ID: 626548
Sample Name: PI PDF.exe
Cookbook: default.jbs
Time: 12:25:09
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

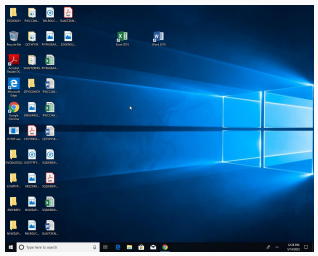
Windows Analysis Report

PI PDF.exe

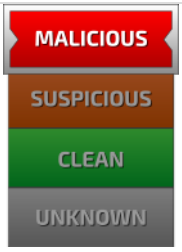
Overview

General Information

Sample Name:	PI PDF.exe
Analysis ID:	626548
MD5:	530c898ee06562..
SHA1:	316f4b32bdcaca…
SHA256:	56e4da2be0de52.
Tags:	agenttesla exe
Infos:	



Detection



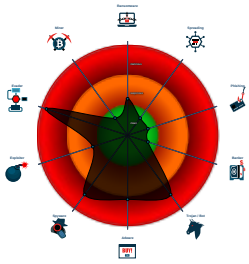
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for drop…
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Modifies the hosts file
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- PI PDF.exe (PID: 6928 cmdline: "C:\Users\user\Desktop\PI PDF.exe" MD5: 530C898EE065629D77B0B12781991D4F)
  - schtasks.exe (PID: 6320 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\jAZPdPbNZIxFH" /XML "C:\Users\user\AppData\Local\Temp\tmp3224.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6292 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - PI PDF.exe (PID: 6384 cmdline: {path} MD5: 530C898EE065629D77B0B12781991D4F)
  - PI PDF.exe (PID: 6344 cmdline: {path} MD5: 530C898EE065629D77B0B12781991D4F)
- bwjRNo.exe (PID: 5976 cmdline: "C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe" MD5: 530C898EE065629D77B0B12781991D4F)
  - schtasks.exe (PID: 6948 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\jAZPdPbNZIxFH" /XML "C:\Users\user\AppData\Local\Temp\tmpC00D.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - bwjRNo.exe (PID: 1112 cmdline: {path} MD5: 530C898EE065629D77B0B12781991D4F)
  - bwjRNo.exe (PID: 4588 cmdline: {path} MD5: 530C898EE065629D77B0B12781991D4F)
  - bwjRNo.exe (PID: 1252 cmdline: {path} MD5: 530C898EE065629D77B0B12781991D4F)
  - bwjRNo.exe (PID: 6808 cmdline: {path} MD5: 530C898EE065629D77B0B12781991D4F)
- bwjRNo.exe (PID: 6228 cmdline: "C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe" MD5: 530C898EE065629D77B0B12781991D4F)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "basker@ocenmasters.com",
  "Password": "donblack12345",
  "Host": "webmail.ocenmasters.com"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000000.291840024.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000000.291840024.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000008.00000000.290109897.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000000.290109897.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000008.00000000.291116090.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 38 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.PI PDF.exe.3f50928.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PI PDF.exe.3f50928.4.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.PI PDF.exe.3f50928.4.raw.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x10fb9d:$s10: logins • 0x10f604:$s11: credential • 0x10bac6:$g1: get_Clipboard • 0x10bad4:$g2: get_Keyboard • 0x10bae1:$g3: get_Password • 0x10ce98:$g4: get_CtrlKeyDown • 0x10cea8:$g5: get_ShiftKeyDown • 0x10ceb9:$g6: get_AltKeyDown
0.2.PI PDF.exe.3e18ae8.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PI PDF.exe.3e18ae8.3.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 64 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Spam, unwanted Advertisements and Ransom Demands

Modifies the hosts file

System Summary

Malicious sample detected (through community Yara rule)

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion

Modifies the hosts file

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings

Modifies the hosts file

Stealing of Sensitive Information

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality

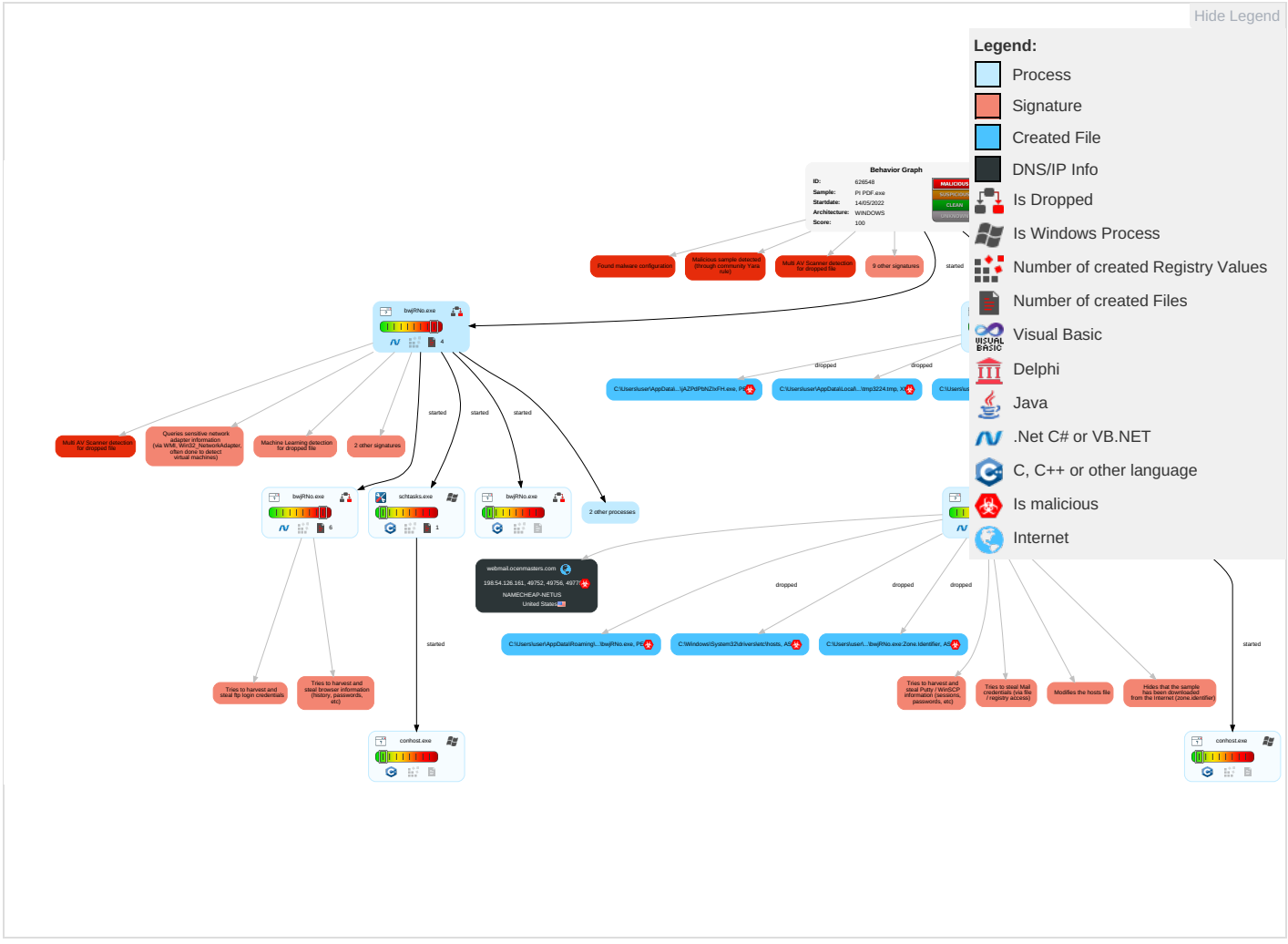
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 1 Process Injection	1 File and Directory Permissions Modification	2 OS Credential Dumping	1 File and Directory 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 Scheduled Task/Job	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 Disable or Modify Tools	1 Credentials in Registry	1 1 4 System Information Discovery	Remote Desktop Protocol	2 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)	1 Registry Run Keys / Startup Folder	3 Obfuscated Files or Information	Security Account Manager	1 Query Registry	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)	2 Software Packing	NTDS	3 1 1 Security Software Discovery	Distributed Component Object Model	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 Masquerading	LSA Secrets	1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 1 Process Injection	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Hidden Files and Directories	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
PI PDF.exe	35%	Virustotal		Browse
PI PDF.exe	58%	ReversingLabs	ByteCode-MSIL.Trojan.Injuke	
PI PDF.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\jAZPdPbNZIxFH.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe	49%	ReversingLabs	ByteCode-MSIL.Trojan.Injuke	
C:\Users\user\AppData\Roaming\jAZPdPbNZIxFH.exe	49%	ReversingLabs	ByteCode-MSIL.Trojan.Injuke	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.0.PI PDF.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1203024		Download File
8.0.PI PDF.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1203024		Download File

Source	Detection	Scanner	Label	Link	Download
8.0.PI PDF.exe.400000.12.unpack	100%	Avira	HEUR/AGEN.1203024		Download File
29.2.bwjRNo.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1203024		Download File
29.0.bwjRNo.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1203024		Download File
8.2.PI PDF.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1203024		Download File
29.0.bwjRNo.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1203024		Download File
8.0.PI PDF.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1203024		Download File
8.0.PI PDF.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1203024		Download File
29.0.bwjRNo.exe.400000.12.unpack	100%	Avira	HEUR/AGEN.1203024		Download File
29.0.bwjRNo.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1203024		Download File
29.0.bwjRNo.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1203024		Download File

Domains

Source	Detection	Scanner	Label	Link
webmail.ocenmasters.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comessedg	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/x	0%	Avira URL Cloud	safe	
http://www.fonts.comFB	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.tiro.comnf	0%	Avira URL Cloud	safe	
http://www.tiro.comB	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgreta	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.founder.com.cn/cnr	0%	URL Reputation	safe	
http://https://RHjTIBqqVW.com	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comalsvP	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://webmail.ocenmasters.com	0%	Avira URL Cloud	safe	
http://www.fonts.comtaT	0%	Avira URL Cloud	safe	
http://www.fonts.comWu	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comce9	0%	Avira URL Cloud	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comZ	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.tiro.comcomE	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdn	0%	Avira URL Cloud	safe	
http://www.tiro.comtn	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn0	0%	URL Reputation	safe	
http://www.sajatypeworks.comint	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comu	0%	URL Reputation	safe	
http://www.sajatypeworks.com#	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnk-s	0%	URL Reputation	safe	
http://KCCXXE.com	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com(	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsief	0%	URL Reputation	safe	
http://www.founder.com.cn/cn#	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
webmail.ocenmasters.com	198.54.126.161	true	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comessedg	PI PDF.exe, 00000000.00000003.248368737.0000000005BE9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	PI PDF.exe, 00000008.00000002.509270910.0000000002D01000.00000004.00000800.00020000.00000000.sdmp, bwjRNo.exe, 0000001D.00000002.509640311.0000000002D41000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/x	PI PDF.exe, 00000000.00000003.242100146.0000000005BE4000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comFB	PI PDF.exe, 00000000.00000003.239145630.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.239081087.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false		high

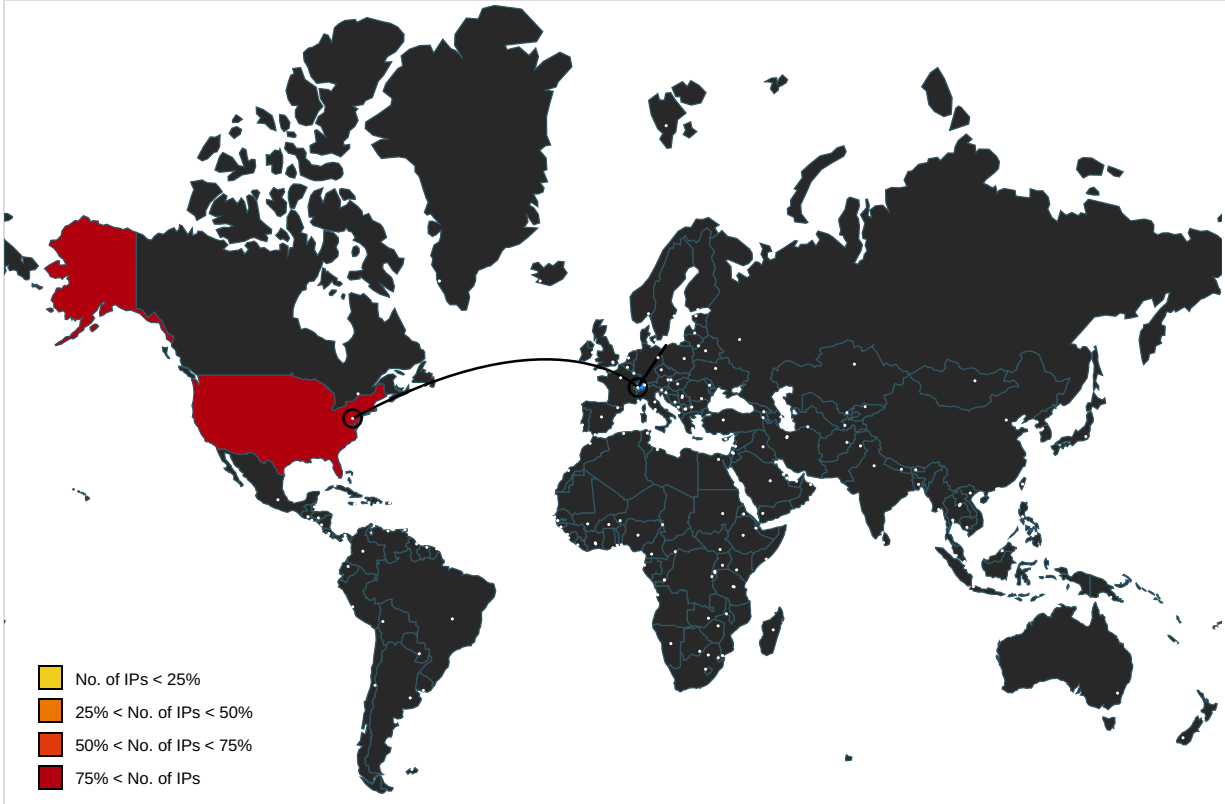
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comessed	PI PDF.exe, 00000000.00000003.248368737.0000000005BE9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comnf	PI PDF.exe, 00000000.00000003.239543641.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comB	PI PDF.exe, 00000000.00000003.239462569.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	PI PDF.exe, 00000000.00000003.253289800.0000000005BE9000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgrita	PI PDF.exe, 00000000.00000003.248368737.0000000005BE9000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.249055911.0000000005BEA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgreta	PI PDF.exe, 00000000.00000002.300963676.0000000005BE0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comcom	PI PDF.exe, 00000000.00000003.248368737.0000000005BE9000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.249987331.0000000005BE9000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.249055911.0000000005BEA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnr	PI PDF.exe, 00000000.00000003.242100146.0000000005BE4000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.241735377.0000000005BE4000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.242239716.0000000005BEB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://RHjTIBqqVW.com	bwjRNo.exe, 0000001D.00000002.510192777.000000000309D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	bwjRNo.exe, 0000001D.00000002.509640311.0000000002D41000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comalsvP	PI PDF.exe, 00000000.00000003.249987331.0000000005BE9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	PI PDF.exe, 00000000.00000003.239145630.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.239081087.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	PI PDF.exe, 00000000.00000003.240656249.0000000005BE6000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	PI PDF.exe, 00000000.00000003.249987331.0000000005BE9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PI PDF.exe, 00000000.00000002.294550223.0000000002C01000.00000004.00000800.00020000.00000000.sdmp, bwjRNo.exe, 00000013.00000002.392889468.00000000033A1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://webmail.ocenmasters.com	PI PDF.exe, 00000008.00000002.510095094.0000000003081000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000008.00000002.510025331.0000000003064000.00000004.00000800.00020000.00000000.sdmp, bwjRNo.exe, 0000001D.00000002.510209841.00000000030A5000.00000004.00000800.00020000.00000000.sdmp, bwjRNo.exe, 0000001D.00000002.510248333.00000000030BF000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comtaT	PI PDF.exe, 00000000.00000003.239206343.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.239173555.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comWu	PI PDF.exe, 00000000.00000003.239145630.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.239081087.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	PI PDF.exe, 00000000.00000002.300963676.0000000005BE0000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.249987331.0000000005BE9000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.247754281.0000000005BE8000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comF	PI PDF.exe, 00000000.00000003.249987331.0000000005BE9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comce9	PI PDF.exe, 00000000.00000002.300963676.0000000005BE0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.agfamonotype.	PI PDF.exe, 00000000.00000003.254344595.0000000005BF1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comZ	PI PDF.exe, 00000000.00000003.244849066.0000000005BED000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.244669874.0000000005BED000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.245136691.0000000005BED000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	PI PDF.exe, 00000008.00000002.509270910.0000000002D01000.00000004.00000800.00020000.00000000.sdmp, bwjRNo.exe, 0000001D.00000002.509640311.0000000002D41000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comcomE	PI PDF.exe, 00000000.00000003.240259326.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comdn	PI PDF.exe, 00000000.00000003.248368737.0000000005BE9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.comtn	PI PDF.exe, 00000000.00000003.239488128.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	PI PDF.exe, 00000000.00000003.249987331.0000000005BE9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comX	PI PDF.exe, 00000000.00000003.239145630.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	PI PDF.exe, 00000000.00000003.238574491.000000000123D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	PI PDF.exe, 00000000.00000003.244849066.0000000005BED000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.244669874.0000000005BED000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.245136691.0000000005BED000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	PI PDF.exe, 00000000.00000003.241607174.0000000005C1D000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.241735377.0000000005BE4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn0	PI PDF.exe, 00000000.00000003.241607174.0000000005C1D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.comint	PI PDF.exe, 00000000.00000003.238934806.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.239014164.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.238957767.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.238846807.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.239145630.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.239165623.0000000005C04000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.239081087.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.238911883.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.238991885.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	PI PDF.exe, 00000000.00000003.249138762.0000000005C1D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	PI PDF.exe, 00000000.00000002.301150695.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comu	PI PDF.exe, 00000000.00000003.248368737.0000000005BE9000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.249987331.0000000005BE9000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.249055911.0000000005BEA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com#	PI PDF.exe, 00000000.00000003.238934806.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.239014164.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.238957767.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.238846807.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.239145630.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.239165623.0000000005C04000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.239081087.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.238911883.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp, PI PDF.exe, 00000000.00000003.238991885.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnk-s	PI PDF.exe, 00000000.00000003.241607174.0000000005C1D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://KCCXXE.com	bwjRNo.exe, 0000001D.00000002.509640311.0000000002D41000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com(	PI PDF.exe, 00000000.00000003.238846807.0000000005BFB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comsief	PI PDF.exe, 00000000.00000003.249987331.0000000005BE9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn#	PI PDF.exe, 00000000.00000003.241607174.0000000005C1D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.126.161	webmail.ocenmasters.com	United States		22612	NAMECHEAP-NETUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626548
Start date and time: 14/05/202212:25:09	2022-05-14 12:25:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PI PDF.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:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.spyw.evad.winEXE@21/10@4/1
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 3.4% (good quality ratio 3.4%) • Quality average: 83% • Quality standard deviation: 1%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target PI PDF.exe, PID 6384 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:26:18	API Interceptor	634x Sleep call for process: PI PDF.exe modified
12:26:40	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run bwjRNo C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe
12:26:49	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run bwjRNo C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe
12:26:55	API Interceptor	334x Sleep call for process: bwjRNo.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\PI PDF.exe.log

Process:	C:\Users\user\Desktop\PI PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

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

Process:	C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87

SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	false
Reputation:	unknown
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, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Cultur e=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.Con figuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp3224.tmp

Process:	C:\Users\user\Desktop\PI PDF.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.203453803097939
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBH93Btn:cbh47TlNQ//rydbz9I3YODOLNdq3P3T
MD5:	977B4AD5C289482E309FBF6BD147FF93
SHA1:	1F2715FC226E643FC4F1B6255228E89F38ACD738
SHA-256:	B28491B184A5EEDF25BE98D21F1957F16EC3F280D5E59FBE6218009B9AA11C9E
SHA-512:	08990A0A8E47354799F7D5490D58FCB0BF4DE92AF47A40E7FB8018F57D4DD896E8FF61A672C2260F97A62984951C69D3D552E60281EB46FE555E0A01A8107850
Malicious:	**true**
Reputation:	unknown
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>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpC00D.tmp

Process:	C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.203453803097939
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBH93Btn:cbh47TlNQ//rydbz9I3YODOLNdq3P3T
MD5:	977B4AD5C289482E309FBF6BD147FF93
SHA1:	1F2715FC226E643FC4F1B6255228E89F38ACD738
SHA-256:	B28491B184A5EEDF25BE98D21F1957F16EC3F280D5E59FBE6218009B9AA11C9E
SHA-512:	08990A0A8E47354799F7D5490D58FCB0BF4DE92AF47A40E7FB8018F57D4DD896E8FF61A672C2260F97A62984951C69D3D552E60281EB46FE555E0A01A8107850
Malicious:	false
Reputation:	unknown
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>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

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

Process:	C:\Users\user\Desktop\PI PDF.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	904704
Entropy (8bit):	7.867040525817705
Encrypted:	false
SSDEEP:	12288:t/icL3Ygn2Y75AbVmtCVOdgF/y+mizs/yeCMrKxB+6qP8rgTc4Mpi/F:t6co4JdgrhzsamrKxPmigwWd
MD5:	530C898EE065629D77B0B12781991D4F
SHA1:	316F4B32BDCACA1902A7E9898A31F3FAE42EBE30

SHA-256:	56E4DA2BE0DE5210FA5F78B35AED78DC18145164B03C396D85098368AAE825A5
SHA-512:	3F35683D138D80FF728A2878D0DA0E5FF8EF5D342D085A7C051A0BD6F1A0A85E6B58050D07595B1C535A40D011968B1516A1B31F8B112DBE0A2EA2B8DDA776A6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 49%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....E~b.....P..... .....@.. .....@..... ..@.....O..... ....H.....text..... .... `.rsrc.....@..@.reloc..... .....@..B.....H.....Y...Z.....`.....-.....(....*&..(.....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0.....~.... o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....()....,!r...p.....(*...o+...s,.....~.....+..*.0.....~.....+..*"".....*.0..&.....(....r+..p~....o-...(.....t$....+..*Vs....(/...t.....*..(0...*.0.....

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

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

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

Process:	C:\Users\user\Desktop\PI PDF.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	904704
Entropy (8bit):	7.867040525817705
Encrypted:	false
SSDEEP:	12288:t/icL3Ygn2Y75AbVmtCVOdgF/y+mizs/yeCMrKxB+6qP8rgTc4Mpi/F:t6co4JdgrhzsamrKxPmigwWd
MD5:	530C898EE065629D77B0B12781991D4F
SHA1:	316F4B32BDCACA1902A7E9898A31F3FAE42EBE30
SHA-256:	56E4DA2BE0DE5210FA5F78B35AED78DC18145164B03C396D85098368AAE825A5
SHA-512:	3F35683D138D80FF728A2878D0DA0E5FF8EF5D342D085A7C051A0BD6F1A0A85E6B58050D07595B1C535A40D011968B1516A1B31F8B112DBE0A2EA2B8DDA776A6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 49%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....E~b.....P..... .....@.. .....@..... ..@.....O..... ....H.....text..... .... `.rsrc.....@..@.reloc..... .....@..B.....H.....Y...Z.....`.....-.....(....*&..(.....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0.....~.... o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....()....,!r...p.....(*...o+...s,.....~.....+..*.0.....~.....+..*"".....*.0..&.....(....r+..p~....o-...(.....t$....+..*Vs....(/...t.....*..(0...*.0.....

C:\Users\user\AppData\Roaming\xkhii1zz.ywa\Chrome\Default\Cookies

Process:	C:\Users\user\Desktop\PI PDF.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB

SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Roaming\zktusgco.ufg\Chrome\Default\Cookies

Process:	C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

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

Process:	C:\Users\user\Desktop\PI PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA2F
Malicious:	**true**
Reputation:	unknown
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.867040525817705
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	PI PDF.exe
File size:	904704

MD5:	530c898ee065629d77b0b12781991d4f
SHA1:	316f4b32bdcaca1902a7e9898a31f3fae42ebe30
SHA256:	56e4da2be0de5210fa5f78b35aed78dc18145164b03c396d85098368aae825a5
SHA512:	3f35683d138d80ff728a2878d0da0e5ff8ef5d342d085a7c051a0bd6f1a0a85e6b58050d07595b1c535a40d011968b1516a1b31f8b112dbe0a2ea2b8dda776a6
SSDEEP:	12288:t/icL3Ygn2Y75AbVmtCVOdgF/y+mizs/yeCMrKxB+6qP8rgTc4Mpi/F:t6co4JdgrhzsamrKxPmigwWd
TLSH:	181512013B6C7D66D4ABDB345211C0088AF1AC5FBD27E22A3DD77C8E985974097B1EB1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....E~b.....P..... .....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4de2de
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:	0x627E45A6 [Fri May 13 11:48:54 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
or al, byte ptr [eax+00h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [esi], cl
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
adc byte ptr [eax+00h], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax+eax*2], cl
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
adc dword ptr [eax+00h], eax
add byte ptr [eax], al
add byte ptr [eax], al

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xde28c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe0000	0x5a4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe2000	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	0xdc30c	0xdc400	False	0.90938475454	data	7.87186503084	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe0000	0x5a4	0x600	False	0.420572916667	data	4.07782470148	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe2000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe0090	0x314	data		
RT_MANIFEST	0xe03b4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

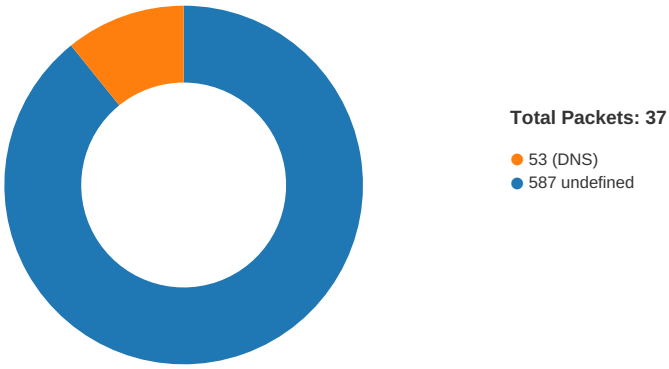
Version Infos

Description	Data
Translation	0x0000 0x04b0

Description	Data
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	ZPXmS.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Coffee Shop
ProductVersion	1.0.0.0
FileDescription	Coffee Shop
OriginalFilename	ZPXmS.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 12:26:45.863831997 CEST	49752	587	192.168.2.3	198.54.126.161
May 14, 2022 12:26:46.036645889 CEST	587	49752	198.54.126.161	192.168.2.3
May 14, 2022 12:26:46.036787033 CEST	49752	587	192.168.2.3	198.54.126.161
May 14, 2022 12:26:46.521317005 CEST	587	49752	198.54.126.161	192.168.2.3
May 14, 2022 12:26:46.521672964 CEST	49752	587	192.168.2.3	198.54.126.161
May 14, 2022 12:26:46.695774078 CEST	587	49752	198.54.126.161	192.168.2.3
May 14, 2022 12:26:46.698307037 CEST	49752	587	192.168.2.3	198.54.126.161
May 14, 2022 12:26:46.871859074 CEST	587	49752	198.54.126.161	192.168.2.3
May 14, 2022 12:26:46.872452974 CEST	49752	587	192.168.2.3	198.54.126.161
May 14, 2022 12:26:47.085675955 CEST	587	49752	198.54.126.161	192.168.2.3
May 14, 2022 12:26:48.456665993 CEST	587	49752	198.54.126.161	192.168.2.3
May 14, 2022 12:26:48.464423895 CEST	49752	587	192.168.2.3	198.54.126.161
May 14, 2022 12:26:48.637429953 CEST	587	49752	198.54.126.161	192.168.2.3
May 14, 2022 12:26:48.638108969 CEST	587	49752	198.54.126.161	192.168.2.3
May 14, 2022 12:26:48.638216019 CEST	49752	587	192.168.2.3	198.54.126.161
May 14, 2022 12:26:48.645277977 CEST	49752	587	192.168.2.3	198.54.126.161
May 14, 2022 12:26:48.817888021 CEST	587	49752	198.54.126.161	192.168.2.3
May 14, 2022 12:26:50.134658098 CEST	49756	587	192.168.2.3	198.54.126.161
May 14, 2022 12:26:50.308897018 CEST	587	49756	198.54.126.161	192.168.2.3
May 14, 2022 12:26:50.311944962 CEST	49756	587	192.168.2.3	198.54.126.161
May 14, 2022 12:26:50.580655098 CEST	587	49756	198.54.126.161	192.168.2.3
May 14, 2022 12:26:50.582381964 CEST	49756	587	192.168.2.3	198.54.126.161

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 12:26:50.756458044 CEST	587	49756	198.54.126.161	192.168.2.3
May 14, 2022 12:26:50.757569075 CEST	49756	587	192.168.2.3	198.54.126.161
May 14, 2022 12:26:50.972130060 CEST	587	49756	198.54.126.161	192.168.2.3
May 14, 2022 12:26:54.943469048 CEST	587	49756	198.54.126.161	192.168.2.3
May 14, 2022 12:26:54.944633961 CEST	49756	587	192.168.2.3	198.54.126.161
May 14, 2022 12:26:55.122080088 CEST	587	49756	198.54.126.161	192.168.2.3
May 14, 2022 12:26:57.174988031 CEST	587	49756	198.54.126.161	192.168.2.3
May 14, 2022 12:26:57.175209999 CEST	49756	587	192.168.2.3	198.54.126.161
May 14, 2022 12:26:57.349693060 CEST	587	49756	198.54.126.161	192.168.2.3
May 14, 2022 12:26:57.349997997 CEST	587	49756	198.54.126.161	192.168.2.3
May 14, 2022 12:26:57.350090027 CEST	49756	587	192.168.2.3	198.54.126.161
May 14, 2022 12:26:57.350496054 CEST	49756	587	192.168.2.3	198.54.126.161
May 14, 2022 12:26:57.524431944 CEST	587	49756	198.54.126.161	192.168.2.3
May 14, 2022 12:27:30.868840933 CEST	49778	587	192.168.2.3	198.54.126.161
May 14, 2022 12:27:31.045579910 CEST	587	49778	198.54.126.161	192.168.2.3
May 14, 2022 12:27:31.045717955 CEST	49778	587	192.168.2.3	198.54.126.161
May 14, 2022 12:27:31.266168118 CEST	587	49778	198.54.126.161	192.168.2.3
May 14, 2022 12:27:31.266634941 CEST	49778	587	192.168.2.3	198.54.126.161
May 14, 2022 12:27:31.444529057 CEST	587	49778	198.54.126.161	192.168.2.3
May 14, 2022 12:27:31.444958925 CEST	49778	587	192.168.2.3	198.54.126.161
May 14, 2022 12:27:31.622293949 CEST	587	49778	198.54.126.161	192.168.2.3
May 14, 2022 12:27:31.623956919 CEST	49778	587	192.168.2.3	198.54.126.161
May 14, 2022 12:27:31.841794014 CEST	587	49778	198.54.126.161	192.168.2.3
May 14, 2022 12:27:33.153253078 CEST	587	49778	198.54.126.161	192.168.2.3
May 14, 2022 12:27:33.153584957 CEST	49778	587	192.168.2.3	198.54.126.161
May 14, 2022 12:27:33.331151962 CEST	587	49778	198.54.126.161	192.168.2.3
May 14, 2022 12:27:33.331515074 CEST	587	49778	198.54.126.161	192.168.2.3
May 14, 2022 12:27:33.331624985 CEST	49778	587	192.168.2.3	198.54.126.161
May 14, 2022 12:27:33.348444939 CEST	49778	587	192.168.2.3	198.54.126.161
May 14, 2022 12:27:33.525588036 CEST	587	49778	198.54.126.161	192.168.2.3
May 14, 2022 12:27:35.495639086 CEST	49793	587	192.168.2.3	198.54.126.161
May 14, 2022 12:27:35.670006990 CEST	587	49793	198.54.126.161	192.168.2.3
May 14, 2022 12:27:35.670198917 CEST	49793	587	192.168.2.3	198.54.126.161
May 14, 2022 12:27:35.901343107 CEST	587	49793	198.54.126.161	192.168.2.3
May 14, 2022 12:27:35.971069098 CEST	49793	587	192.168.2.3	198.54.126.161
May 14, 2022 12:27:36.152457952 CEST	49793	587	192.168.2.3	198.54.126.161
May 14, 2022 12:27:36.327141047 CEST	587	49793	198.54.126.161	192.168.2.3
May 14, 2022 12:27:36.327440023 CEST	49793	587	192.168.2.3	198.54.126.161
May 14, 2022 12:27:36.542601109 CEST	587	49793	198.54.126.161	192.168.2.3
May 14, 2022 12:27:40.508548975 CEST	587	49793	198.54.126.161	192.168.2.3
May 14, 2022 12:27:40.529777050 CEST	49793	587	192.168.2.3	198.54.126.161
May 14, 2022 12:27:40.704498053 CEST	587	49793	198.54.126.161	192.168.2.3
May 14, 2022 12:27:42.439783096 CEST	587	49793	198.54.126.161	192.168.2.3
May 14, 2022 12:27:42.440644026 CEST	49793	587	192.168.2.3	198.54.126.161
May 14, 2022 12:27:42.615334988 CEST	587	49793	198.54.126.161	192.168.2.3
May 14, 2022 12:27:42.615612030 CEST	587	49793	198.54.126.161	192.168.2.3
May 14, 2022 12:27:42.615740061 CEST	49793	587	192.168.2.3	198.54.126.161
May 14, 2022 12:27:42.616202116 CEST	49793	587	192.168.2.3	198.54.126.161
May 14, 2022 12:27:42.790404081 CEST	587	49793	198.54.126.161	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 12:26:45.816303968 CEST	49873	53	192.168.2.3	8.8.8.8
May 14, 2022 12:26:45.837141991 CEST	53	49873	8.8.8.8	192.168.2.3
May 14, 2022 12:26:50.101141930 CEST	63332	53	192.168.2.3	8.8.8.8
May 14, 2022 12:26:50.121200085 CEST	53	63332	8.8.8.8	192.168.2.3
May 14, 2022 12:27:30.753124952 CEST	59795	53	192.168.2.3	8.8.8.8
May 14, 2022 12:27:30.775355101 CEST	53	59795	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 12:27:35.432094097 CEST	63861	53	192.168.2.3	8.8.8.8
May 14, 2022 12:27:35.454005003 CEST	53	63861	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 12:26:45.816303968 CEST	192.168.2.3	8.8.8.8	0x8863	Standard query (0)	webmail.ocenmasters.com	A (IP address)	IN (0x0001)
May 14, 2022 12:26:50.101141930 CEST	192.168.2.3	8.8.8.8	0x53a2	Standard query (0)	webmail.ocenmasters.com	A (IP address)	IN (0x0001)
May 14, 2022 12:27:30.753124952 CEST	192.168.2.3	8.8.8.8	0x5ff3	Standard query (0)	webmail.ocenmasters.com	A (IP address)	IN (0x0001)
May 14, 2022 12:27:35.432094097 CEST	192.168.2.3	8.8.8.8	0x9827	Standard query (0)	webmail.ocenmasters.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 12:26:45.837141991 CEST	8.8.8.8	192.168.2.3	0x8863	No error (0)	webmail.ocenmasters.com		198.54.126.161	A (IP address)	IN (0x0001)
May 14, 2022 12:26:50.121200085 CEST	8.8.8.8	192.168.2.3	0x53a2	No error (0)	webmail.ocenmasters.com		198.54.126.161	A (IP address)	IN (0x0001)
May 14, 2022 12:27:30.775355101 CEST	8.8.8.8	192.168.2.3	0x5ff3	No error (0)	webmail.ocenmasters.com		198.54.126.161	A (IP address)	IN (0x0001)
May 14, 2022 12:27:35.454005003 CEST	8.8.8.8	192.168.2.3	0x9827	No error (0)	webmail.ocenmasters.com		198.54.126.161	A (IP address)	IN (0x0001)

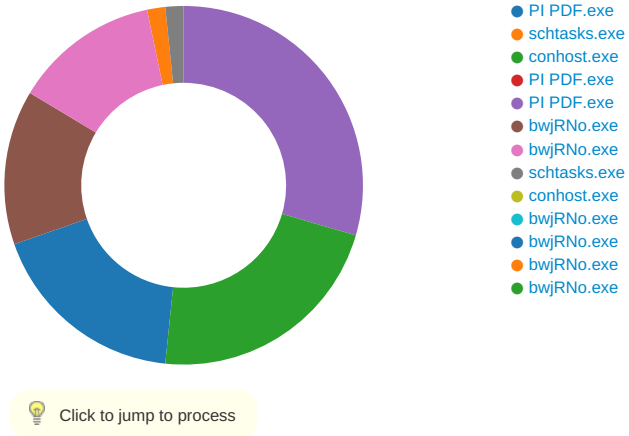
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 14, 2022 12:26:46.521317005 CEST	587	49752	198.54.126.161	192.168.2.3	220-premium12.web-hosting.com ESMTP Exim 4.94.2 #2 Sat, 14 May 2022 06:26:46 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 14, 2022 12:26:46.521672964 CEST	49752	587	192.168.2.3	198.54.126.161	EHLO 216554
May 14, 2022 12:26:46.695774078 CEST	587	49752	198.54.126.161	192.168.2.3	250-premium12.web-hosting.com Hello 216554 [102.129.143.55] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 14, 2022 12:26:46.698307037 CEST	49752	587	192.168.2.3	198.54.126.161	AUTH login YmFza2VyQG9jZW5tYXN0ZXJzLmNvbQ==
May 14, 2022 12:26:46.871859074 CEST	587	49752	198.54.126.161	192.168.2.3	334 UGFzc3dvcmQ6
May 14, 2022 12:26:48.456665993 CEST	587	49752	198.54.126.161	192.168.2.3	535 Incorrect authentication data
May 14, 2022 12:26:48.464423895 CEST	49752	587	192.168.2.3	198.54.126.161	MAIL FROM:<basker@ocenmasters.com>
May 14, 2022 12:26:48.637429953 CEST	587	49752	198.54.126.161	192.168.2.3	550 Access denied - Invalid HELO name (See RFC2821 4.1.1.1)
May 14, 2022 12:26:50.580655098 CEST	587	49756	198.54.126.161	192.168.2.3	220-premium12.web-hosting.com ESMTP Exim 4.94.2 #2 Sat, 14 May 2022 06:26:50 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 14, 2022 12:26:50.582381964 CEST	49756	587	192.168.2.3	198.54.126.161	EHLO 216554
May 14, 2022 12:26:50.756458044 CEST	587	49756	198.54.126.161	192.168.2.3	250-premium12.web-hosting.com Hello 216554 [102.129.143.55] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 14, 2022 12:26:50.757569075 CEST	49756	587	192.168.2.3	198.54.126.161	AUTH login YmFza2VyQG9jZW5tYXN0ZXJzLmNvbQ==
May 14, 2022 12:26:54.943469048 CEST	587	49756	198.54.126.161	192.168.2.3	334 UGFzc3dvcmQ6
May 14, 2022 12:26:57.174988031 CEST	587	49756	198.54.126.161	192.168.2.3	535 Incorrect authentication data
May 14, 2022 12:26:57.175209999 CEST	49756	587	192.168.2.3	198.54.126.161	MAIL FROM:<basker@ocenmasters.com>
May 14, 2022 12:26:57.349693060 CEST	587	49756	198.54.126.161	192.168.2.3	550 Access denied - Invalid HELO name (See RFC2821 4.1.1.1)
May 14, 2022 12:27:31.266168118 CEST	587	49778	198.54.126.161	192.168.2.3	220-premium12.web-hosting.com ESMTP Exim 4.94.2 #2 Sat, 14 May 2022 06:27:31 -0400 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
May 14, 2022 12:27:31.266634941 CEST	49778	587	192.168.2.3	198.54.126.161	EHLO 216554
May 14, 2022 12:27:31.444529057 CEST	587	49778	198.54.126.161	192.168.2.3	250-premium12.web-hosting.com Hello 216554 [102.129.143.55] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 14, 2022 12:27:31.444958925 CEST	49778	587	192.168.2.3	198.54.126.161	AUTH login YmFza2VyQG9jZW5tYXN0ZXJzLmNvbQ==
May 14, 2022 12:27:31.622293949 CEST	587	49778	198.54.126.161	192.168.2.3	334 UGFzc3dvcmQ6
May 14, 2022 12:27:33.153253078 CEST	587	49778	198.54.126.161	192.168.2.3	535 Incorrect authentication data
May 14, 2022 12:27:33.153584957 CEST	49778	587	192.168.2.3	198.54.126.161	MAIL FROM:<basker@ocenmasters.com>
May 14, 2022 12:27:33.331151962 CEST	587	49778	198.54.126.161	192.168.2.3	550 Access denied - Invalid HELO name (See RFC2821 4.1.1.1)
May 14, 2022 12:27:35.901343107 CEST	587	49793	198.54.126.161	192.168.2.3	220-premium12.web-hosting.com ESMTP Exim 4.94.2 #2 Sat, 14 May 2022 06:27:35 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 14, 2022 12:27:36.152457952 CEST	49793	587	192.168.2.3	198.54.126.161	EHLO 216554
May 14, 2022 12:27:36.327141047 CEST	587	49793	198.54.126.161	192.168.2.3	250-premium12.web-hosting.com Hello 216554 [102.129.143.55] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 14, 2022 12:27:36.327440023 CEST	49793	587	192.168.2.3	198.54.126.161	AUTH login YmFza2VyQG9jZW5tYXN0ZXJzLmNvbQ==
May 14, 2022 12:27:40.508548975 CEST	587	49793	198.54.126.161	192.168.2.3	334 UGFzc3dvcmQ6
May 14, 2022 12:27:42.439783096 CEST	587	49793	198.54.126.161	192.168.2.3	535 Incorrect authentication data
May 14, 2022 12:27:42.440644026 CEST	49793	587	192.168.2.3	198.54.126.161	MAIL FROM:<basker@ocenmasters.com>
May 14, 2022 12:27:42.615334988 CEST	587	49793	198.54.126.161	192.168.2.3	550 Access denied - Invalid HELO name (See RFC2821 4.1.1.1)

Statistics

Behavior



System Behavior

Analysis Process: PI PDF.exe PID: **6928**, Parent PID: **3772**

General

Target ID:	0

Start time:	12:26:06
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\PI PDF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PI PDF.exe"
Imagebase:	0x800000
File size:	904704 bytes
MD5 hash:	530C898EE065629D77B0B12781991D4F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.299681122.0000000003F42000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.299681122.0000000003F42000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.298244806.0000000003C1F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.298244806.0000000003C1F000.00000004.00000800.00020000.00000000.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	6DC4CF06	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	6DC4CF06	unknown
C:\Users\user\AppData\Roaming\jAZPdPbNZIxFH.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C0D1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp3224.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C0D7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PI PDF.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF5C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3224.tmp	success or wait	1	6C0D6A95	DeleteFileW

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\Roaming\jAZPdPbNZIxFH.exe	0	904704	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 45 7e 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 50 00 00 fd 0d 00 00 08 00 00 00 00 00 00 fd fd 0d 00 00 20 00 00 00 00 0e 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 40 0e 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.$PELE~bP @ @@	success or wait	1	6C0D1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp3224.tmp	0	1646	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 68 61 72 64 7a 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.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationIn	success or wait	1	6C0D1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PI PDF.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	6DF5C907	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	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Users\user\Desktop\PI PDF.exe	unknown	904704	success or wait	1	6C0D1B4F	ReadFile

Analysis Process: schtasks.exe PID: **6320**, Parent PID: **6928**

General

Target ID:	4
Start time:	12:26:28
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\jAZPdPbNZIxFH" /XML "C:\Users\user\AppData\Local\Temp\tmp3224.tmp
Imagebase:	0x1370000
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\tmp3224.tmp	unknown	2	success or wait	1	137AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp3224.tmp	unknown	1647	success or wait	1	137ABD9	ReadFile

Analysis Process: conhost.exe PID: **6292**, Parent PID: **6320**

General

Target ID:	5
Start time:	12:26:29
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: PI PDF.exe PID: **6384**, Parent PID: **6928**

General

Target ID:	7
Start time:	12:26:29
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\PI PDF.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x160000
File size:	904704 bytes
MD5 hash:	530C898EE065629D77B0B12781991D4F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: PI PDF.exe PID: **6344**, Parent PID: **6928**

General

Target ID:	8
Start time:	12:26:30
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\PI PDF.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x920000
File size:	904704 bytes

MD5 hash:	530C898EE065629D77B0B12781991D4F
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: 00000008.00000000.291840024.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.291840024.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.290109897.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.290109897.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.291116090.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.291116090.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.290705194.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.290705194.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.503050607.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.503050607.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.509270910.0000000002D01000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.509270910.0000000002D01000.00000004.00000800.00020000.00000000.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	6DC4CF06	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	6DC4CF06	unknown
C:\Users\user\AppData\Roaming\bwjRNo	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C0DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.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	6C0DDD66	CopyFileW
C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C0DDD66	CopyFileW
C:\Users\user\AppData\Roaming\xkhii1zz.ywa	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C0DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\xkhii1zz.ywa\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	6C0DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\xkhii1zz.ywa\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	6C0DBEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\xkhii1zz.ywa\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6C0DDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe:Zone.Identifier	success or wait	1	5E7C632	DeleteFileW
C:\Users\user\AppData\Roaming\xkhii1zz.ywa\Chrome\Default\Cookies	success or wait	1	6C0D6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\etc\hosts	824	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	127.0.0.1	success or wait	1	6C0D1B4F	WriteFile
C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 45 7e 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 50 00 00 fd 0d 00 00 08 00 00 00 00 00 00 fd fd 0d 00 00 20 00 00 00 00 0e 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 40 0e 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.$PELE~bP @ @@	success or wait	4	6C0DDD66	CopyFileW
C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.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	6C0DDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\xkhii1zz.ywa\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 00 00 00 03 00 2e 43 fd 0d 0f fd 00 04 0d 20 00 0f 67 0f fd 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	SQLite format 3@ .C g 8	success or wait	1	6C0DDD66	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	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C0D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C0D1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\05b98e77-fe4c-4961-9081-bc8c3f45dec3	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C0D1B4F	ReadFile
C:\Users\user\AppData\Roaming\xkhii1zz.ywa\Chrome\Default\Cookies	unknown	16384	success or wait	2	6C0D1B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	bwjRNo	unicode	C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe	success or wait	1	6C0D646A	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	bwjRNo	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C0DDE2E	RegSetValueExW

Analysis Process: bwjRNo.exe PID: **5976**, Parent PID: **3968**

General

Target ID:	19
Start time:	12:26:49
Start date:	14/05/2022
Path:	C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe"
Imagebase:	0xed0000
File size:	904704 bytes
MD5 hash:	530C898EE065629D77B0B12781991D4F
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: 00000013.00000002.395553350.00000000043BF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000013.00000002.395553350.00000000043BF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000002.397542210.00000000046E2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000013.00000002.397542210.00000000046E2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 49%, 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	6DC4CF06	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	6DC4CF06	unknown
C:\Users\user\AppData\Local\Temp\tmpC00D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C0D7038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC00D.tmp	success or wait	1	6C0D6A95	DeleteFileW

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\Temp\tmpC00D.tmp	0	1646	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 68 61 72 64 7a 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.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationIn	success or wait	1	6C0D1B4F	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	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C0D1B4F	ReadFile

Analysis Process: bwjRNo.exe PID: **6228**, Parent PID: **3968**

General

Target ID:	20
Start time:	12:26:57
Start date:	14/05/2022
Path:	C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe"
Imagebase:	0x360000
File size:	904704 bytes
MD5 hash:	530C898EE065629D77B0B12781991D4F
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: 00000014.00000002.374264940.00000000037CF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000014.00000002.374264940.00000000037CF000.00000004.00000800.00020000.00000000.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	6DC4CF06	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	6DC4CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\bwjRNo.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF5C78D	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\bwjRNo.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 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	6DF5C907	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	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC25705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C0D1B4F	ReadFile

Analysis Process: schtasks.exe PID: **6948**, Parent PID: **5976**

General

Target ID:	22
Start time:	12:27:06
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\jAZPdPbNZIxFH" /XML "C:\Users\user\AppData\Local\Temp\tmpC00D.tmp
Imagebase:	0x1370000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC00D.tmp	unknown	2	success or wait	1	137AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpC00D.tmp	unknown	1647	success or wait	1	137ABD9	ReadFile

Analysis Process: conhost.exe PID: **6968**, Parent PID: **6948**

General

Target ID:	23
Start time:	12:27:06
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: bwjRNo.exe PID: **1112**, Parent PID: **5976**

General

Target ID:	24
Start time:	12:27:07
Start date:	14/05/2022
Path:	C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe
Wow64 process (32bit):	false

Commandline:	{path}
Imagebase:	0x160000
File size:	904704 bytes
MD5 hash:	530C898EE065629D77B0B12781991D4F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: bwjRNo.exe PID: **4588**, Parent PID: **5976**

General	
Target ID:	27
Start time:	12:27:09
Start date:	14/05/2022
Path:	C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x200000
File size:	904704 bytes
MD5 hash:	530C898EE065629D77B0B12781991D4F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: bwjRNo.exe PID: **1252**, Parent PID: **5976**

General	
Target ID:	28
Start time:	12:27:11
Start date:	14/05/2022
Path:	C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x30000
File size:	904704 bytes
MD5 hash:	530C898EE065629D77B0B12781991D4F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: bwjRNo.exe PID: **6808**, Parent PID: **5976**

General	
Target ID:	29
Start time:	12:27:12
Start date:	14/05/2022
Path:	C:\Users\user\AppData\Roaming\bwjRNo\bwjRNo.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x750000
File size:	904704 bytes
MD5 hash:	530C898EE065629D77B0B12781991D4F
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: 0000001D.00000002.503093780.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001D.00000002.503093780.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001D.00000000.382535137.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001D.00000000.382535137.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001D.00000000.383158880.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001D.00000000.383158880.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001D.00000000.380264934.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001D.00000000.380264934.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001D.00000002.509640311.0000000002D41000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001D.00000002.509640311.0000000002D41000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001D.00000000.381604157.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001D.00000000.381604157.0000000000402000.00000040.00000400.00020000.00000000.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	6DC4CF06	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	6DC4CF06	unknown
C:\Users\user\AppData\Roaming\zktusgco.ufg	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C0DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\zktusgco.ufg\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	6C0DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\zktusgco.ufg\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	6C0DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\zktusgco.ufg\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	6C0DDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\zktusgco.ufg\Chrome\Default\Cookies	success or wait	1	6C0D6A95	DeleteFileW

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\Roaming\zktusgco.ufg\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 00 00 00 00 00 00 00 03 00 2e 43 fd 0d 0f fd 00 04 0d 20 00 0f 67 0f fd 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	SQLite format 3@ .C g 8	success or wait	1	6C0DDD66	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	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C0D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C0D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C0D1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\05b98e77-fe4c-4961-9081-bc8c3f45dec3	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C0D1B4F	ReadFile
C:\Users\user\AppData\Roaming\zktusgco.ufg\Chrome\Default\Cookies	unknown	16384	success or wait	2	6C0D1B4F	ReadFile

Disassembly

No disassembly