ID: 344520
Sample Name: bXFjrxjRlb.exe
Cookbook: default.jbs
Time: 16:58:12
Date: 26/01/2021
Version: 31.0.0 Emerald

Table of Contents

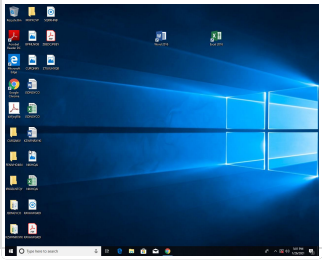
Analysis Report bXFjrxjRlb.exe

Overview

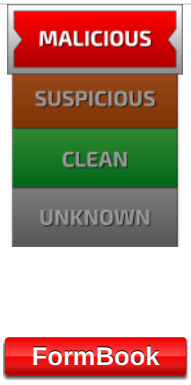
General Information

Sample Name:	bXFjrxjRlb.exe
Analysis ID:	344520
MD5:	4a595c5540f0a09.
SHA1:	9bd00bf1ffbdf53c..
SHA256:	d6c54588834faae.
Tags:	exe Formbook

Most interesting Screenshot:



Detection



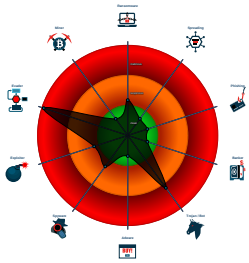
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- Allocates memory in foreign process…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…

Classification



Startup

- **System is w10x64**
- bXFjrxjRlb.exe (PID: 1212 cmdline: 'C:\Users\user\Desktop\bXFjrxjRlb.exe' MD5: 4A595C5540F0A097A5F11159CDF5C015)
  - AddInProcess32.exe (PID: 6460 cmdline: C:\Users\user\AppData\Local\Temp\AddInProcess32.exe MD5: F2A47587431C466535F3C3D3427724BE)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cscript.exe (PID: 3684 cmdline: C:\Windows\SysWOW64\cscript.exe MD5: 00D3041E47F99E48DD5FFFEDF60F6304)
        - cmd.exe (PID: 6932 cmdline: /c del 'C:\Users\user\AppData\Local\Temp\AddInProcess32.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6940 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x99c2",
    "KEY1_OFFSET 0x1e39e",
    "CONFIG SIZE : 0xf7",
    "CONFIG OFFSET 0x1e4a9",
    "URL SIZE : 33",
    "searching string pattern",
    "strings_offset 0x1cfb3",
    "searching hashes pattern",
    "--------------------------------------------------",
    "Decrypted Function Hashes",
    "--------------------------------------------------",
    "0x369b5b11",
    "0xf43668a6",
    "0x9804476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d70b3",
    "0x9f715020",
    "0xbf0a5e41",
    "0x2902d074",
    "0xf653b199",
    "0xc8c42cc6",
```

```
"0x2e1b7599",
"0x210d4d07",
"0x6d2a7921",
"0x8ea85a2f",
"0x207c50ff",
"0xb967410a",
"0x1eb17415",
"0xb46802f8",
"0x11da8518",
"0xf42ed5c",
"0x2885a3d3",
"0x445675fa",
"0x5c289b4c",
"0x40ede5aa",
"0xf24946a2",
"0x8559c3e2",
"0xb9d34d23",
"0xa14d0a19",
"0x2d07bbe2",
"0xbbd1d68c",
"0xb28c29d4",
"0x3911edeb",
"0xefad046d",
"0xa0605497",
"0xf5529cbf",
"0x5507576a",
"0xfa2467c8",
"0x5b6423bf",
"0xe22409b9",
"0xde1eba2",
"0xae847e2",
"0xa8cfcc9",
"0x26fc2c69",
"0x5d8a75ac",
"0x22eb3474",
"0x2b37c918",
"0x79402007",
"0x7544791c",
"0x641b2c94",
"0x1db04ecf",
"0xf5d02cd8",
"0xad0121a0",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd014c5",
"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",
"ecatcom.com",
"what3emoji.com",
"primbathandbody.com",
"yt-itclub.com",
"newbieeer.com",
"getyoursofa.com",
"mexicanitems.info",
"catalogcardgames.net",
"leagueofwomengolfers.com",
"gvanmp.com",
"midnightsunhi.com",
"cnluma.com",
"sunsetcherrydesigns.com",
"cosmoproturkey.com",
"inifinityapps.net",
"making50masks.com",
"battalionice.com",
"uk-calculation.net",
"frosteatlove.com",
"bs-mag.com",
"cuisd.life",
"searchlx.com",
"treycorbies.com",
"excellencepi.com",
"4week-keto-results.com",
"rotationdietplan.com",
"chinahousecoralville.com",
"xidao168.com",
"detuimelaar.com",
"fairschedulinglaws.com",
"jinnolouie.com",
"expresslacross.com",
"akealuminum.com",
"madebazar.com",
"phimixx.com",
"jel-tv365.com",
"shakahats.com",
"thabaddieztrap.net",
"petsglorious.com",
"misuperblog.com",
"scorebuddycx.com",
"sgbsmb.com",
"coolbeanstudios.com",
"khitthihonvidai.com",
"myattorneychoicesyoufind.info",
"thenewsdig.com",
"freeuikit.net",
"everydaycollars.com",
"carrerco.com",
"reviewdrkofford.com",
"dragonflyroad.com",
"quinple.com",
"kollektiv.agency",
"cimbank.info",
"productoshealthyandfun.com",
"dovecuwnebawe.com",
"saihohealth.com",
"thehostingroad.com",
"tadalafil.website",
"whereiswillgroup.com",
"ukchealth.com",
"alaskanoddgoods.com",
"praktik-stuff.online",
"gaiactg.com",
"f-end",
"--------------------------------------------------",
"Decrypted CnC URL",
"--------------------------------------------------",
"www.unitedfootballgames.com/bf3/lv0000"
```

```
        www.unitedjobboardcamps.com/bj3/\u0000
    ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.359609187.0000000003FE5000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.359609187.0000000003FE5000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9b4a:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9dc4:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x37408:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x37682:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x158e7:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x431a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x153d3:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x42c91:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x159e9:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x432a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x15b61:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x4341f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa7dc:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x3809a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1464e:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x41f0c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb4d5:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x38d93:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b599:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x48e57:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c59c:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000002.359609187.0000000003FE5000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1867b:$sqlite3step: 68 34 1C 7B E1 • 0x1878e:$sqlite3step: 68 34 1C 7B E1 • 0x45f39:$sqlite3step: 68 34 1C 7B E1 • 0x4604c:$sqlite3step: 68 34 1C 7B E1 • 0x186aa:$sqlite3text: 68 38 2A 90 C5 • 0x187cf:$sqlite3text: 68 38 2A 90 C5 • 0x45f68:$sqlite3text: 68 38 2A 90 C5 • 0x4608d:$sqlite3text: 68 38 2A 90 C5 • 0x186bd:$sqlite3blob: 68 53 D8 7F 8C • 0x187e5:$sqlite3blob: 68 53 D8 7F 8C • 0x45f7b:$sqlite3blob: 68 53 D8 7F 8C • 0x460a3:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.699879470.00000000003D0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.699879470.00000000003D0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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 • 0x1b337:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c33a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

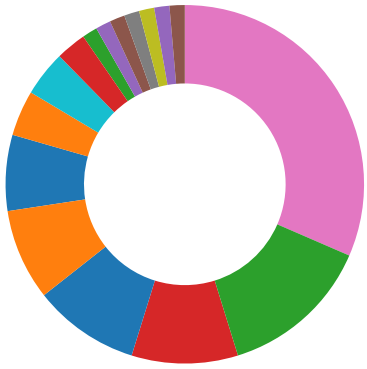
Source	Rule	Description	Author	Strings
1.2.AddInProcess32.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
1.2.AddInProcess32.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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b337:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c33a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.AddInProcess32.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18419:$sqlite3step: 68 34 1C 7B E1 • 0x1852c:$sqlite3step: 68 34 1C 7B E1 • 0x18448:$sqlite3text: 68 38 2A 90 C5 • 0x1856d:$sqlite3text: 68 38 2A 90 C5 • 0x1845b:$sqlite3blob: 68 53 D8 7F 8C • 0x18583:$sqlite3blob: 68 53 D8 7F 8C
1.2.AddInProcess32.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.AddInProcess32.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$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 • 0x1a537:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b53a:$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
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- 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 sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

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)

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

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

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

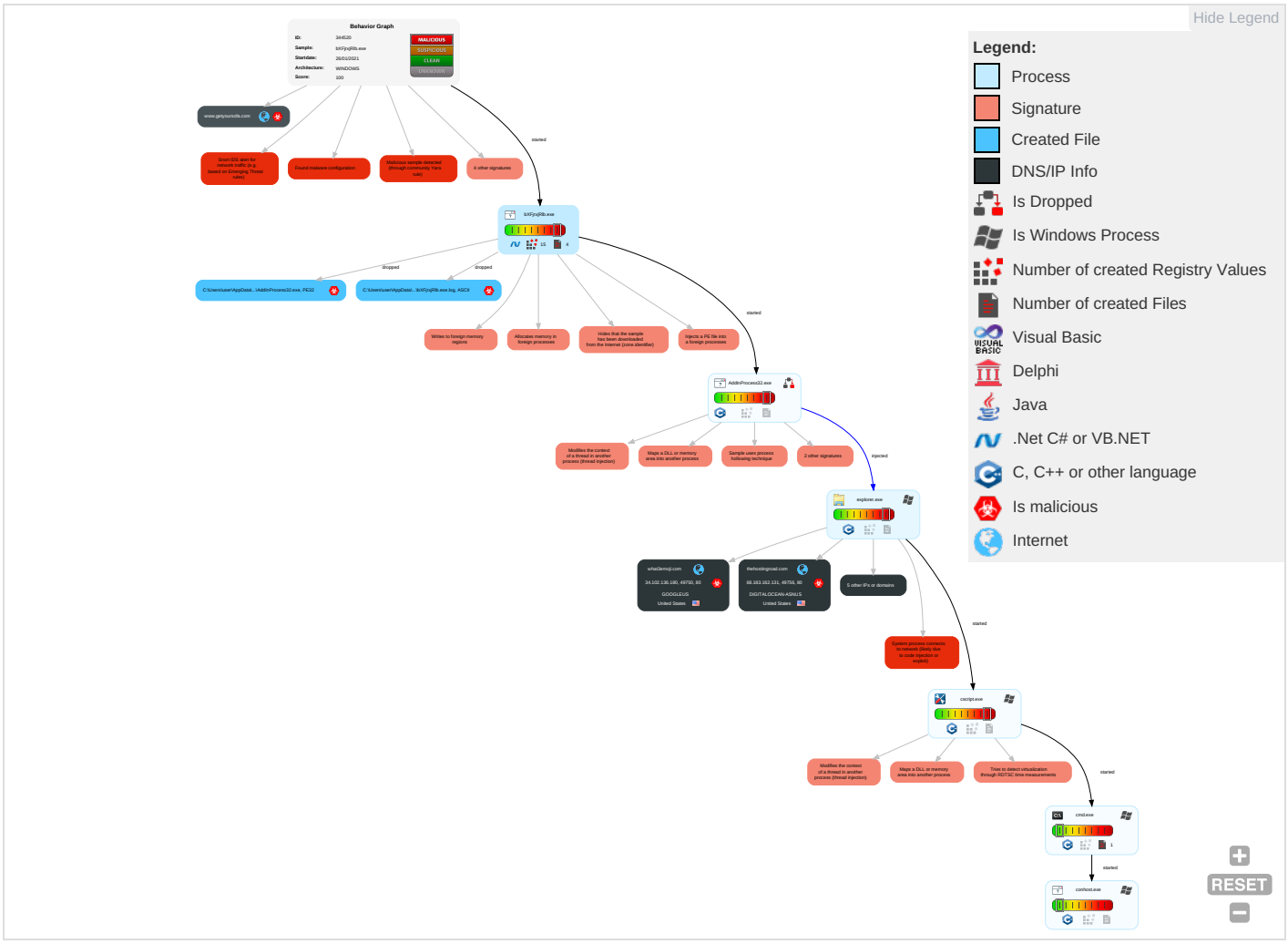
Remote Access Functionality:

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 8 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 1 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	Input Capture 1	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Ph 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	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Devic 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 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 8 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
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	Hidden Files and Directories 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statio

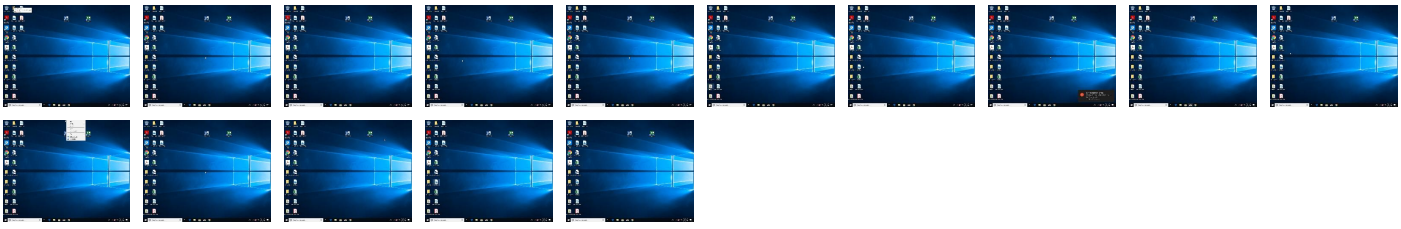
Behavior Graph



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
bXFjrxjRlb.exe	27%	Virustotal		Browse
bXFjrxjRlb.exe	28%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	
bXFjrxjRlb.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.AddInProcess32.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.getyoursofa.com	0%	Virustotal		Browse

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://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://www.what3emoji.com/bf3/?pPX=m4Qmgz02ndzlkmzRdXbnUnIUoJvahqq5/3lLTCGwMTubC4gHDN74yJVcJDUGCd+LoHuKsTQ0JA==&W6=jnKpRl-xV	0%	Avira URL Cloud	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://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	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://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://crl.microsofB	0%	Avira URL Cloud	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.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.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://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	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.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	

Source	Detection	Scanner	Label	Link
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.inifinityapps.net/bf3/?pPX=swuzFfgzYDLB3Bi4piS9eAlbkrlhpvPYJEwerncel/wmg54lN6WJu/MxY2hlnTt8ZuQ329MgbQ==&W6=jnKpRl-xV	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	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	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
thehostingroad.com	68.183.162.131	true	true		unknown
what3emoji.com	34.102.136.180	true	true		unknown
www.getyoursofa.com	162.241.30.16	true	true	• 0%, Virustotal, Browse	unknown
parkingpage.namecheap.com	198.54.117.215	true	false		high
www.thehostingroad.com	unknown	unknown	true		unknown
www.akealuminum.com	unknown	unknown	true		unknown
www.what3emoji.com	unknown	unknown	true		unknown
www.inifinityapps.net	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.what3emoji.com/bf3/?pPX=m4Qmgz02ndzlkmzRdXbnUnlUoJvahqq5/3ILTCGwMTubC4gHDN74yJVcJDUGCd+LoHuKsTQ0JA==&W6=jnKpRl-xV	true	• Avira URL Cloud: safe	unknown
http://www.inifinityapps.net/bf3/?pPX=swuzFfgzYDLB3Bi4piS9eAlbkrlhpvPYJEwerncel/wmg54lN6WJu/MxY2hlnTt8ZuQ329MgbQ==&W6=jnKpRl-xV	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000002.0000000 2.700588761.000000000095C000.0 0000004.00000020.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000002.0000000 0.386826331.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000002.0000000 0.386826331.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000002.0000000 0.386826331.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000002.0000000 0.386826331.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000002.0000000 0.386826331.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.adobe.cobj	bXFjrxjRlb.exe, 00000000.00000003.355490056.0000000008402000.00000004.00000001.sdmp, bXFjrxjRlb.exe, 00000000.00000003.341220156.00000000083F1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000002.00000000.386826331.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000002.00000000.386826331.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0	bXFjrxjRlb.exe, 00000000.00000002.356057420.000000000096F000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000002.00000000.386826331.000000000B1A6000.00000002.00000001.sdmp	false		high
http://ns.adobe.c/g	bXFjrxjRlb.exe, 00000000.00000003.355490056.0000000008402000.00000004.00000001.sdmp, bXFjrxjRlb.exe, 00000000.00000003.341220156.00000000083F1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.goog/gsr202	bXFjrxjRlb.exe, 00000000.00000002.356057420.000000000096F000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr	explorer.exe, 00000002.00000000.386826331.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	bXFjrxjRlb.exe, 00000000.00000002.356057420.000000000096F000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.microsofB	bXFjrxjRlb.exe, 00000000.00000003.349237983.000000000802D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schema.org/WebPage	bXFjrxjRlb.exe, 00000000.00000002.356197969.000000000254F000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000002.00000000.386826331.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000002.00000000.386826331.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000002.00000000.386826331.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000002.00000000.386826331.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000002.00000000.386826331.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000002.00000000.386826331.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000002.00000000.386826331.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000002.00000000.386826331.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000002.00000000.386826331.000000000B1A6000.00000002.00000001.sdmp	false		high
http://ocsp.pki.goog/gts1o1core0	bXFjrxjRlb.exe, 00000000.00000002.356057420.000000000096F000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/GTS1O1core.crl0	bXFjrxjRlb.exe, 00000000.00000002.356057420.000000000096F000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000002.00000000.386826331.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000002.00000000.386826331.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers8	explorer.exe, 00000002.0000000 0.386826331.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000002.0000000 0.386826331.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000002.0000000 0.386826331.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000002.0000000 0.386826331.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	bXFjrxjRlb.exe, 00000000.00000 002.356057420.000000000096F000 .00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000002.0000000 0.386826331.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	bXFjrxjRlb.exe, 00000000.00000 002.356178733.0000000002521000 .00000004.00000001.sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000002.0000000 0.386826331.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.ado/1	bXFjrxjRlb.exe, 00000000.00000 003.355490056.0000000008402000 .00000004.00000001.sdmp, bXFjr xjRlb.exe, 00000000.00000003.3 41220156.00000000083F1000.0000 0004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
68.183.162.131	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
198.54.117.215	unknown	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344520
Start date:	26.01.2021
Start time:	16:58:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	bXFjrxjRlb.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:	24
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@7/2@5/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 10.4% (good quality ratio 9.1%) • Quality average: 71.2% • Quality standard deviation: 33.2%
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: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 13.88.21.125, 172.217.23.36, 51.104.139.180, 95.101.22.224, 95.101.22.216, 95.101.27.142, 95.101.27.163, 52.155.217.156, 20.54.26.129, 51.103.5.186, 23.210.248.85 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, www.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:59:14	API Interceptor	1x Sleep call for process: bXFjrxjRlb.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
34.102.136.180	xl2Ml2iNJe.exe	Get hash	malicious	Browse	• www.ricardoinman.com/xle/?-ZnD=LjoXU6n8-&iBrlPD=43tORsMo6Gry83Td78nIWgxEplzIHXHZqBl7iQpQA31ZPQcRtwVYWDcsKQV/txd+LHV0DSgDXQ==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	v07PSzmSp9.exe	Get hash	malicious	Browse	• www.jikzo.com/c8so/?3ff87=Bcwq9mo1SLdxGMzaDRBSbVH3gidTK8xbNEF8M/tGLQ2aKWcuDQCQFtxR7k1oF3yRZXKc&uZWD=XPmPajepJ2gdvnZ
	NEW ORDER.xlsx	Get hash	malicious	Browse	• www.simplifiedvirtualsolutions.com/oean/?MdLxlt=mKgmb7I6yODGcWmnOnDfCd0CfDEQGPBdVeZhKsaKMoR3Qh4v4CLN6oxN3p9trG3799qCow==&gnU4Pf=yZPLGZXHl
	Inquiry_73834168_.xlsx	Get hash	malicious	Browse	• www.kaiyuansu.pro/incn/?9r_PU=-ZQLEn&e2Jdlzf8=4y+UTKzAJ4dBlp/RYYS74WaP+qCjnKVRzK/jF/x906cXBmLcUo8gxmNUvdqUiR1QG2msPA==
	winlog(1).exe	Get hash	malicious	Browse	• www.growingequity.fund/oean/?8pNhXv=yVML0zB0&u4XpH=VZAj6Grbo5w3dBd7w+9BSoe0Fg1VHX3dphJz9/egos9dVzX5qD6mqxE3tlZZ2ImCjS7epxmUBA==
	win32.exe	Get hash	malicious	Browse	• www.findthatsmartphone.com/incn/?8pBP5p=/AA5bjKPiaWw22bzCdt7lqNbxAyyPpv3elVlM12b4Zuyr5w4xH0F6TlfefQNvJyZz9qG&L6Ah=2dSLFXghYtFd0
	1-26.exe	Get hash	malicious	Browse	• www.catalogcardgames.net/bf3/?UXrxP8=0T3HW8l&URfXx=Sdh36sWiaQaHmuW5OuhNg2ZSKBobeXsq4DWTIDdmgtvI732RtscB8O3t4ssmBmGg4ghZ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Request.xlsx	Get hash	malicious	Browse	• www.cleverwares.com/c8so/?Rf=P253+QYRdhKTDdzjq4pa7Wp7svBpTNddHFol+cUWSKGzAXl94gLhBIvIcl/Xp4fU197lMA==&LDHHp=z4D80PDX
	INV_TMB_210567Y00.xlsx	Get hash	malicious	Browse	• www.5050alberta.com/xle/?8pqhs=XuVPlIEgAAku+dXH+MR8cy20ZHkP0iJzlT7lKUj3PYBKa8v0bSmzSfHWFfmBCUSgIWFn2Q==&tDH=XRR8
	RFQ.xlsx	Get hash	malicious	Browse	• www.blacknation.info/c8so/?pBU=HzuD_&gb24XB=6ATEh1s0NdZErsRPIUioXmvz20sSLCkN4f+QHjKAbluYenOJN9FSbPt8XJ2H+dMMf4Jp2Q==
	New Year Inquiry List.xlsx	Get hash	malicious	Browse	• www.primeoneimplants.com/qjnt/?tB=TtdpPpppFvG&1bwhC=nh3Tl/oLs4HXZ5hiWyD3n36TA5+xQ+CwXb+KxfiJNOta6blp58Sj1H/LHtoCWuUTeWdwKg==
	RF-E93-STD-068 SUPPLIES.xlsx	Get hash	malicious	Browse	• www.harperandchloe.com/xle/?5jFlkJJh=FNtvxHF14RtgzuhKSaLd0lIzxL3LkdKZj/Q/Opos8UfLtbug0tkzhu0XdD0TouZ6l/qGUQ==&LR-T=vBK0GdQp
	gPGTcEMoM1.exe	Get hash	malicious	Browse	• www.ctfocbdwholesale.com/bw82/?W6=Rxta6xhtzzdBFDuy4SYKtO8XUaMinJcredo77YczPu8Lep1ecFiaWqXH8h2T5haNROfU&odeTY=cnxhAP6x
	bgJPIZIYby.exe	Get hash	malicious	Browse	• www.engageautism.info/bw82/?GFND=n1L9MQk6NEQOasYlfxU4KXziLGivOllQbNtATfsC4RjAZctNbAJfQ2ExV87fcKcU54A&Rlj=YVlX8Hyx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	vA0mtZ7JzJ.exe	Get hash	malicious	Browse	• www.brainandbodystrengthcoach.com/csv8/?MjklsrcX=4rzgp1jZc7l8Whg0lztLQnvubqNqMY/2oz5HEUeZ+SGIDqCjyjtIs6qqwwlb5soGHyjF&Hp0xlh=EVvxc8
	E4Q30tDEB9.exe	Get hash	malicious	Browse	• www.conanbiopharma.com/z9n/?GzuX=Jhwq104eoCBg19EU7i3a/UNFlUD6BU+epYAdz34/Q5fulRMc24e0hydyrjaAvIdaUf1m&9rspoR=ffn0iZa81
	INGNhYonmgtGZ9Updf.exe	Get hash	malicious	Browse	• www.4thop.com/ur06/?2d=9rm4l4y&nt=yKWvtfxgXgd1h/cfVfwsL+vVHM9GHRLI6tHsLUWr1fII7HM154cThMJKgGXJGqB7HwFq
	560911_P.EXE	Get hash	malicious	Browse	• www.leagueofwomengolfers.com/bf3/?2d=8pJhqv2&mt=Rg5SRlzVdqtJGgbKsvZ2Ay09186BQEC1kuNds6zR1M82qUcQWtSjBMIC0cP/+2kk9Xcq
	RevisedPO.24488_pdf.exe	Get hash	malicious	Browse	• www.luxpropertyandassociates.com/nki/?-Z=9rwO08mLgykW/+F5WoH4KAy1ieMCsMl+05AKyLP7HaXoaQuR30wAwJPKQkPQMY0RHvTE&rTILhT=X4XHRfqP
	documents_0084568546754.exe	Get hash	malicious	Browse	• www.unlikelypolitician.com/hpg3/?GzuX=AgT4KauKKZQ2JUupBAGVU1xj9lzNj8Soa1/lSyFuPG4dLNFEFBMtgFS5ro8vw6+alj0G&AnB=O2Mxhrspi
68.183.162.131	IMG_1107.EXE	Get hash	malicious	Browse	• www.thehostingroad.com/bf3/?DXOX-=l8I6XPguYKFPGKeVh8gT1y9i2fKE+hPHZakSNaciRtP7EZ8w/BzDNNldYjh/9U9ktH10&KzuH=XPjDi0j0G

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.117.215	RevisedPO.24488_pdf.exe	Get hash	malicious	Browse	• www.doggybargains.com/nki/?-Z=TOQH/B74eY+lLUBsPfn02/AyeWt7NTM3T5MQ11peB6QiRzS5xhI/XYvznkNG9/RZ90Wt&rTILhT=X4XHRfqP
	yxYmHtT7uT.exe	Get hash	malicious	Browse	• www.accessible.legal/csv8/?EHU40X=gbWtoXjpHB&Aro=oGqbtMom9WGYi+RBhVD/q4yy78sx6VM5qFnCf+91Xqn8W7yN0ac+rgSlx9DJFvjgpGDVDlUe9g==
	Project review_Pdf.exe	Get hash	malicious	Browse	• www.volemate.com/dll/?t81X=+rBDSeByYOuwiyCs2FmR2y2szzEgjgAAJgIvvmfJRMvBkX5MwbWWrzyN0ALTtAZKZ6Ir&WPXhU=wBWHJtHHN
	Banking Details Review_Pdf.exe	Get hash	malicious	Browse	• www.workonlinetimallen.com/dll/?FPWlH4K=22Ck7sZymRlue/F9el9iWIuDvjTWQNWCbFaq8o3IMCkjvmOJhGd/Odg920f9GQzD8gYG&Bl=sHdPVHypI2c
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• www.swavhca.com/jskg/?9roHn=d8LPYq+5Arayfm1vXo3Q9MeTj0bruQyaWpvdMQHKTdQ1FO0+Z34o/nFcLDTuqn6wJ28t&npHhW=3fq4gDD0abs8
	RFQ 00068643 New Order Shipment to Jebel Ali Port UAE.exe	Get hash	malicious	Browse	• www.alitlereward.com/x2ee/?8pGxKNk8=Vtb1/iiBU+uCF3AJeGCOPklMCv99vxzvnxKn5/cIaWE1JMwW91M+jgsTK6I+a0rF2zAW&DzudC=Bxo0src
	3Y690n1UsS.exe	Get hash	malicious	Browse	• www.accessible.legal/csv8/?SR-D3jP=oGqbtMom9WGYi+RBhVD/q4yy78sx6VM5qFnCf+91Xqn8W7yN0ac+rgSlx+vzGuPbqxiE&J0GTk=3fPL-xo0rXp0UNn

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	hlNvQKaRR3.exe	Get hash	malicious	Browse	• www.pnorg .net/jskg/? yN6Ddr1H= FFllKUI2Vy 3AcuNhWrh4 fKbis3luBq Lkf2wubdQ4 CJ+GPQXPDv WWudAl4bM3 GwbQsdH4&8 p=2dOPB6nHz
	AT113020.exe	Get hash	malicious	Browse	• www.thank sforlove.c om/9t6k/?U Rflh=kTde6 z/9FBgibCJ h75hFV8EYW atL1OQ/rhf r5oU2UZBR6 XWcBOIn723 UV5Uezh3ZQ 4ot&UfrDal =0nMpqJVP5 t_PDD5p
	invoice No_SINI0068206497.exe	Get hash	malicious	Browse	• www.whole salebrands .xyz/mkr/
	PI210941.exe	Get hash	malicious	Browse	• www.teamc hi.club/t4vo/? o2J=Np nlt5ZtO906 n53msd9G5p BOdHOEeXQy D/1EjRFLMV 7cbHJomhnA cg5WDQDM5e zuEyU2&4h0 =vZR8DbS8Z 4yXah
	NA_GRAPH.EXE	Get hash	malicious	Browse	• www.teamc hi.club/t4vo/? lN64=N pnlt5ZtO90 6n53msd9G5 pBOdHOEeXQ yD/1EjRFLM V7cbHJomhn Acg5WDQDmm uDuAwc2&8p =MTKP1hb
	HussCrypted.exe	Get hash	malicious	Browse	• www.7days cale.info/cia6/? JtxL=XPv4nNDh& DXFTE=xgSo djwNOpvqRB gSHkNiwEBg /WwFTBg6sv wXL9igyoS1 pHT72fkq2l lttMIrDbkz mKwF7fpjCw==
	M11sVPvWUT.exe	Get hash	malicious	Browse	• www.kurdi shrealesta teagents.c om/ggb4/?p 6A=VzUgzpi Qkn30N256P Bkiej7gQ1K ho/1eBKyyw WWjmt2Ui9x M46LvrOITG rNcM7OxpBG x&oN9D=p4s XLLIPy2U4-N70
	#Uacac#Uc801 #Ud488#Ubaa9 #Ub9ac#Uc2a4#Ud2b8.exe	Get hash	malicious	Browse	• www.grand sonretail. com/5bs/?r 0=AmztrAFP eyVzzS+3x4 KThX9CMtZ1 P8IrwIWrZY ptpQCuj7ZP VnXcrmo/iP f97oeMmrlf &sZLdvf=8p Qt_4k

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	AAPUR2-M.exe	Get hash	malicious	Browse	• www.passiontip.com/g456/?8pt0_NFP=PuON5O03Ksi8fY7rErP/3xSQ1dHRQax2yunXZCWMmHTE5PPAC5+YkNyA1Bevc9/c9Z1b&RZ=X2JpoVIXxdlT_B0
	over.exe	Get hash	malicious	Browse	• www.exeteraesthetics.com/72w/
	William Smith CV.doc	Get hash	malicious	Browse	• www.fvqlkgedqjiqgapudkgq.com/post.php
	Michael Smith Resume.xls	Get hash	malicious	Browse	• www.march262020.site/post.php
	William Smith Resume.xls	Get hash	malicious	Browse	• www.march262020.site/post.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parkingpage.namecheap.com	winlog(1).exe	Get hash	malicious	Browse	• 198.54.117.216
	RevisedPO.24488_pdf.exe	Get hash	malicious	Browse	• 198.54.117.215
	SAMSUNG C&T UPCOMING PROJECTS19-027-MP-010203.exe.exe	Get hash	malicious	Browse	• 198.54.117.212
	IMG_1107.EXE	Get hash	malicious	Browse	• 198.54.117.212
	LOI.exe	Get hash	malicious	Browse	• 198.54.117.211
	PO_610.20-21.A2424.UP_PDF.exe	Get hash	malicious	Browse	• 198.54.117.217
	insz.exe	Get hash	malicious	Browse	• 198.54.117.218
	Invoice Payment Details.exe	Get hash	malicious	Browse	• 198.54.117.218
	Purchase order nr.0119-21.exe	Get hash	malicious	Browse	• 198.54.117.211
	Request for Quotation.exe	Get hash	malicious	Browse	• 198.54.117.216
	Bank details.exe	Get hash	malicious	Browse	• 198.54.117.212
	yxYmHtT7uT.exe	Get hash	malicious	Browse	• 198.54.117.215
	ins.exe	Get hash	malicious	Browse	• 198.54.117.210
	SHEXD2101127S_ShippingDocument_DkD.xlsx	Get hash	malicious	Browse	• 198.54.117.211
	PI_JAN9071011998_BARYSLpdf.exe	Get hash	malicious	Browse	• 198.54.117.217
	15012021.exe	Get hash	malicious	Browse	• 198.54.117.215
	Inv.exe	Get hash	malicious	Browse	• 198.54.117.217
	in.exe	Get hash	malicious	Browse	• 198.54.117.212
	urgent specification request.exe	Get hash	malicious	Browse	• 198.54.117.210
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• 198.54.117.210
www.getyoursofa.com	po071.exe	Get hash	malicious	Browse	• 162.241.30.16

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	Dridex-06-bc1b.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	Dridex-06-bc1b.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	winlog(1).exe	Get hash	malicious	Browse	• 198.54.117.216
	Revise Bank Details_pdf.exe	Get hash	malicious	Browse	• 198.54.116.236
	SecuriteInfo.com.BehavesLike.Win32.Generic.tz.exe	Get hash	malicious	Browse	• 198.187.31.7
	SecuriteInfo.com.Trojan.DownLoader36.37393.29158.exe	Get hash	malicious	Browse	• 198.187.31.7
	Payment Swift Copy_USD 206,832,000.00.pdf.exe	Get hash	malicious	Browse	• 198.54.116.236
	INGNhYonmgtGZ9Updf.exe	Get hash	malicious	Browse	• 198.54.117.244
	DSksIiT85D.exe	Get hash	malicious	Browse	• 199.188.200.97
	file.exe	Get hash	malicious	Browse	• 198.54.116.236
	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	• 104.219.248.112
	file.exe	Get hash	malicious	Browse	• 198.54.116.236
	RevisedPO.24488_pdf.exe	Get hash	malicious	Browse	• 198.54.117.215
	74725794.exe	Get hash	malicious	Browse	• 198.54.122.60

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	• 198.54.117.212
	ACH Funds Transferred.xls	Get hash	malicious	Browse	• 199.188.20 0.124
	ACH Funds Transferred.xls	Get hash	malicious	Browse	• 199.188.20 0.124
	BENVAV31BU.html	Get hash	malicious	Browse	• 63.250.38.8
	roK1cuvuLG.exe	Get hash	malicious	Browse	• 199.188.206.63
	DHL Details.exe	Get hash	malicious	Browse	• 198.54.126.165
DIGITALOCEAN-ASNUS	xDKOaCQQTQ.dll	Get hash	malicious	Browse	• 159.89.91.92
	4bEUfowOcg.dll	Get hash	malicious	Browse	• 159.89.91.92
	DAT.doc	Get hash	malicious	Browse	• 167.71.148.58
	ARCH_98_24301.doc	Get hash	malicious	Browse	• 138.68.42.38
	Bestellung.doc	Get hash	malicious	Browse	• 157.245.145.87
	RF-E93-STD-068 SUPPLIES.xlsx	Get hash	malicious	Browse	• 178.62.115.183
	vA0mtZ7JzJ.exe	Get hash	malicious	Browse	• 107.170.138.56
	SecuriteInfo.com.Generic.mg.b70d9bf0d6567964.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Artemis5EFC4C46397A.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Generic.mg.75b2def6a7e110ad.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Generic.mg.32d178838c0fd41b.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Artemis8353855AD729.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Generic.mg.b817172e5515b1af.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.ArtemisAA8578417627.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Artemis58690C2E2BCA.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.ArtemisTrojan.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Generic.mg.0551f32bbe68c20b.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Artemis961F6F63FB8F.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Generic.mg.11330b175b08895e.dll	Get hash	malicious	Browse	• 159.89.91.92
	SecuriteInfo.com.Generic.mg.284f325559f6aab1.dll	Get hash	malicious	Browse	• 159.89.91.92
GOOGLEUS	xl2Ml2iNJe.exe	Get hash	malicious	Browse	• 34.102.136.180
	eEXZHxdxFE.exe	Get hash	malicious	Browse	• 35.228.108.144
	v07PSzmSp9.exe	Get hash	malicious	Browse	• 34.102.136.180
	o3Z5sgjhEM.exe	Get hash	malicious	Browse	• 35.186.223.98
	ltf94qhZ37.exe	Get hash	malicious	Browse	• 35.228.108.144
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	Inquiry_73834168_.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	winlog(1).exe	Get hash	malicious	Browse	• 34.102.136.180
	win32.exe	Get hash	malicious	Browse	• 34.102.136.180
	DAT.doc	Get hash	malicious	Browse	• 35.200.206.198
	Bestellung.doc	Get hash	malicious	Browse	• 172.217.6.174
	.01.2021a.js	Get hash	malicious	Browse	• 35.228.108.144
	QT21006189.exe	Get hash	malicious	Browse	• 108.177.11 9.109
	1-26.exe	Get hash	malicious	Browse	• 34.102.136.180
	Request.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	INV_TMB_210567Y00.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	RFQ.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	New Year Inquiry List.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	RF-E93-STD-068 SUPPLIES.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	gPGTcEMoM1.exe	Get hash	malicious	Browse	• 34.102.136.180

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	Generator.cont.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	560911_P.EXE	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	IMG_61779.pdf.exe	Get hash	malicious	Browse	
	IMG_5391.EXE	Get hash	malicious	Browse	
	czZ769nM6r.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IMG_1107.EXE	Get hash	malicious	Browse	
	r3q6Bv8naR.exe	Get hash	malicious	Browse	
	sy1RnlHl8Y.exe	Get hash	malicious	Browse	
	qyMlTIBawC.exe	Get hash	malicious	Browse	
	Qn2AQrgfqJ.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.509.28611.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.509.17348.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.509.7497.exe	Get hash	malicious	Browse	
	IMG_12283.exe	Get hash	malicious	Browse	
	IMG_06176.pdf.exe	Get hash	malicious	Browse	
	IMG_50617.pdf.exe	Get hash	malicious	Browse	
	IMG_06177.pdf.exe	Get hash	malicious	Browse	
	Order_List_PO# 081929.exe	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Users\user\Desktop\bXFjrxjRlb.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1873
Entropy (8bit):	5.355036985457214
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjovitHoxHhAHKzvr1qHj:iqXeqm00YqhQnouRqjoKtlxHeqzTwD
MD5:	CDA95282F22F47DA2FDDC9E912B67FEF
SHA1:	67A40582A092B5DF40C3EB61A361A2D336FC69E0
SHA-256:	179E50F31095D0CFA13DCBB9CED6DEE424DFE8CEF8E05BDE1F840273F45E5F49
SHA-512:	1D151D92AE982D2149C2255826C2FFB89A475A1EB9B9FE93DC3706F3016CD6B309743B36A4D7F6D68F48CE25391FDA7A2BAE42061535EEA7862460424A3A2036
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Local\Temp\AddInProcess32.exe

Process:	C:\Users\user\Desktop\bXFjrxjRlb.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	42080
Entropy (8bit):	6.2125074198825105
Encrypted:	false
SSDEEP:	384:gc3JOvwWj8Gpw0A67dOpRIMKJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+QsPZw:g4JU8g17dl6Iq88MoBd7mFViqM5sL2
MD5:	F2A47587431C466535F3C3D3427724BE
SHA1:	90DF719241CE04828F0DD4D31D683F84790515FF
SHA-256:	23F4A2CCDCE499C524CF43793FDA8E773D809514B5471C02FA5E68F0CDA7A10B
SHA-512:	E9D0819478DDDA47763C7F5F617CD258D0FACBBBFFE0C7A965EDE9D0D884A6D7BB445820A3FD498B243BBD8BECBA146687B61421745E32B86272232C6F9E90D8
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	
Joe Sandbox View:	• Filename: Generator.cont.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: 560911_P.EXE, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: IMG_61779.pdf.exe, Detection: malicious, Browse • Filename: IMG_5391.EXE, Detection: malicious, Browse • Filename: czZ769nM6r.exe, Detection: malicious, Browse • Filename: IMG_1107.EXE, Detection: malicious, Browse • Filename: r3q6Bv8naR.exe, Detection: malicious, Browse • Filename: sy1RnlHl8Y.exe, Detection: malicious, Browse • Filename: qyMlTlBawC.exe, Detection: malicious, Browse • Filename: Qn2AQrgfqJ.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PackedNET.509.28611.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PackedNET.509.17348.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PackedNET.509.7497.exe, Detection: malicious, Browse • Filename: IMG_12283.exe, Detection: malicious, Browse • Filename: IMG_06176.pdf.exe, Detection: malicious, Browse • Filename: IMG_50617.pdf.exe, Detection: malicious, Browse • Filename: IMG_06177.pdf.exe, Detection: malicious, Browse • Filename: Order_List_PO# 081929.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..X.....w... .....@.. ..... .`.....Hw..O..... .....f..`>.....v..... ....H.....text....W... ...X..... ..`.rsrc... .....Z.....@..@.relo c.....d.....@..B.....|w.....H.....#...Q.....u.....0..K.....-..*..i....*...r...p.o....,...r...p.o....-..*.....o.....o.....$...*.....o....(....(.....:...(....o.....r...p.o.....4.....o..... .....o.....s .....o!...s".....s#.....r]..prg..po$.....r...p.o$.....r...pr...po$.....s.....(%.....tB...r...p(&...&..r...p.('...s(.....o)...&..o*....(+...o,.....&...(- ....*.....3..@.....R...s.....s....(....*:.(/.....}P...*J.{P....o0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.620907239788479
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:	bXFjrxjRlb.exe
File size:	772608
MD5:	4a595c5540f0a097a5f11159cdf5c015
SHA1:	9bd00bf1ffbdf53c841cd8d8b0a4244fdb7ba583
SHA256:	d6c54588834faae60153c6a2e7318a7e9f243b9dbfbd6e0fc44d45f4d55c9fcf
SHA512:	5d00dca3ca2b9cf7e381576ac61d9dcd9166529f4a77b9b196962b295ced4af5d372af8aa351da6aef9d3fdbd897f0e1273799601f6429e5069ce826ecdff1d2
SSDEEP:	12288:Axu4lHfNbxp4FiDROtGr4eYNriW4/zxPZVCq6r8FSl:Axu4H/4RtRe2+TVCq6r8FS
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...K..^.....~...J..... .....@.. ....`.....

File Icon

Icon Hash:	aaacae8e96a2c0e6

Static PE Info

General

Entrypoint:	0x4b9cfe
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

General

Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x5E2E884B [Mon Jan 27 06:50:51 2020 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
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb9ca4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xba000	0x46fa	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0xb7d04	0xb7e00	False	0.557449226717	data	5.60682914242	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xba000	0x46fa	0x4800	False	0.154405381944	data	2.48778714004	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc0000	0xc	0x200	False	0.041015625	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xba130	0x4028	data		
RT_GROUP_ICON	0xbe158	0x14	data		
RT_VERSION	0xbe16c	0x3a4	data		
RT_MANIFEST	0xbe510	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 2005 4;@:9>CF>>5?A@<AE4D4
Assembly Version	1.0.0.0
InternalName	IMG_155710.exe
FileVersion	5.8.10.13
CompanyName	4;@:9>CF>>5?A@<AE4D4
Comments	A7E@4HA4?@7HB;B98GH
ProductName	56:53B29963AH9:F76>A
ProductVersion	5.8.10.13
FileDescription	56:53B29963AH9:F76>A
OriginalFilename	IMG_155710.exe

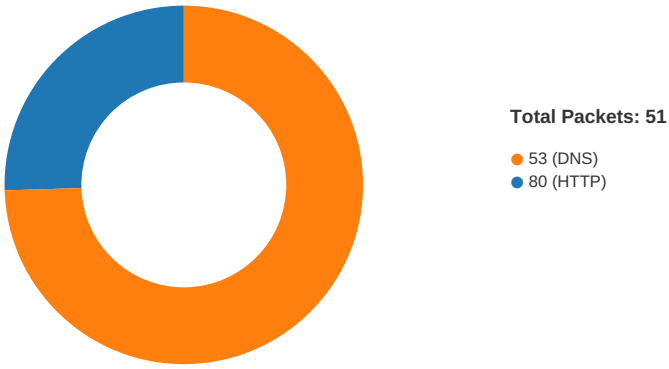
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/26/21-17:00:12.996209	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49750	34.102.136.180	192.168.2.6
01/26/21-17:00:54.182765	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49758	80	192.168.2.6	198.54.117.215
01/26/21-17:00:54.182765	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49758	80	192.168.2.6	198.54.117.215
01/26/21-17:00:54.182765	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49758	80	192.168.2.6	198.54.117.215
01/26/21-17:01:57.688028	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49759	80	192.168.2.6	162.241.30.16

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/26/21-17:01:57.688028	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49759	80	192.168.2.6	162.241.30.16
01/26/21-17:01:57.688028	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49759	80	192.168.2.6	162.241.30.16

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 17:00:12.814466000 CET	49750	80	192.168.2.6	34.102.136.180
Jan 26, 2021 17:00:12.857068062 CET	80	49750	34.102.136.180	192.168.2.6
Jan 26, 2021 17:00:12.857337952 CET	49750	80	192.168.2.6	34.102.136.180
Jan 26, 2021 17:00:12.857362032 CET	49750	80	192.168.2.6	34.102.136.180
Jan 26, 2021 17:00:12.897577047 CET	80	49750	34.102.136.180	192.168.2.6
Jan 26, 2021 17:00:12.996208906 CET	80	49750	34.102.136.180	192.168.2.6
Jan 26, 2021 17:00:12.996234894 CET	80	49750	34.102.136.180	192.168.2.6
Jan 26, 2021 17:00:12.996419907 CET	49750	80	192.168.2.6	34.102.136.180
Jan 26, 2021 17:00:12.996989965 CET	49750	80	192.168.2.6	34.102.136.180
Jan 26, 2021 17:00:13.038964987 CET	80	49750	34.102.136.180	192.168.2.6
Jan 26, 2021 17:00:33.377145052 CET	49756	80	192.168.2.6	68.183.162.131
Jan 26, 2021 17:00:33.572619915 CET	80	49756	68.183.162.131	192.168.2.6
Jan 26, 2021 17:00:33.572856903 CET	49756	80	192.168.2.6	68.183.162.131
Jan 26, 2021 17:00:33.572993994 CET	49756	80	192.168.2.6	68.183.162.131
Jan 26, 2021 17:00:33.769326925 CET	80	49756	68.183.162.131	192.168.2.6
Jan 26, 2021 17:00:33.769351959 CET	80	49756	68.183.162.131	192.168.2.6
Jan 26, 2021 17:00:33.769365072 CET	80	49756	68.183.162.131	192.168.2.6
Jan 26, 2021 17:00:33.769821882 CET	49756	80	192.168.2.6	68.183.162.131
Jan 26, 2021 17:00:33.769942045 CET	49756	80	192.168.2.6	68.183.162.131
Jan 26, 2021 17:00:33.965962887 CET	80	49756	68.183.162.131	192.168.2.6
Jan 26, 2021 17:00:53.989685059 CET	49758	80	192.168.2.6	198.54.117.215
Jan 26, 2021 17:00:54.182435989 CET	80	49758	198.54.117.215	192.168.2.6
Jan 26, 2021 17:00:54.182614088 CET	49758	80	192.168.2.6	198.54.117.215
Jan 26, 2021 17:00:54.182765007 CET	49758	80	192.168.2.6	198.54.117.215
Jan 26, 2021 17:00:54.375332117 CET	80	49758	198.54.117.215	192.168.2.6
Jan 26, 2021 17:00:54.375354052 CET	80	49758	198.54.117.215	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 16:58:59.737405062 CET	56023	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:58:59.793910027 CET	53	56023	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:01.634555101 CET	58384	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:01.682532072 CET	53	58384	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:03.126521111 CET	60261	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:03.174284935 CET	53	60261	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:04.347095966 CET	56061	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 16:59:04.395015955 CET	53	56061	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:06.558878899 CET	58336	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:06.609677076 CET	53	58336	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:06.882843018 CET	53781	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:06.939060926 CET	53	53781	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:07.675842047 CET	54064	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:07.726490021 CET	53	54064	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:09.141752958 CET	52811	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:09.192516088 CET	53	52811	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:10.480093956 CET	55299	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:10.528147936 CET	53	55299	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:12.182248116 CET	63745	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:12.232950926 CET	53	63745	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:22.726092100 CET	50055	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:22.774058104 CET	53	50055	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:23.954519033 CET	61374	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:24.005290985 CET	53	61374	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:24.974210978 CET	50339	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:25.022103071 CET	53	50339	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:28.057495117 CET	63307	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:28.105453014 CET	53	63307	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:32.877170086 CET	49694	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:32.937530994 CET	53	49694	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:47.445007086 CET	54982	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:47.503876925 CET	53	54982	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:48.435337067 CET	50010	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:48.491889954 CET	53	50010	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:49.027430058 CET	63718	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:49.086314917 CET	53	63718	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:49.512528896 CET	62116	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:49.560516119 CET	53	62116	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:49.687978029 CET	63816	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:49.732337952 CET	55014	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:49.747180939 CET	53	63816	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:49.783117056 CET	53	55014	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:50.231868982 CET	62208	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:50.282481909 CET	53	62208	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:51.278779984 CET	57574	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:51.336147070 CET	53	57574	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:51.915112019 CET	51818	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:51.974304914 CET	53	51818	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:52.664999008 CET	56628	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:52.723587036 CET	53	56628	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:53.605007887 CET	60778	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:53.661519051 CET	53	60778	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:54.538484097 CET	53799	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:54.597676039 CET	53	53799	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:55.061053991 CET	54683	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:55.117429972 CET	53	54683	8.8.8.8	192.168.2.6
Jan 26, 2021 16:59:55.668350935 CET	59329	53	192.168.2.6	8.8.8.8
Jan 26, 2021 16:59:55.725994110 CET	53	59329	8.8.8.8	192.168.2.6
Jan 26, 2021 17:00:12.740839005 CET	64021	53	192.168.2.6	8.8.8.8
Jan 26, 2021 17:00:12.807508945 CET	53	64021	8.8.8.8	192.168.2.6
Jan 26, 2021 17:00:28.781791925 CET	56129	53	192.168.2.6	8.8.8.8
Jan 26, 2021 17:00:28.829874039 CET	53	56129	8.8.8.8	192.168.2.6
Jan 26, 2021 17:00:29.233709097 CET	58177	53	192.168.2.6	8.8.8.8
Jan 26, 2021 17:00:29.290179968 CET	53	58177	8.8.8.8	192.168.2.6
Jan 26, 2021 17:00:33.129590034 CET	50700	53	192.168.2.6	8.8.8.8
Jan 26, 2021 17:00:33.187967062 CET	53	50700	8.8.8.8	192.168.2.6
Jan 26, 2021 17:00:33.200325012 CET	54069	53	192.168.2.6	8.8.8.8
Jan 26, 2021 17:00:33.374711037 CET	53	54069	8.8.8.8	192.168.2.6
Jan 26, 2021 17:00:50.817951918 CET	61178	53	192.168.2.6	8.8.8.8
Jan 26, 2021 17:00:50.865824938 CET	53	61178	8.8.8.8	192.168.2.6
Jan 26, 2021 17:00:53.927881002 CET	57017	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 17:00:53.988415003 CET	53	57017	8.8.8.8	192.168.2.6
Jan 26, 2021 17:01:37.210289955 CET	56327	53	192.168.2.6	8.8.8.8
Jan 26, 2021 17:01:37.280924082 CET	53	56327	8.8.8.8	192.168.2.6
Jan 26, 2021 17:01:57.442735910 CET	50243	53	192.168.2.6	8.8.8.8
Jan 26, 2021 17:01:57.517740011 CET	53	50243	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2021 17:00:12.740839005 CET	192.168.2.6	8.8.8.8	0xc8c8	Standard query (0)	www.what3emoji.com	A (IP address)	IN (0x0001)
Jan 26, 2021 17:00:33.200325012 CET	192.168.2.6	8.8.8.8	0x750a	Standard query (0)	www.thehostingroad.com	A (IP address)	IN (0x0001)
Jan 26, 2021 17:00:53.927881002 CET	192.168.2.6	8.8.8.8	0x41dd	Standard query (0)	www.inifinityapps.net	A (IP address)	IN (0x0001)
Jan 26, 2021 17:01:37.210289955 CET	192.168.2.6	8.8.8.8	0x368d	Standard query (0)	www.akealuminum.com	A (IP address)	IN (0x0001)
Jan 26, 2021 17:01:57.442735910 CET	192.168.2.6	8.8.8.8	0xa7fe	Standard query (0)	www.getyoursofa.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 17:00:12.807508945 CET	8.8.8.8	192.168.2.6	0xc8c8	No error (0)	www.what3emoji.com	what3emoji.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 17:00:12.807508945 CET	8.8.8.8	192.168.2.6	0xc8c8	No error (0)	what3emoji.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 26, 2021 17:00:33.374711037 CET	8.8.8.8	192.168.2.6	0x750a	No error (0)	www.thehostingroad.com	thehostingroad.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 17:00:33.374711037 CET	8.8.8.8	192.168.2.6	0x750a	No error (0)	thehostingroad.com		68.183.162.131	A (IP address)	IN (0x0001)
Jan 26, 2021 17:00:53.988415003 CET	8.8.8.8	192.168.2.6	0x41dd	No error (0)	www.inifinityapps.net	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 17:00:53.988415003 CET	8.8.8.8	192.168.2.6	0x41dd	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 26, 2021 17:00:53.988415003 CET	8.8.8.8	192.168.2.6	0x41dd	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 26, 2021 17:00:53.988415003 CET	8.8.8.8	192.168.2.6	0x41dd	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 26, 2021 17:00:53.988415003 CET	8.8.8.8	192.168.2.6	0x41dd	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 26, 2021 17:00:53.988415003 CET	8.8.8.8	192.168.2.6	0x41dd	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 26, 2021 17:00:53.988415003 CET	8.8.8.8	192.168.2.6	0x41dd	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 26, 2021 17:00:53.988415003 CET	8.8.8.8	192.168.2.6	0x41dd	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 26, 2021 17:01:37.280924082 CET	8.8.8.8	192.168.2.6	0x368d	Server failure (2)	www.akealuminum.com	none	none	A (IP address)	IN (0x0001)
Jan 26, 2021 17:01:57.517740011 CET	8.8.8.8	192.168.2.6	0xa7fe	No error (0)	www.getyoursofa.com		162.241.30.16	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.what3emoji.com
- www.thehostingroad.com
- www.inifinityapps.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49750	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 17:00:12.857362032 CET	5589	OUT	GET /bf3/?pPX=m4Qmgz02ndzlkmzRdXbnUnIUoJvahqq5/3ILTCGwMTubC4gHDN74yJVcJDUGCd+LoHuKsTQ0JA== &W6=jnKpRl-xV HTTP/1.1 Host: www.what3emoji.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 26, 2021 17:00:12.996208906 CET	5589	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 26 Jan 2021 16:00:12 GMT Content-Type: text/html Content-Length: 275 ETag: "600b4d46-113" 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	192.168.2.6	49756	68.183.162.131	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 17:00:33.572993994 CET	5614	OUT	GET /bf3/?pPX=l8I6XPguYKFPGKeVh8gT1y9i2fKE+hPHZakSNaciRtP7EZ8w/BzDNNldYjt/uExn0X1icGC4Ug== &W6=jnKpRl-xV HTTP/1.1 Host: www.thehostingroad.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 17:00:33.769351959 CET	5616	IN	HTTP/1.1 302 Found Connection: close Content-Type: text/html Content-Length: 682 Date: Tue, 26 Jan 2021 16:00:33 GMT Server: LiteSpeed Cache-Control: no-cache, no-store, must-revalidate, max-age=0 Location: http://www.thehostingroad.com/cgi-sys/suspendedpage.cgi?pPX=l8I6XPguYKFPGKeVh8gT1y9i2fKE+hPHZakSNaciRtP7EZ8w/BzDNNldYjt/uExn0X1icGC4Ug==&W6=jnKpRl-xV Vary: User-Agent Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 32 20 46 6f 75 6e 64 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 32 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 46 6f 75 6e 64 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" ><title> 302 Found</title></head><body style="color: #444; margin:0;font: normal 14px /20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 302 Found The document has been temporarily moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49758	198.54.117.215	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 17:00:54.182765007 CET	5628	OUT	GET /bf3/?pPX=swuzFfgzYDLB3Bi4piS9eAlbkrlhpvPYJEwernceI/wmg54lN6WJu/MxY2hInTt8ZuQ329MgbQ==&W6=jnKpRl-xV HTTP/1.1 Host: www.inifinityapps.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

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

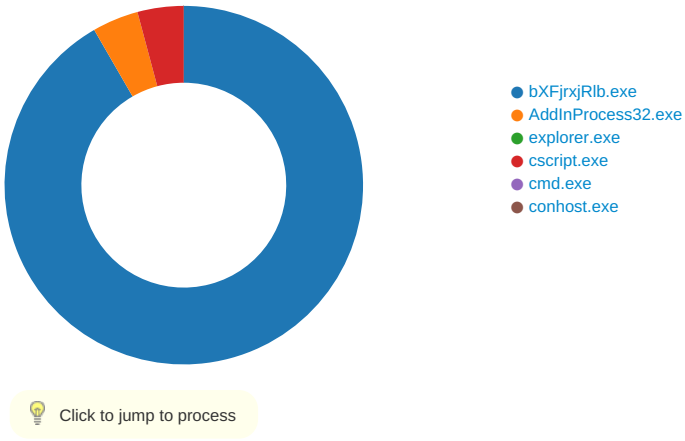
Processes

Process: explorer.exe, Module: user32.dll

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

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: bXFjrxjRlb.exe PID: 1212 Parent PID: 5976

General

Start time:	16:59:04
Start date:	26/01/2021
Path:	C:\Users\user\Desktop\bXFjrxjRlb.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\bXFjrxjRlb.exe'
Imagebase:	0x110000
File size:	772608 bytes
MD5 hash:	4A595C5540F0A097A5F11159CDF5C015
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: 00000000.00000002.359609187.0000000003FE5000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.359609187.0000000003FE5000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.359609187.0000000003FE5000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.359423289.0000000003E79000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.359423289.0000000003E79000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.359423289.0000000003E79000.00000004.00000001.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	6DCCCF06	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	6DCCCF06	unknown
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	69CE27B	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\bXFjrxjRlb.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFDC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0	42080	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 1d 5a 8e 5a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 58 00 00 00 0c 00 00 00 00 00 00 9a 77 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 c0 00 00 00 02 00 00 dc 8d 01 00 03 00 60 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....Z.Z.......... ....0..X...........w... ....@.. ....`.................	success or wait	1	69CE27B	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\bXFjrxjRlb.exe.log	unknown	1873	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 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 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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..3,"PresentationCore, Version=	success or wait	1	6DFDC907	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	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CC11B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: AddInProcess32.exe PID: 6460 Parent PID: 1212

General

Start time:	16:59:11
Start date:	26/01/2021
Path:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
Imagebase:	0x9e0000
File size:	42080 bytes
MD5 hash:	F2A47587431C466535F3C3D3427724BE
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: 00000001.00000002.401988886.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.401988886.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.401988886.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.402861692.0000000001280000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.402861692.0000000001280000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.402861692.0000000001280000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.402643394.0000000001250000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.402643394.0000000001250000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.402643394.0000000001250000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	419E67	NtReadFile

Analysis Process: explorer.exe PID: 3440 Parent PID: 6460

General

Start time:	16:59:21
Start date:	26/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
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: cscript.exe PID: 3684 Parent PID: 3440

General

Start time:	16:59:33
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\cscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cscript.exe
Imagebase:	0x1190000
File size:	143360 bytes
MD5 hash:	00D3041E47F99E48DD5FFFEDF60F6304
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: 00000007.00000002.699879470.00000000003D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.699879470.00000000003D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.699879470.00000000003D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.700544777.0000000000D90000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.700544777.0000000000D90000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.700544777.0000000000D90000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.700734017.00000000010F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.700734017.00000000010F0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.700734017.00000000010F0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	3E9E67	NtReadFile

Analysis Process: cmd.exe PID: 6932 Parent PID: 3684

General

Start time:	16:59:37
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Local\Temp\AddInProcess32.exe'
Imagebase:	0x2a0000
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: 6940 Parent PID: 6932

General

Start time:	16:59:38
Start date:	26/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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