ID: 385436
Sample Name: Payment Confirmation WRT547879808054962 -copy-PDF.exe
Cookbook: default.jbs
Time: 14:21:27
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

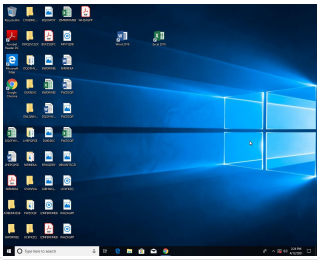
Analysis Report Payment Confirmation WRT5478798080…

Overview

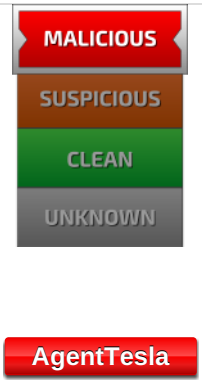
General Information

Sample Name:	Payment Confirmation WRT547879808054962 -copy- PDF.exe
Analysis ID:	385436
MD5:	4fd9b2fe1302836..
SHA1:	7b76fc786ae6827.
SHA256:	c42183aaf2368c1..
Tags:	agenttesla
Infos:	

Most interesting Screenshot:



Detection

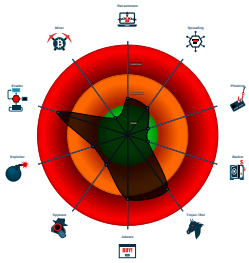


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- .NET source code contains potentia…
- .NET source code contains very larg…
- Drops PE files to the startup folder
- Executable has a suspicious name (…
- Initial sample is a PE file and has a …
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Suspicious powershell command line…
- AV process strings found (often use…
- Antivirus or Machine Learning detec…
- Checks if Antivirus/Antispyware/Fire…

Classification



Startup

- **System is w10x64**
- Payment Confirmation WRT547879808054962 -copy- PDF.exe (PID: 7004 cmdline: 'C:\Users\user\Desktop\Payment Confirmation WRT547879808054962 -copy- PDF.exe' MD5: 4FD9B2FE130283684B83A724E907F9CC)
  - cmd.exe (PID: 6312 cmdline: cmd.exe /c timeout 4 & 'C:\Windows\System32\wscript.exe' 'C:\Users\user\AppData\Local\Temp\\310197.js' && powershell -command Start-Sleep -s 4; Start-Process -WindowStyle hidden -FilePath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confirmation WRT547879808054962 -copy- PDF.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 3152 cmdline: timeout 4 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
    - wscript.exe (PID: 3436 cmdline: 'C:\Windows\System32\wscript.exe' 'C:\Users\user\AppData\Local\Temp\\310197.js' MD5: 7075DD7B9BE8807FCA93ACD86F724884)
    - powershell.exe (PID: 6616 cmdline: powershell -command Start-Sleep -s 4; Start-Process -WindowStyle hidden -FilePath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confirmation WRT547879808054962 -copy- PDF.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - Payment Confirmation WRT547879808054962 -copy- PDF.exe (PID: 6756 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confirmation WRT547879808054962 -copy- PDF.exe' MD5: 4FD9B2FE130283684B83A724E907F9CC)
        - Payment Confirmation WRT547879808054962 -copy- PDF.exe (PID: 5568 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confirmation WRT547879808054962 -copy- PDF.exe MD5: 4FD9B2FE130283684B83A724E907F9CC)
- Payment Confirmation WRT547879808054962 -copy- PDF.exe (PID: 6972 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confirmation WRT547879808054962 -copy- PDF.exe' MD5: 4FD9B2FE130283684B83A724E907F9CC)
  - Payment Confirmation WRT547879808054962 -copy- PDF.exe (PID: 6064 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confirmation WRT547879808054962 -copy- PDF.exe MD5: 4FD9B2FE130283684B83A724E907F9CC)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "francisco.branco@raposolda.ptraposowebmail.raposolda.ptdexter.chan.arkema@gmail.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000002.795783950.000000000397 7000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000E.00000002.899443671.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000014.00000002.901766585.0000000002DF 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000014.00000002.901766585.0000000002DF 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
0000000E.00000002.901604187.000000000298 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 14 entries				

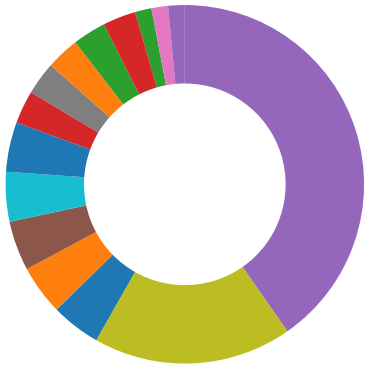
Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.Payment Confirmation WRT547879808054962 -copy-PDF.exe.35a91d8.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.Payment Confirmation WRT547879808054962 -copy-PDF.exe.3549198.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Payment Confirmation WRT547879808054962 -copy-PDF.exe.4298370.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Payment Confirmation WRT547879808054962 -copy-PDF.exe.42d8390.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
18.2.Payment Confirmation WRT547879808054962 -copy-PDF.exe.39777e0.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 12 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

System Summary:

.NET source code contains very large array initializations

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Suspicious powershell command line found

Boot Survival:

Drops PE files to the startup folder

Malware Analysis System Evasion:

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

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

Stealing of Sensitive Information:

Yara detected AgentTesla

Remote Access Functionality:

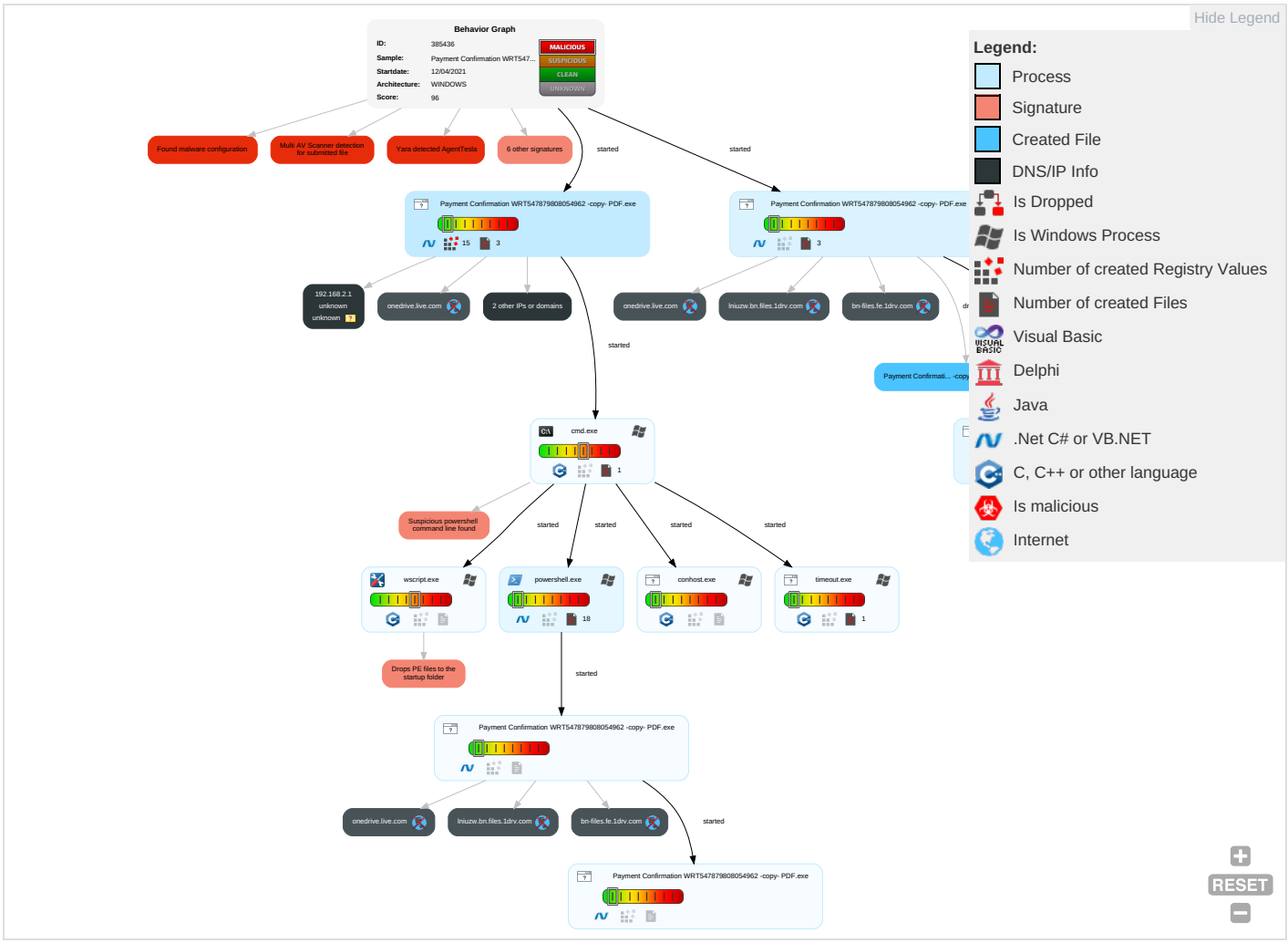
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 2 2 1	Registry Run Keys / Startup Folder 1	Process Injection 1 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	E In N C
Default Accounts	Command and Scripting Interpreter 1	DLL Side-Loading 1	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 5 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	E R C
Domain Accounts	Scripting 1	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 1 5 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	E Tr Lo
Local Accounts	PowerShell 1	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Virtualization/Sandbox Evasion 1 5 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	S Sy
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja D Si
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R Ac
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 1	Proc Filesystem	System Information Discovery 1 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D In P

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	R B

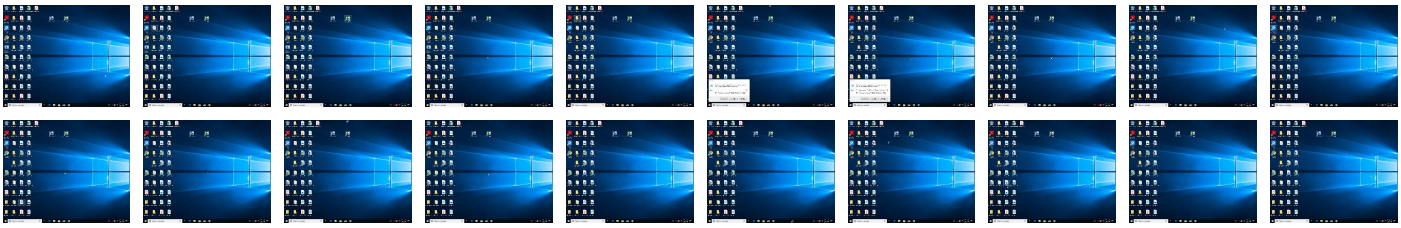
Behavior Graph



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
Payment Confirmation WRT547879808054962 -copy- PDF.exe	7%	Virustotal		Browse
Payment Confirmation WRT547879808054962 -copy- PDF.exe	2%	ReversingLabs	ByteCode-MSIL.Trojan.Injuke	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
20.2.Payment Confirmation WRT547879808054962 -copy- PDF.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.2.Payment Confirmation WRT547879808054962 -copy- PDF.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://lniuzw.bn.files.1drv.com46kxM	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://WOxurg.com	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://lniuzw.bn.files.1drv.com46kpMH	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://lniuzw.bn.files.1drv.com46k	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	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/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.pngL	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
onedrive.live.com	unknown	unknown	false		high
lniuzw.bn.files.1drv.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000E.00000002.901604187.000000002981000.00000004.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000014.00000002.901766585.000000002DF1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.000000005630000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.000000005630000.00000002.00000001.sdmp	false		high
http://https://onedrive.live.com/download?cid=A263F254A0224137&resid=A263F254A0224137%211108&authkey=AC8o8n	Payment Confirmation WRT547879808054962 -copy- PDF.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.000000005630000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lniuzw.bn.files.1drv.com46kxM	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.792585458.000000002841000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/Pester/PesterL	powershell.exe, 00000006.00000002.762740880.0000000005383000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers?	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.000000005630000.00000002.00000001.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000006.00000002.766581176.00000000062A4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.com	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.000000005630000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://WOxurg.com	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000014.00000002.901766585.0000000002DF1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.000000005630000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.000000005630000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.000000005630000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.000000005630000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/cThe	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.0000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.0000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.0000000005630000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.0000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.0000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.0000000005630000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.0000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.0000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.0000000005630000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contoso.com/	powershell.exe, 00000006.00000002.766581176.00000000062A4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000006.00000002.766581176.00000000062A4000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.0000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.0000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.0000000005630000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.0000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.0000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.0000000005630000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.0000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.0000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.0000000005630000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

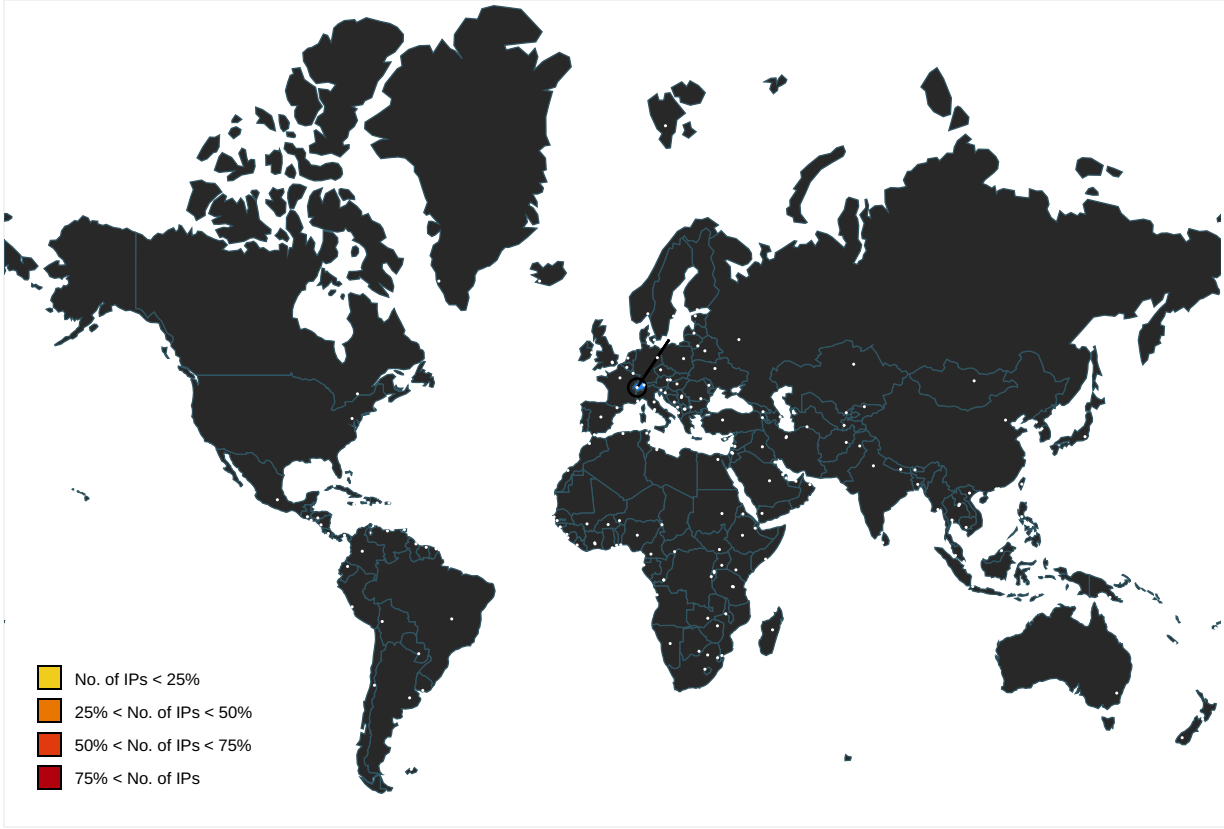
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.000000005630000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.000000005630000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.657236916.000000003151000.00000004.00000001.sdmp, powershell.exe, 00000006.00000002.762327814.0000000005241000.00000004.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.732726445.0000000002421000.00000004.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.792255406.00000000027F1000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.000000005630000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lniuzw.bn.files.1drv.com46kpMH	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.732872905.000000002471000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.658411301.00000000042D8000.00000004.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.734498913.000000003531000.00000004.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000E.00000002.899443671.000000000402000.00000040.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.795783950.000000003977000.00000004.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000014.00000002.899443040.000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://nuget.org/NuGet.exe	powershell.exe, 00000006.00000002.766581176.00000000062A4000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.000000005630000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.000000005630000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000014.00000002.901766585.0000000002DF1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000006.00000002.762740880.0000000005383000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.657236916.000000003151000.00000004.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.732726445.000000002421000.00000004.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.792255406.0000000027F1000.00000004.00000001.sdmp	false		high
http://https://lniuzw.bn.files.1drv.com/y4mXLu603m3jm6-CIIGtC1Az35xWdigz4o0siY8DGpOvlqCOwFnvAGFtLpqNdNR5rqj	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.792439393.000000002826000.00000004.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.792585458.000000002841000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000E.00000002.901604187.000000002981000.00000004.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000014.00000002.901766585.000000002DF1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000006.00000002.762740880.0000000005383000.00000004.00000001.sdmp	false		high
http://https://go.micro	powershell.exe, 00000006.00000002.766180901.0000000005AC4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lniuzw.bn.files.1drv.com/y4m5XX6QkrwADm0BE9F-KSc8YnyeZDSlbhZLWTjlFVYy-veD8YYcFqN28-tktG1NL85	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.732872905.000000002471000.00000004.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.732784004.000000002456000.00000004.00000001.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 00000006.00000002.766581176.00000000062A4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/download?cid=A263F254A0224137&resid=A263F254A0224137	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.657236916.000000003151000.00000004.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.732726445.000000002421000.00000004.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.792255406.00000027F1000.00000004.00000001.sdmp	false		high
http://https://lniuzw.bn.files.1drv.com46k	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.657314649.00031A2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000006.00000002.762740880.0000000005383000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.000000005630000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.000000005630000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.000000005630000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.000000005630000.00000002.00000001.sdmp	false		high
http://pesterbdd.com/images/Pester.pngL	powershell.exe, 00000006.00000002.762740880.0000000005383000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://lniuzw.bn.files.1drv.com/y4mfan37UkvAP8TzysQzz8DHHDcbHobX5nJ5uM87bEKvhvSbPaxkqGBpPPXuMtIgMOn	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.657349528.000000000320B000.00000004.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.657277111.000000003186000.00000004.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.732784004.0000000002456000.00000004.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.732944742.00000000024DA000.00000004.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.792439393.0000000002826000.00000004.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.792755020.00000000028AA000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.0000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.0000000005630000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://lniuzw.bn.files.1drv.com/y4mMeZFRcepSUvfHHz78iFvE-ZuqZc3MQxw65cL9BgxxRG8uSqXuaPfM-QzJZ6boj4Z	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.657303347.000000000319A000.00000004.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.657314649.00000000031A2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers8	Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000000.00000002.660012387.0000000006160000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 0000000B.00000002.738975716.000000005380000.00000002.00000001.sdmp, Payment Confirmation WRT547879808054962 -copy- PDF.exe, 00000012.00000002.797577914.0000000005630000.00000002.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.htmlL	powershell.exe, 00000006.00000002.762740880.0000000005383000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385436
Start date:	12.04.2021
Start time:	14:21:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment Confirmation WRT547879808054962 -copy-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:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal96.troj.adwa.evad.winEXE@17/5@12/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.107.3.254, 13.107.246.254, 40.88.32.150, 13.107.42.13, 13.107.43.13, 13.107.43.12, 13.107.42.12, 20.82.210.154, 104.42.151.234, 92.122.213.194, 92.122.213.247, 13.88.21.125, 104.43.139.144, 52.155.217.156, 20.54.26.129, 168.61.161.212, 20.50.102.62 • Excluded domains from analysis (whitelisted): odc-bn-files.onedrive.akadns.net.l-0003.dc-msedge.net.l-0003.l-msedge.net, odc-web-brs.onedrive.akadns.net, arc.msn.com.nsatc.net, s-ring.msedge.net, a1449.dscg2.akamai.net, arc.msn.com, l-0004.dc-msedge.net, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, odc-bn-files-geo.onedrive.akadns.net, l-0004.l-msedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, l-0003.l-msedge.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, odc-web-geo.onedrive.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, odc-bn-files-brs.onedrive.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, l-0003.dc-msedge.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, s-ring.s-9999.s-msedge.net, t-ring.msedge.net, ris.api.iris.microsoft.com, t-9999.t-msedge.net, s-9999.s-msedge.net, blobcollector.events.data.trafficmanager.net, t-ring.t-9999.t-msedge.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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
14:22:17	API Interceptor	733x Sleep call for process: Payment Confirmation WRT547879808054962 -copy- PDF.exe modified
14:22:31	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confirmation WRT547879808054962 -copy- PDF.exe

Time	Type	Description
14:22:53	API Interceptor	23x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment Confirmation WRT547879808054962 -copy- PDF.exe.log	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confirmation WRT547879808054962 -copy- PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	17500
Entropy (8bit):	5.278168442568793
Encrypted:	false
SSDEEP:	384:Qt9/UPInSQLQTQbLU0K3I1JNHGnudTNkQsF:VIQQbLU0bXhGudo
MD5:	F5F1413CCD1DC090DD88239D4A39BAB5

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
SHA1:	14EF31F6555443DBA547B0DE806B3231B713A30B
SHA-256:	FF8D5A5E7DC7307172BDDA03D536B45E6522B9F5D2F881017A42E2420A82C2DA
SHA-512:	229A735B581F1858A29AFC614901E535FB1925EB3A6673FC095B575F6C03588B911C8AF27533904AC14EA1DE12DAA40EBDA3C9DF67C05489D8877B77D832EB9
Malicious:	false
Reputation:	low
Preview:	@...e.....P.=.....~.:.....@.....D.....fZve...F.....x.)a.....System.Management.AutomationH.....<@.^.L."My...:'..... .Microsoft.PowerShell .ConsoleHost4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jdlw2aem.w5f.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qurmoeqb.f3b.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\Documents\20210412\PowerShell_transcript.688098.PfOYUrM6.20210412142231.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1257
Entropy (8bit):	5.228057303399328
Encrypted:	false
SSDEEP:	24:BxSA57vBZ1Zx2DOXdBmmuVMyx0WBHjeTKKjX4CIym1ZJXLBmmuVMyxWmnxSAZc:BZVvj/oONFubBqDYB1ZFFu6oZZc
MD5:	8CBD1A6C02FC25E98075A9AA33023528
SHA1:	82C3BA2269D1DBE9FBD75E3223A7AEC5298BA082
SHA-256:	6754F1A11062ECF59AD6035B40E55599EE625F2CF7EF2EB6616994E936709116
SHA-512:	BDF621458CC87A23270AE408D68B6E84E162167C77D4F3C97AD13BECB63A05F7A4B2EC9A5E022373E0827EEAB1DC4BA1DC37E5FE2E7249D3B5AF917218BC1B28
Malicious:	false

C:\Users\user\Documents\20210412\PowerShell_transcript.688098.PfOYUrM6.20210412142231.txt	
Preview:	**********..Windows PowerShell transcript start..Start time: 20210412142246..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 688098 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -command Start-Sleep -s 4; Start-Process -WindowStyle hidden -FilePath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confirmation WRT547879808054962 -copy- PDF.exe'..Process ID: 6616..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210412142247..**********..PS>Start-Sleep -s 4; Start-Process -WindowStyle hidden -FilePath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confi

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.957838652068988
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Payment Confirmation WRT547879808054962 -copy- PDF.exe
File size:	50688
MD5:	4fd9b2fe130283684b83a724e907f9cc
SHA1:	7b76fc786ae6827a016008d8f673f965382df74f
SHA256:	c42183aaf2368c13bddd363af982f2725e599581869f08f9041d6cd0c47cfe41
SHA512:	1fc302fc8b19f30b5ac118be018938c9724fc0405b1d7eea56a3b773d544528d29615fc43e172153e948b1b01b6160bd2a9ad92bb8ce2d148913345011b45946
SSDEEP:	768:967uC4xLTVJ/9kayxYuvqjCoe9aNz08WNc2:ayLPLuCj2cNz0vJ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...(.e`.....0.....v.... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40da76
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:	0x6065C628 [Thu Apr 1 13:10:00 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xda24	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe000	0x540	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x10000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xd8ec	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xba7c	0xbc00	False	0.311689660904	data	5.0246251873	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe000	0x540	0x600	False	0.39453125	data	3.87421246893	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x10000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe090	0x2b0	data		
RT_MANIFEST	0xe350	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	0.0.0.0
InternalName	Zandi.exe
FileVersion	0.0.0.0
CompanyName	
Comments	
ProductName	Zandi
ProductVersion	0.0.0.0
FileDescription	Zandi
OriginalFilename	Zandi.exe

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:22:01.802047014 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:01.976550102 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:02.025477886 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:03.085555077 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:03.134634018 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:04.036870956 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:04.089728117 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:15.124603033 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:15.176505089 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:15.191438913 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:15.252652884 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:15.811966896 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:15.952936888 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:15.964736938 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:16.099365950 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:33.239751101 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:33.302366018 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:37.047015905 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:37.100610971 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:38.358124018 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:38.417256117 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:40.778233051 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:40.831481934 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:42.231142044 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:42.285109997 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:45.063591957 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:45.112826109 CEST	53	56621	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:22:46.478192091 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:46.570987940 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:46.596683979 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:46.661503077 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:47.501341105 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:47.576450109 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:47.598403931 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:47.737687111 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:56.550940990 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:56.602713108 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:57.217248917 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:57.501565933 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:57.831146002 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:57.882616043 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:58.302270889 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:58.453994036 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:58.731311083 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:58.789798975 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:59.059166908 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:59.231391907 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 12, 2021 14:22:59.778220892 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:22:59.840100050 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:00.689821959 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:00.750257969 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:02.180051088 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:02.342681885 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:03.767469883 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:03.824595928 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:04.870042086 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:04.927144051 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:06.078257084 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:06.135668993 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:07.270997047 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:07.333539963 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:10.252119064 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:10.300569057 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:10.355849028 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:10.413444042 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:11.144407034 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:11.202083111 CEST	53	59794	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:11.211198092 CEST	55916	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:11.273487091 CEST	53	55916	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:13.633805037 CEST	52752	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:13.692388058 CEST	53	52752	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:22.148554087 CEST	60542	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:22.202380896 CEST	53	60542	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:23.078506947 CEST	60689	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:23.130515099 CEST	53	60689	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:24.128814936 CEST	64206	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:24.180645943 CEST	53	64206	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:25.317631960 CEST	50904	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:25.376395941 CEST	53	50904	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:41.039392948 CEST	57525	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:41.090745926 CEST	53	57525	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:42.727632999 CEST	53814	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:42.777848005 CEST	53	53814	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:47.441457033 CEST	53418	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:47.490138054 CEST	53	53418	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:47.678069115 CEST	62833	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:47.726665974 CEST	53	62833	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:49.166157007 CEST	59260	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:49.232930899 CEST	53	59260	8.8.8.8	192.168.2.4
Apr 12, 2021 14:23:56.312482119 CEST	49944	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:56.364100933 CEST	53	49944	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:23:59.689462900 CEST	63300	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:23:59.740407944 CEST	53	63300	8.8.8.8	192.168.2.4
Apr 12, 2021 14:24:00.599550962 CEST	61449	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:24:00.651227951 CEST	53	61449	8.8.8.8	192.168.2.4
Apr 12, 2021 14:24:01.490228891 CEST	51275	53	192.168.2.4	8.8.8.8
Apr 12, 2021 14:24:01.541055918 CEST	53	51275	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 14:22:15.124603033 CEST	192.168.2.4	8.8.8.8	0xfb05	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:22:15.191438913 CEST	192.168.2.4	8.8.8.8	0xcdec	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:22:15.811966896 CEST	192.168.2.4	8.8.8.8	0xdf6e	Standard query (0)	lniuzw.bn.files.1drv.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:22:15.964736938 CEST	192.168.2.4	8.8.8.8	0xc5c0	Standard query (0)	lniuzw.bn.files.1drv.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:22:46.478192091 CEST	192.168.2.4	8.8.8.8	0xebcd	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:22:46.596683979 CEST	192.168.2.4	8.8.8.8	0xd6f0	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:22:47.501341105 CEST	192.168.2.4	8.8.8.8	0x93a	Standard query (0)	lniuzw.bn.files.1drv.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:22:47.598403931 CEST	192.168.2.4	8.8.8.8	0x1eea	Standard query (0)	lniuzw.bn.files.1drv.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:23:10.252119064 CEST	192.168.2.4	8.8.8.8	0x181e	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:23:10.355849028 CEST	192.168.2.4	8.8.8.8	0x8266	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:23:11.144407034 CEST	192.168.2.4	8.8.8.8	0x751c	Standard query (0)	lniuzw.bn.files.1drv.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:23:11.211198092 CEST	192.168.2.4	8.8.8.8	0x1160	Standard query (0)	lniuzw.bn.files.1drv.com	A (IP address)	IN (0x0001)

DNS Answers

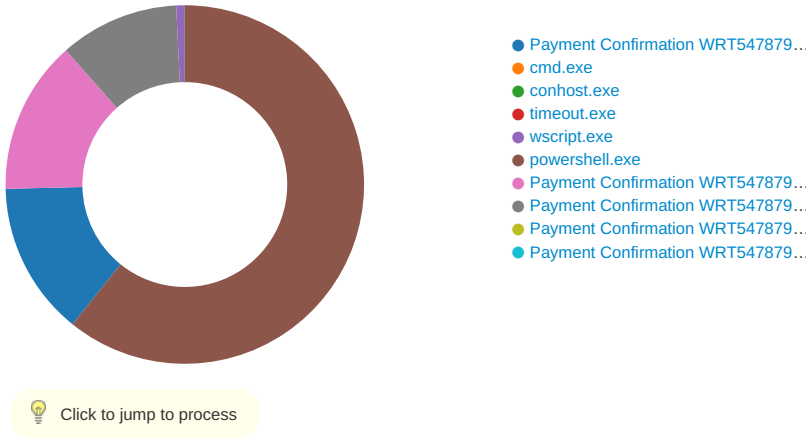
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 14:22:15.176505089 CEST	8.8.8.8	192.168.2.4	0xfb05	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:22:15.252652884 CEST	8.8.8.8	192.168.2.4	0xcdec	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:22:15.952936888 CEST	8.8.8.8	192.168.2.4	0xdf6e	No error (0)	lniuzw.bn.files.1drv.com	bn-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:22:15.952936888 CEST	8.8.8.8	192.168.2.4	0xdf6e	No error (0)	bn-files.fe.1drv.com	odc-bn-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:22:16.099365950 CEST	8.8.8.8	192.168.2.4	0xc5c0	No error (0)	lniuzw.bn.files.1drv.com	bn-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:22:16.099365950 CEST	8.8.8.8	192.168.2.4	0xc5c0	No error (0)	bn-files.fe.1drv.com	odc-bn-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:22:46.570987940 CEST	8.8.8.8	192.168.2.4	0xebcd	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:22:46.661503077 CEST	8.8.8.8	192.168.2.4	0xd6f0	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:22:47.576450109 CEST	8.8.8.8	192.168.2.4	0x93a	No error (0)	lniuzw.bn.files.1drv.com	bn-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:22:47.576450109 CEST	8.8.8.8	192.168.2.4	0x93a	No error (0)	bn-files.fe.1drv.com	odc-bn-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:22:47.737687111 CEST	8.8.8.8	192.168.2.4	0x1eea	No error (0)	lniuzw.bn.files.1drv.com	bn-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:22:47.737687111 CEST	8.8.8.8	192.168.2.4	0x1eea	No error (0)	bn-files.fe.1drv.com	odc-bn-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 14:23:10.300569057 CEST	8.8.8.8	192.168.2.4	0x181e	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:23:10.413444042 CEST	8.8.8.8	192.168.2.4	0x8266	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:23:11.202083111 CEST	8.8.8.8	192.168.2.4	0x751c	No error (0)	lniuzw.bn.files.1drv.com	bn-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:23:11.202083111 CEST	8.8.8.8	192.168.2.4	0x751c	No error (0)	bn-files.fe.1drv.com	odc-bn-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:23:11.273487091 CEST	8.8.8.8	192.168.2.4	0x1160	No error (0)	lniuzw.bn.files.1drv.com	bn-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:23:11.273487091 CEST	8.8.8.8	192.168.2.4	0x1160	No error (0)	bn-files.fe.1drv.com	odc-bn-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Payment Confirmation WRT547879808054962 -copy- PDF.exe PID: 7004 Parent PID: 6052

General

Start time:	14:22:08
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\Payment Confirmation WRT547879808054962 -copy- PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Payment Confirmation WRT547879808054962 -copy- PDF.exe'
Imagebase:	0xcb0000
File size:	50688 bytes
MD5 hash:	4FD9B2FE130283684B83A724E907F9CC

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: 00000000.00000002.658411301.00000000042D8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.658331129.0000000004260000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1CCF06	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	6D1CCF06	unknown
C:\Users\user\AppData\Local\Temp\310197.js	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C011E60	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	326	76 61 72 20 46 53 4f 20 3d 20 57 53 63 72 69 70 74 2e 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 53 63 72 69 70 74 69 6e 67 2e 46 69 6c 65 53 79 73 74 65 6d 4f 62 6a 65 63 74 22 29 3b 20 74 72 79 20 7b 20 46 53 4f 2e 4d 6f 76 65 46 69 6c 65 28 22 43 3a 5c 5c 55 73 65 72 73 5c 5c 6a 6f 6e 65 73 5c 5c 44 65 73 6b 74 6f 70 5c 5c 50 61 79 6d 65 6e 74 20 43 6f 6e 66 69 72 6d 61 74 69 6f 6e 20 57 52 54 35 34 37 38 37 39 38 30 38 30 35 34 39 36 32 20 2d 63 6f 70 79 2d 20 50 44 46 2e 65 78 65 22 2c 20 22 43 3a 5c 5c 55 73 65 72 73 5c 5c 6a 6f 6e 65 73 5c 5c 41 70 70 44 61 74 61 5c 5c 52 6f 61 6d 69 6e 67 5c 5c 4d 69 63 72 6f 73 6f 66 74 5c 5c 57 69 6e 64 6f 77 73 5c 5c 53 74 61 72 74 20 4d 65 6e 75 5c 5c 50 72 6f 67 72 61 6d 73 5c 5c 53 74 61 72 74 75 70 5c 5c 50	var FSO = Wscr ipt.CreateObject("scr<wbr>ipting.FileSystemObject"); try { FSO. MoveFile("C:\\Users\\user\\ Desktop\\Payment Confirmation WRT 547879808054962 -copy-PDF.exe", "C:\\Users\\user\\AppData\\ Roaming\\Microsoft\\Windo ws\\Start Menu\\Programs\\Startup\\ P	success or wait	1	6C011B4F	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	6D1A5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6312 Parent PID: 7004

General

Start time:	14:22:19
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /c timeout 4 & 'C:\Windows\System32\wscript.exe' 'C:\Users\user\AppData\Local\Temp\\310197.js' && powershell -command Start-Sleep -s 4; Start-Process -WindowStyle hidden -FilePath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confirmation WRT547879808054962 -copy- PDF.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: conhost.exe PID: 6428 Parent PID: 6312

General

Start time:	14:22:19
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000

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

Analysis Process: timeout.exe PID: 3152 Parent PID: 6312

General

Start time:	14:22:20
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 4
Imagebase:	0xe50000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
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

Analysis Process: wscript.exe PID: 3436 Parent PID: 6312

General

Start time:	14:22:27
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\wscript.exe' 'C:\Users\user\AppData\Local\Temp\\310197.js'
Imagebase:	0xaf0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Payment Confirmation WRT547879808054962 -copy- PDF.exe	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confirmation WRT547879808054962 -copy- PDF.exe	success or wait	1	6EDFC13B	MoveFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 6616 Parent PID: 6312

General

Start time:	14:22:29
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -command Start-Sleep -s 4; Start-Process -WindowStyle hidden -FilePath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confirmation WRT547879808054962 -copy- PDF.exe'
Imagebase:	0xf30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\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	6D1CCF06	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	6D1CCF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BF75B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BF75B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qurmoeqb.f3b.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C011E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jdlw2aem.w5f.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C011E60	CreateFileW
C:\Users\user\Documents\20210412	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C01BEFF	CreateDirectoryW
C:\Users\user\Documents\20210412\PowerShell_transcript.688098.PfOYUrM6.20210412142231.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C011E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qurmoeqb.f3b.ps1	success or wait	1	6C016A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jdlw2aem.w5f.psm1	success or wait	1	6C016A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qurmoeqb.f3b.ps1	unknown	1	31	1	success or wait	1	6C011B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jdlw2aem.w5f.psm1	unknown	1	31	1	success or wait	1	6C011B4F	WriteFile
C:\Users\user\Documents\20210412\PowerShell_transcript.688098.PfOYUrM6.20210412142231.txt	unknown	3	ef bb bf	...	success or wait	1	6C011B4F	WriteFile
C:\Users\user\Documents\20210412\PowerShell_transcript.688098.PfOYUrM6.20210412142231.txt	unknown	757	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 34 31 32 31 34 32 32 34 36 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 36 38 38 30 39 38 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	**********..Windows PowerShell transcript start..Start time: 20210412142246..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 688098 (Microsoft Windows NT 10.0.17134.0)..Host Application: power	success or wait	11	6C011B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 12 00 00 00 c9 0f 00 00 18 00 00 00 ea 0d 9a 05 50 08 3d 08 83 07 00 00 00 00 7e 02 3a 00 ca 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....P.=.....~.:.....@.....	success or wait	1	6D4976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	44 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 66 5a 76 65 a7 f4 b9 46 9f a9 b0 89 11 78 b4 29 61 0f 00 00 0e 00 1c 00	D.....fZve...F.....x.)a.....	success or wait	18	6D4976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	28	53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e	System.Management.Automation	success or wait	18	6D4976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6D4976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	8	6D4976FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	01 0e 80 00 00 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 58 64 40 00 56 64 40 00 fb 2a 40 00 54 01 40 01 f9 3e 40 00 cb 00 40 01 56 01 40 01 48 01 40 01 58 01 40 01 5b 01 40 01 4e 54 40 00 48 54 40 00 f4 53 40 00 8b 53 40 00 68 54 40 00 91 53 40 00 fa 53 40 00 82 53 40 00 5c 01 40 01 00 54 40 00 02 54 40 00 40 58 40 00 3f 58 40 00 1c 54 40 00 b8 53 40 00 fb 53 40 00 1e 54 40 00 19 54 40 00 78 54 40 00 7a 54 00 00 95 54 00 00 3d 4d 00 00 44 4d 00 00 3a 4d 00 00 22 4d 00 00 20 4d 00 00 21 4d 00 00 3b 4d 00 00 e0 44 00 00 e5 44 00 00 40 4d 00 00 3c 4d 00 00 24 4d 00 00 38 4d 00 00 3f 4d 00 00 16 3b 40 00 42 4d 00 00 ed 44 00 00 6d 45 00 00 45 4d 00 00 dc 71 00 00 dd 71 00 00 f8 53 00 00 98 25 00	....Xd@.Vd@..*@.T.@. .>@...@.V.@.H.@.X.@. [.@.NT@.HT@..S @..S@.hT@..S@..S@..S @.\.@..T@..T@.@X@.? X@..T@..S@..S@..T@..T @.xT@.zT...T..=M..DM..:M .."M.. M..!M..;M...D...D..@M.. <M..$M..8M..? M...;@.BM...D..mE..EM.. .q...q...S...%.	success or wait	8	6D4976FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D1ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D1A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D1B1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21312	success or wait	1	6D1B203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C011B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C011B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C011B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C011B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C011B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C011B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C011B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C011B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	129	6C011B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C011B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Analysis Process: Payment Confirmation WRT547879808054962 -copy- PDF.exe PID: 6972 Parent PID: 3424

General

Start time:	14:22:40
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confirmation WRT547879808054962 -copy- PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confirmation WRT547879808054962 -copy- PDF.exe'
Imagebase:	0x90000
File size:	50688 bytes

MD5 hash:	4FD9B2FE130283684B83A724E907F9CC
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: 0000000B.00000002.734498913.0000000003531000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.734571526.00000000035A9000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1CCF06	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	6D1CCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment Confirmation WRT547879808054962 -copy- PDF.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4DC78D	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\Payment Confirmation WRT547879808054962 -copy- PDF.exe.log	unknown	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",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_v4.0.3	success or wait	1	6D4DC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol

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	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Analysis Process: Payment Confirmation WRT547879808054962 -copy- PDF.exe PID: 6064 Parent PID: 6972

General

Start time:	14:22:53
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confirmation WRT547879808054962 -copy- PDF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confirmation WRT547879808054962 -copy- PDF.exe
Imagebase:	0x610000
File size:	50688 bytes
MD5 hash:	4FD9B2FE130283684B83A724E907F9CC
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: 0000000E.00000002.899443671.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.901604187.0000000002981000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.901604187.0000000002981000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1CCF06	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	6D1CCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Analysis Process: Payment Confirmation WRT547879808054962 -copy- PDF.exe PID: 6756 Parent PID: 6616

General

Start time:	14:23:05
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confirmation WRT547879808054962 -copy- PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confirmation WRT547879808054962 -copy- PDF.exe'
Imagebase:	0x330000
File size:	50688 bytes
MD5 hash:	4FD9B2FE130283684B83A724E907F9CC
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: 00000012.00000002.795783950.0000000003977000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.795361955.00000000038FF000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: Payment Confirmation WRT547879808054962 -copy- PDF.exe PID: 5568 Parent PID: 6756

General

Start time:	14:23:18
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confirmation WRT547879808054962 -copy- PDF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment Confirmation WRT547879808054962 -copy- PDF.exe
Imagebase:	0x8b0000
File size:	50688 bytes
MD5 hash:	4FD9B2FE130283684B83A724E907F9CC
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: 00000014.00000002.901766585.0000000002DF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000014.00000002.901766585.0000000002DF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000014.00000002.899443040.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis