.exe
Imagebase:	0x690000
File size:	744960 bytes
MD5 hash:	03D90E26C8A6FBBEB284359B0F90EE91
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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\Microsoft\CLR_v4.0_32\UsageLogs\PO.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CAC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO.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
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	718E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	718E1B4F	ReadFile

Analysis Process: PO.exe PID: **1116**, Parent PID: **5176**

General

Target ID:	6
Start time:	13:55:38
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\PO.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PO.exe
Imagebase:	0xb40000
File size:	744960 bytes
MD5 hash:	03D90E26C8A6FBBEB284359B0F90EE91
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: 00000006.00000002.536082591.0000000002E81000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.536082591.0000000002E81000.00000004.00000800.00020000.00000000.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\keWKhH	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	718EBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\keWKhH\keWKhH.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	718EDD66	CopyFileW
C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	718EDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe:Zone.Identifier	success or wait	1	71845B28	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\keWKhH\keWKhH.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 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 fd 17 64 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 48 0b 00 00 14 00 00 00 00 00 00 fd 66 0b 00 00 20 00 00 00 fd 0b 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 fd 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.$PELd0Hf @ @	success or wait	3	718EDD66	CopyFileW
C:\Users\user\AppData\Roaming\keWKhH\keWKhH.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	718EDD66	CopyFileW

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	718E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	718E1B4F	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	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	718E1B4F	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	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	718E1B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	keWKhH	unicode	C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe	success or wait	1	718E646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	keWKhH	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	718EDE2E	RegSetValueExW

Analysis Process: keWKhH.exe PID: **5144**, Parent PID: **3452**

General

Target ID:	11
Start time:	13:55:52
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe"
Imagebase:	0xa0000
File size:	744960 bytes
MD5 hash:	03D90E26C8A6FBBEB284359B0F90EE91
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 38%, 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\Microsoft\CLR_v4.0_32\UsageLogs\keWKhH.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CAC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\keWKhH.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
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	718E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	718E1B4F	ReadFile

Analysis Process: keWKhH.exe PID: **2888**, Parent PID: **5144**

General

Target ID:	12
Start time:	13:55:58
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe
Imagebase:	0x10000
File size:	744960 bytes
MD5 hash:	03D90E26C8A6FBBEB284359B0F90EE91
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Reputation:	low

Analysis Process: keWKhH.exe PID: **4980**, Parent PID: **5144**

General

Target ID:	13
Start time:	13:55:58
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe
Imagebase:	0xd70000
File size:	744960 bytes
MD5 hash:	03D90E26C8A6FBBEB284359B0F90EE91
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: 0000000D.00000002.536833086.000000000311C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000002.536833086.000000000311C000.00000004.00000800.00020000.00000000.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
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	718E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	718E1B4F	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	718E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	718E1B4F	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	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	718E1B4F	ReadFile

Analysis Process: keWKhH.exe PID: **6084**, Parent PID: **3452**

General

Target ID:	14
Start time:	13:56:00
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe"
Imagebase:	0x850000
File size:	744960 bytes
MD5 hash:	03D90E26C8A6FBBEB284359B0F90EE91
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
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
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	718E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	718E1B4F	ReadFile

Analysis Process: keWKhH.exe PID: **3932**, Parent PID: **6084**

General

Target ID:	15
Start time:	13:56:15
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe
Imagebase:	0x3a0000
File size:	744960 bytes
MD5 hash:	03D90E26C8A6FBBEB284359B0F90EE91
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: keWKhH.exe PID: **3180**, Parent PID: **6084**

General

Target ID:	16
Start time:	13:56:15
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\keWKhH\keWKhH.exe
Imagebase:	0x660000
File size:	744960 bytes
MD5 hash:	03D90E26C8A6FBBEB284359B0F90EE91
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: 00000010.00000002.536562013.0000000002AA1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000010.00000002.536562013.0000000002AA1000.00000004.00000800.00020000.00000000.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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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	718E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	718E1B4F	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	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	718E1B4F	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	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	718E1B4F	ReadFile

Disassembly

No disassembly