ID: 344528
Sample Name:
4NoiNHCNoU.exe
Cookbook: default.jbs
Time: 17:06:45
Date: 26/01/2021
Version: 31.0.0 Emerald

Table of Contents

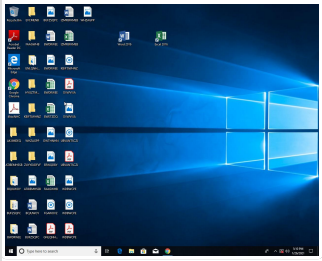
Analysis Report 4NoiNHCNoU.exe

Overview

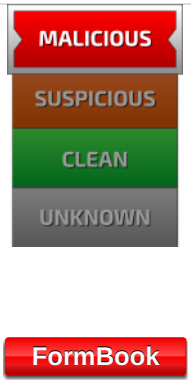
General Information

Sample Name:	4NoiNHCNoU.exe
Analysis ID:	344528
MD5:	204e0bf841b9900.
SHA1:	a3b3152dbea14e..
SHA256:	2ba9185ecb7b43..
Tags:	exe

Most interesting Screenshot:



Detection

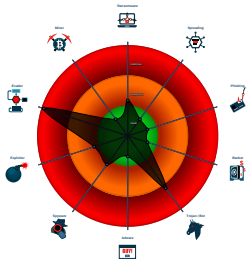


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- 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…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …

Classification



Startup

- **System is w10x64**
- 4NoiNHCNoU.exe (PID: 6340 cmdline: 'C:\Users\user\Desktop\4NoiNHCNoU.exe' MD5: 204E0BF841B9900FA03D6DFF302857F3)
  - AddInProcess32.exe (PID: 6436 cmdline: C:\Users\user\AppData\Local\Temp\AddInProcess32.exe MD5: F2A47587431C466535F3C3D3427724BE)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autoconv.exe (PID: 5752 cmdline: C:\Windows\SysWOW64\autoconv.exe MD5: 4506BE56787EDCD771A351C10B5AE3B7)
      - help.exe (PID: 6840 cmdline: C:\Windows\SysWOW64\help.exe MD5: 09A715036F14D3632AD03B52D1DA6BFF)
        - cmd.exe (PID: 6768 cmdline: /c del 'C:\Users\user\AppData\Local\Temp\AddInProcess32.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6748 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x8bbc",
    "KEY1_OFFSET 0x1d6b1",
    "CONFIG SIZE : 0xc7",
    "CONFIG OFFSET 0x1d7b6",
    "URL SIZE : 25",
    "searching string pattern",
    "strings_offset 0x1c363",
    "searching hashes pattern",
    "--------------------------------------------------",
    "Decrypted Function Hashes",
    "--------------------------------------------------",
    "0x9d07c71e",
    "0xf43668a6",
    "0x980476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d70a3",
    "0x9f716fd2",
    "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",
"0xad012162",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd014b5",
"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",
"gcdragons.com",
"gfdfraveis.xyz",
"diorcve.com",
"souqmar.info",
"websiteinawknd.com",
"esmartdubai.com",
"ctyjg.com",
"monalizacos.com",
"motherkidsonline.com",
"allpackedup.com",
"dl-dianshi.com",
"cobourgautoglass.com",
"goldenhourcpr.com",
"dominantreplacement.com",
"psicologiabenavet.com",
"laxvestcapital.com",
"konsultan-kesehatan.com",
"hudsonhoodle.com",
"zolarcrm.com",
"sorbolento.com",
"hull3dprints.com",
"inclusivevc.com",
"work-yourway.com",
"cheekypundit.com",
"dokhithai.xyz",
"kbsp.site",
"crysalisuk.com",
"atlantamars.com",
"poklonnaya7.com",
"spider-manshopping.com",
"ponyimage.com",
"loveitfactor.com",
"southaustinbullionexchange.com",
"bestloveshayarihindi.com",
"bastienandtaly.com",
"rangers3.xyz",
"living-story.com",
"milkandmemories.com",
"finddealercars.com",
"northernsourcer.com",
"desolaluna.com",
"goodthingtoday.com",
"tatepasini.com",
"itsbrodee.com",
"finecutbutcher.com",
"noodlenoggins.com",
"cookiefoo.com",
"gafademoda.com",
"dandysoftgames.com",
"katysteakhouse.com",
"doblatumonto.com",
"7225662.com",
"qbbkk.com",
"haofeel.com",
"barefootentertainmenthi.com",
"scotrianbank.com",
"makwarthgamer.com",
"dataintegrityindia.com",
"yaseneva.com",
"thepopindia.com",
"eshtemca.com",
"pingpongforlife.com",
"golfbet247.com",
"leesungroadmarking.com",
"f-end",
"-------------------------------------------------",
"Decrypted CnC URL",
"-------------------------------------------------",
```

```
    "www.artdonline.com/wdva/\u0000"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.708829602.0000000001510000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.708829602.0000000001510000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.708829602.0000000001510000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.678246488.0000000004BB9000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.678246488.0000000004BB9000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0xbf9d2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xbfc3c:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xed2b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xed51c:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x11ab82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x11adec:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xcb75f:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xf903f:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x12690f:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xcb24b:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xf8b2b:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1263fb:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xcb861:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xf9141:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x126a11:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xcb9d9:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xf92b9:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x126b89:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xc0654:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0xedf34:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x11b804:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06
Click to see the 19 entries				

Unpacked PEs

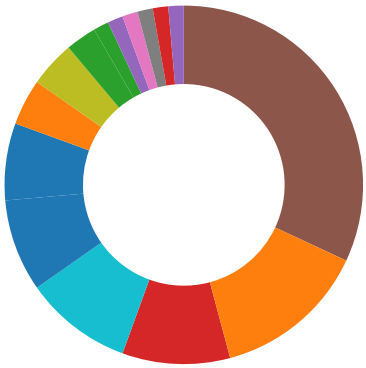
Source	Rule	Description	Author	Strings
2.2.AddInProcess32.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
2.2.AddInProcess32.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a6e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b6ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.AddInProcess32.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
2.2.AddInProcess32.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.AddInProcess32.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

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:

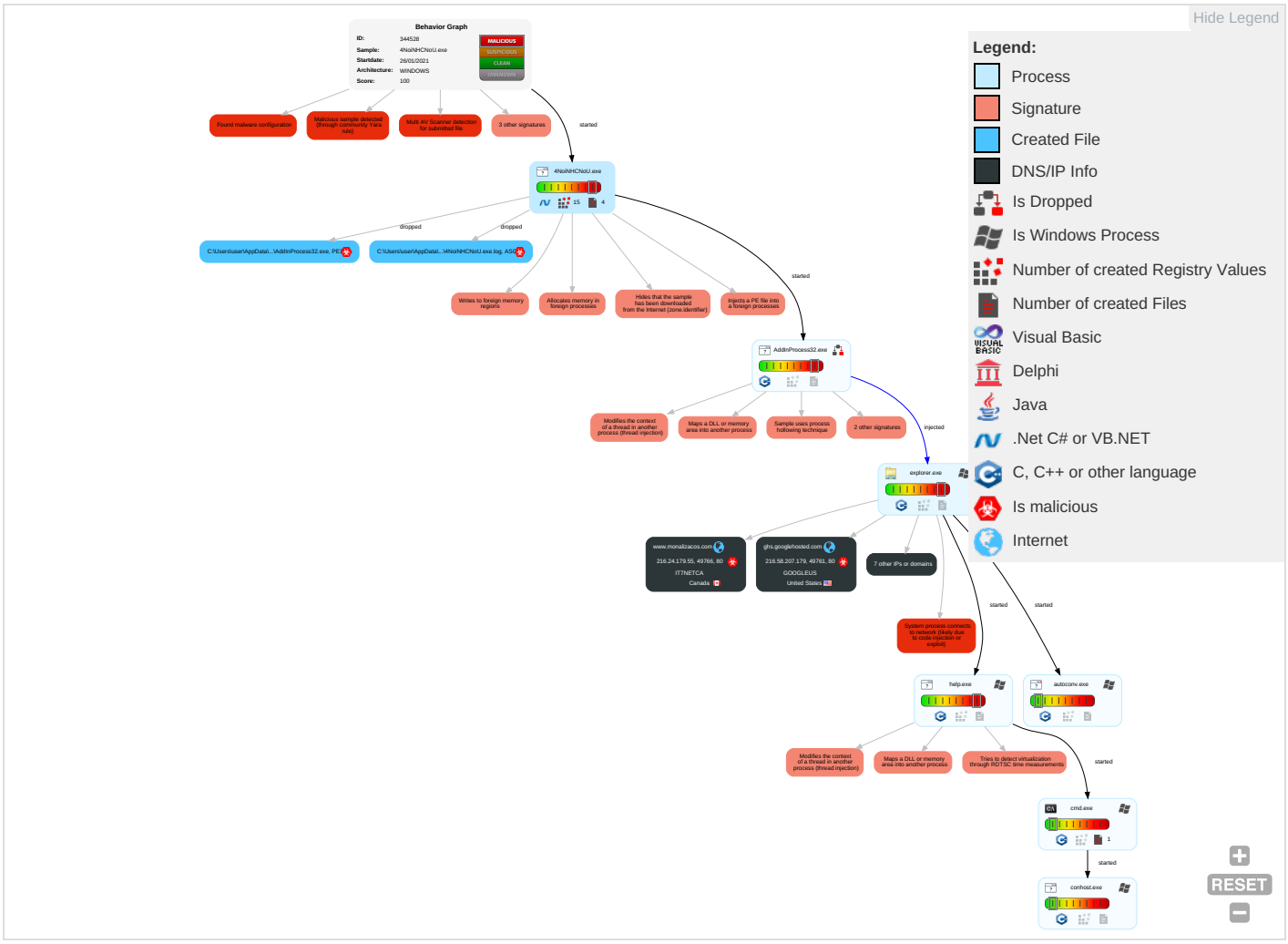
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts 1	Shared Modules 1	Valid Accounts 1	Valid Accounts 1	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Masquerading 1	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 8 1 2	Valid Accounts 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 3	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Disable or Modify Tools 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 8 1 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Deobfuscate/Decode Files or Information 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoco
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Obfuscated Files or Information 3	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Software Packing 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols

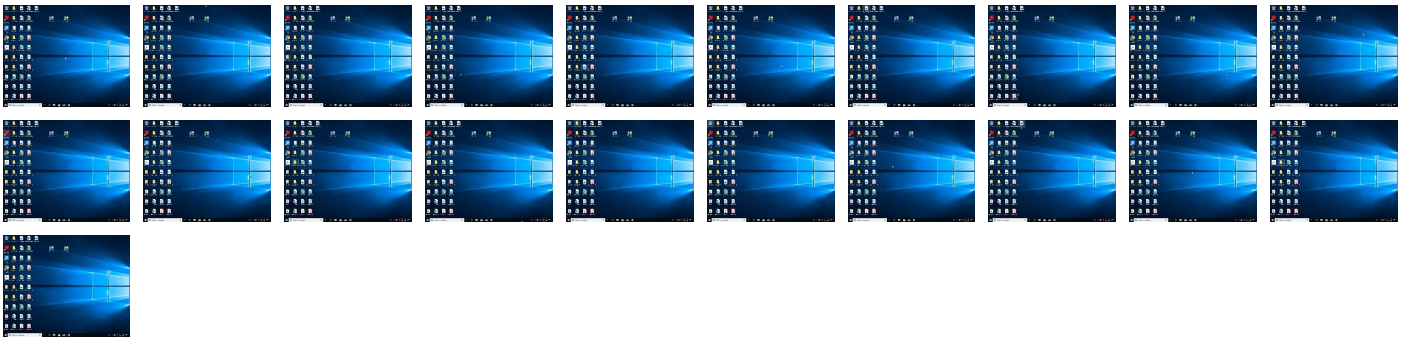
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
4NoiNHCNoU.exe	31%	Virustotal		Browse
4NoiNHCNoU.exe	32%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	
4NoiNHCNoU.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
2.2.AddInProcess32.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.monalizacos.com	0%	Virustotal		Browse
ghs.googlehosted.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://ns.adobe.cobj$	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://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://ns.adobe.c/g$	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://https://www.namebrightstatic.com/images/header_bg.png)	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.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://https://www.namebrightstatic.com/images/bg.png)	0%	Avira URL Cloud	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://https://www.namebrightstatic.com/images/site_maintenance.png)	0%	Avira URL Cloud	safe	
http://https://www.namebrightstatic.com/images/logo_off.gif)	0%	Avira URL Cloud	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://ns.ado/1$	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://ns.adb	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	

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.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://https://www.namebrightstatic.com/images/error_board.png)	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.monalizacos.com	216.24.179.55	true	true	• 0%, Virustotal, Browse	unknown
ghs.googlehosted.com	216.58.207.179	true	true	• 0%, Virustotal, Browse	unknown
nbparking-lb1-e8979d80a94bc16b.elb.us-east-1.amazonaws.com	3.234.181.234	true	false		high
www.artdonline.com	199.59.242.153	true	true		unknown
www.cookiefoo.com	unknown	unknown	true		unknown
www.milkandmemories.com	unknown	unknown	true		unknown
www.hull3dprints.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.cobj	4NoiNHCNoU.exe, 00000000.00000003.672814829.0000000008E81000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.cobj$	4NoiNHCNoU.exe, 00000000.00000003.659052889.0000000008E71000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers?	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0	4NoiNHCNoU.exe, 00000000.00000002.673545069.000000000328F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.adobe.c/g	4NoiNHCNoU.exe, 00000000.00000002.680921348.0000000008E82000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/WebPage	4NoiNHCNoU.exe, 00000000.00000002.673545069.000000000328F000.00000004.00000001.sdmp	false		high
http://statcounter.com/	help.exe, 00000006.00000002.1005440745.0000000003A8F000.00000004.00000001.sdmp	false		high
http://ns.adobe.c/g$	4NoiNHCNoU.exe, 00000000.00000003.659052889.0000000008E71000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.namebrightstatic.com/images/header_bg.png)	help.exe, 00000006.00000002.1005440745.0000000003A8F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.namebrightstatic.com/images/bg.png)	help.exe, 00000006.00000002.1005440745.0000000003A8F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false		high
http://c.statcounter.com/9484561/0/b0cbab70/1/	help.exe, 00000006.00000002.1005440745.0000000003A8F000.00000004.00000001.sdmp	false		high
http://ocsp.pki.goog/gts1o1core0	4NoiNHCNoU.exe, 00000000.00000002.673545069.000000000328F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.namebrightstatic.com/images/site_maintenance.png)	help.exe, 00000006.00000002.1005440745.0000000003A8F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.namebrightstatic.com/images/logo_off.gif)	help.exe, 00000006.00000002.1005440745.0000000003A8F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pki.goog/GTS1O1core.crl0	4NoiNHCNoU.exe, 00000000.00000002.673545069.000000000328F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.ado/1$	4NoiNHCNoU.exe, 00000000.00000003.659052889.0000000008E71000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adb	4NoiNHCNoU.exe, 00000000.00000003.672814829.0000000008E81000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000003.00000000.693818939.000000000B976000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	explorer.exe, 00000003.0000000 2.1005683210.0000000002B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	explorer.exe, 00000003.0000000 0.693818939.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000003.0000000 0.693818939.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000003.0000000 0.693818939.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000003.0000000 0.693818939.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	4NoiNHCNoU.exe, 00000000.00000 002.673522377.0000000003261000 .00000004.00000001.sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000003.0000000 0.693818939.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.ado/1	4NoiNHCNoU.exe, 00000000.00000 003.672814829.0000000008E81000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://www.namebrightstatic.com/images/error_board.png)	help.exe, 00000006.00000002.10 05440745.0000000003A8F000.0000 0004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.24.179.55	unknown	Canada		25820	IT7NETCA	true
199.59.242.153	unknown	United States		395082	BODIS-NJUS	true
216.58.207.179	unknown	United States		15169	GOOGLEUS	true
3.234.181.234	unknown	United States		14618	AMAZON-AESUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344528
Start date:	26.01.2021
Start time:	17:06:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4NoiNHCNoU.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:	20
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@8/2@5/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 11.5% (good quality ratio 10.1%) • Quality average: 71.3% • Quality standard deviation: 33%
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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 168.61.161.212, 172.217.23.36, 51.104.139.180, 95.101.22.216, 95.101.22.224, 23.55.110.161, 23.55.110.134, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, www.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.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
17:07:45	API Interceptor	1x Sleep call for process: 4NoiNHCNoU.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.59.242.153	mtsWWNDaNF.exe	Get hash	malicious	Browse	• www.traptlongview.com/csv8/?9r=9GN7fGOG/XNjrF88E5TxviJgjVB4/la6MjhQ3CZtrJBE6uvlYv2ahYgslVjOxon4Fjc0&w2=jFQp32IXi
	0iEsxw3D7A.exe	Get hash	malicious	Browse	• www.alwayadopt.com/8rg4/?6l=WsO1qizzdQOco4NPhHaDnsysS09xwMceuBioxc/BmkObRZ5eaS/j9hCi62iIB+iWgsUx&_FN4EJ=3fnDH

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FHT210995.exe	Get hash	malicious	Browse	• www.lvc.xyz/wpsb/?DxoLn=lzYwQ3KT7EiJU+03KAj/f46AYxUq3OFtotwkxvEGgl/73ySRAFXID91Rm9K4N5rAjQtd&Jtl=K6AhtzFPqrb
	5I7l3T5ZA5.exe	Get hash	malicious	Browse	• www.bigdudedesign.com/xle/?ndidgN=R2JdCb&JR-=p5BrHqV+x52+8/dkhIH/2RZzzPQHVqXKKEjnsmk8YSbLMdX3vj27OxdUa7tc0TzIhsDi0JEkXg==
	SKM_C221200706052800.exe	Get hash	malicious	Browse	• www.naturalhealthadvisery.com/s9zh/?aFNTkfLx=qOWGaJUZnCmstWLywjk1J1tsNforY2PNRnBf44673G+p7iqzfKfodzHj2/eLCWvbe38h&O2MtVN=iJEt_VihLTLX2JB0
	f4tP1FPuGN.exe	Get hash	malicious	Browse	• www.traptlongview.com/csv8/?4h0=9GN7fGOG/XNjrF88E5TxviJgjVB4/la6MjhQ3CZtrJBE6uvIYv2ahYgslWP0ypLDGU9liE66TA==&wR=LJEtMDJ
	New -PO January.xlsx	Get hash	malicious	Browse	• www.fallguysmovile.com/kgw/?y488D=Q8j3zo2KyRwXAD6KgUT3xIethN2qaDDEMDXD+QAzr+6/Eqg+bI2L4Bsu/fUoKKK2wv8fAQ==&_L34=kt84IRmHLXo
	74852.exe	Get hash	malicious	Browse	• www.pciappky.com/nf3n/?P6A=BWH4JYaT58lXsf+hwUDxH06dhaR/NFiLUxB8VjbVPAJsYgbKUu72S4XTqnjrUaFuA8KvggDN6w==&-ZS=W6O4IjSXA

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	in.exe	Get hash	malicious	Browse	• www.demenageseul.com/uds2/?Y4spQFW=nX62fi3FGck0KYkDLbl3wNFzysJuwQN4fQs5/MCF0tdU2wk9ctHDwkR8RP5qD5uls0RtT2NFRQ==&Ezu=VTChCL_ht2spUrl
	zHgm9k7WYU.exe	Get hash	malicious	Browse	• www.bigdudedesign.com/xle/?0V3lvN=YvRXzPexWxVddR&uXrpEpT=p5BrHqV+x52+8/dkhIH/2RZzzPQHVqXKKEjnsmk8YSbLMdX3vj27OxdUa7hcnD/L48D0
	65BV6gbGFl.exe	Get hash	malicious	Browse	• www.fallguysmovile.com/kgw/?tTrL=Fpgl&D81dO=Q8j3zo2PyWwTAT2GiUT3xlethN2qaDDEMDPTiTcyve6+EbM4cYnHuFUs864URq+F/upv
	PO85937758859777.xlsx	Get hash	malicious	Browse	• www.alwayadopt.com/8rg4/?RJ=WsO1qiz2dXOYooBDjHaDnsysS09xwMceuB64tfjAiEOaRoVYdCuvrl6g5TO0aeWlvtBBiA==&LFQHH=_pgx3Rd
	PO#218740.exe	Get hash	malicious	Browse	• www.shelvesthatsludge.com/wpsb/?Wxo=rpLKkbKOXOuXHBcSnbCAYX8flodJm2eBCOkizxG+Jmq98pcfRrdFVbp7k49Tb//P+n9l&vB=lhv8
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• www.laalianza.net/nki/?-Z1l=PROlUmUOyDGddH4liQ5hJmVkj46+Q85xpoxC45PqJl4e45Ope3SXSrB15gOtY6GR/pks5ou7bA==&5ju=UlSpo
	c6Rg7xug26.exe	Get hash	malicious	Browse	• www.fallguysmovile.com/kgw/?JfExsTlp=Q8j3zo2PyWwTAT2GiUT3xlethN2qaDDEMDPTiTcyve6+EbM4cYnHuFUs864+OaOF7shv&njnddr=RhlPiv

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IRS Notice Letter pdf document.exe	Get hash	malicious	Browse	• www.myaarpdentalpln.com/09rb/?Jt78=5Fl0Gne6++jCyaX7Drm8Xn32HTt8H/jqBsF3NSEqn1nDC6nrfbel4dCYEQQYkDcDl2++&pN9=EXX8_N6xKpqxS
	mQFXD5FxGT.exe	Get hash	malicious	Browse	• thevampire_vvv.byethost32.com/loglogin.html
	099898892.exe	Get hash	malicious	Browse	• www.fux.xyz/nt8e/?2dj=y/4CZD0u6UTnndZ84eN1F0ffB2o9AcFBv2a7yWGMbwZk5TncQjhg8LsZLtt2QtFrhXJ5&BR-LnJ=YVJpeDOX
	ZIPEXT#U007e1.EXE	Get hash	malicious	Browse	• ww1.survey-smiles.com/
	SAWR000148651.exe	Get hash	malicious	Browse	• www.phymath.science/6bu2/?u6u0=C0Tcv4PEDaSqiqbiBHmU4chmBJ2Ib35dQ7WAYQJ79jvi7RJiRJeSkc3aZR5iI925ug+e&9r4l2=xPJtQXiX
216.58.207.179	Payment _Arabian Parts Co BSC#U00a9.exe	Get hash	malicious	Browse	• www.bondstreet.management/oge8/?EZA0lp=Yfxnw+nso+OJBGuY8BdaIL8l7PpgKam5JRC37XhTlanNd1mD6p6qlcL2F05ShQ8JY0Vj&GzrLW=VDKPTvrxnd141V
	SecuriteInfo.com.Trojan.PackedNET.507.15470.exe	Get hash	malicious	Browse	• www.prayerswithmary.com/gqx2/?t6Al=njfRlhVhnDYToBqQ0FRdDD3+20pPuTSuw14qi8c71i/0kv2FA+P8Eg7R/AFYjoWjMB0l&kPm0q=J4kl
	Qs6ySVV95N.exe	Get hash	malicious	Browse	• www.nikolaichan.com/bw82/?9rN46F=xVJHBdo8&u4Td2=nYWM/rwSzX9MyPPoZtrUCAZuUhwRv7E+HNbrnomLB0MgbyAj2S+JrZFjkPtSeg4DEaosV+KRsQ==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IRS Notice Letter pdf document.exe	Get hash	malicious	Browse	• www.thebuzztraders.com/09rb/?Jt78=tK5SHJ/B9VkSEfSQE3soaE4uMhY2LrE6ZvvxVQcBFq9KYH6DfuOZHLVl1n1LVl7A3A7r&pN9=EXX8_N6xKpqxS
	3tTw14SBUw.exe	Get hash	malicious	Browse	• www.byronhobbs.com/3nk4/
	52Order Book PTA MACHINO (M) SDN BHD.xlsx.exe	Get hash	malicious	Browse	• www.beautyandthebesttravel.com/gh/
	26NEFT-PAYMENT.exe	Get hash	malicious	Browse	• www.lorelcraigcollaborative.com/ne/?xL0T0t=B0c9hitv+8rnNFPQQIKvZd0beMBibrTUEh8S1ZB3EHLuGXHfvUfU74cqdLWDbQExUnGw&1bd=Sn1lLTTHhv-tPRH

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
nbparking-lb1-e8979d80a94bc16b.elb.us-east-1.amazonaws.com	1D1PBttduH.exe	Get hash	malicious	Browse	• 3.234.181.234
	NXmokFkh3R.exe	Get hash	malicious	Browse	• 3.234.181.234
	mtq4WgX12m.exe	Get hash	malicious	Browse	• 3.234.181.234
	4F1V33O54M.exe	Get hash	malicious	Browse	• 3.234.181.234
	New Additional Agreement.exe	Get hash	malicious	Browse	• 3.234.181.234
	eBsxgyesfM.exe	Get hash	malicious	Browse	• 3.234.181.234
	ScanHP20.10.20.exe	Get hash	malicious	Browse	• 3.234.181.234
	Scan_Xerox10.18.2020.exe	Get hash	malicious	Browse	• 3.234.181.234
	Shipment doc, INV+BL.exe	Get hash	malicious	Browse	• 3.234.181.234
	Spare Parts Request MV Accord 8.13.20_pdf.exe	Get hash	malicious	Browse	• 3.234.181.234
	INVOICECRFV034.exe	Get hash	malicious	Browse	• 3.234.181.234
	130003150.exe	Get hash	malicious	Browse	• 3.234.181.234
	Revised BL.exe	Get hash	malicious	Browse	• 3.234.181.234
	script.exe.7582a080.0x0000000002360000-0x0000000002401fff.exe	Get hash	malicious	Browse	• 3.234.181.234
	VA_-_New_Wave_Club_Class-X_Box_(Sinners_Day_2011)-3CD-2011 (2).exe	Get hash	malicious	Browse	• 3.234.181.234
ghs.googlehosted.com	Payment _Arabian Parts Co BSC#U00a9.exe	Get hash	malicious	Browse	• 216.58.207.179
	SecuriteInfo.com.Trojan.PackedNET.507.15470.exe	Get hash	malicious	Browse	• 216.58.207.179
	Qs6ySVV95N.exe	Get hash	malicious	Browse	• 216.58.207.179
	0f9zzITIbk.exe	Get hash	malicious	Browse	• 172.217.22.243
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 142.250.180.83
	P4fZLHrU6d.exe	Get hash	malicious	Browse	• 172.217.168.19
	arrival_notice.xlsx	Get hash	malicious	Browse	• 172.217.168.19
	Draft FCR-HBL.exe	Get hash	malicious	Browse	• 172.217.168.83
	QN-03507-20.exe	Get hash	malicious	Browse	• 108.177.119.121
	3v3Aosgyxw.exe	Get hash	malicious	Browse	• 108.177.119.121
	20210111 Virginie.exe	Get hash	malicious	Browse	• 108.177.119.121
	81msxxUisn.exe	Get hash	malicious	Browse	• 108.177.119.121
	LOI.exe	Get hash	malicious	Browse	• 108.177.119.121
	Revise Order.exe	Get hash	malicious	Browse	• 108.177.119.121
	IRS Notice Letter pdf document.exe	Get hash	malicious	Browse	• 216.58.207.179
	PO21010699XYJ.exe	Get hash	malicious	Browse	• 216.58.198.51
	current productlist.exe	Get hash	malicious	Browse	• 216.58.198.51

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://da930.infusion-links.com/api/v1/click/5782635710906368/4861645707411456	Get hash	malicious	Browse	• 172.217.168.83
	Rfq 214871_TAWI Catalog.exe	Get hash	malicious	Browse	• 172.217.168.83
	Copy111.exe	Get hash	malicious	Browse	• 172.217.168.83

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
IT7NETCA	Rfq 214871_TAWI Catalog.exe	Get hash	malicious	Browse	• 64.64.251.229
	utox.exe	Get hash	malicious	Browse	• 176.122.158.102
	0dJ67KOYIS.exe	Get hash	malicious	Browse	• 23.105.200.208
	v7tCVYRqnH.exe	Get hash	malicious	Browse	• 23.105.200.208
	COMMERCIAL INVOICE, BILL OF LADING, DOC.exe	Get hash	malicious	Browse	• 74.120.168.133
	M36vYI4j67.exe	Get hash	malicious	Browse	• 97.64.22.226
	fFH9LTYQsa.exe	Get hash	malicious	Browse	• 97.64.22.226
	derApTVcOg.exe	Get hash	malicious	Browse	• 97.64.22.226
	dkKLT12ieu.exe	Get hash	malicious	Browse	• 97.64.22.226
	PO_08102020EX.doc	Get hash	malicious	Browse	• 144.34.218.189
	purchase order.exe	Get hash	malicious	Browse	• 67.218.128.107
BODIS-NJUS	mtsWWNDaNF.exe	Get hash	malicious	Browse	• 199.59.242.153
	0iEsxw3D7A.exe	Get hash	malicious	Browse	• 199.59.242.153
	FHT210995.exe	Get hash	malicious	Browse	• 199.59.242.153
	5I7l3T5ZA5.exe	Get hash	malicious	Browse	• 199.59.242.153
	SKM_C221200706052800.exe	Get hash	malicious	Browse	• 199.59.242.153
	f4tP1FPuGN.exe	Get hash	malicious	Browse	• 199.59.242.153
	New -PO January.xlsx	Get hash	malicious	Browse	• 199.59.242.153
	74852.exe	Get hash	malicious	Browse	• 199.59.242.153
	in.exe	Get hash	malicious	Browse	• 199.59.242.153
	zHgm9k7WYU.exe	Get hash	malicious	Browse	• 199.59.242.153
	65BV6gbGFl.exe	Get hash	malicious	Browse	• 199.59.242.153
	PO85937758859777.xlsx	Get hash	malicious	Browse	• 199.59.242.153
	PO#218740.exe	Get hash	malicious	Browse	• 199.59.242.153
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• 199.59.242.153
	c6Rg7xug26.exe	Get hash	malicious	Browse	• 199.59.242.153
	sample20210111-01.xlsm	Get hash	malicious	Browse	• 199.59.242.150
	IRS Notice Letter pdf document.exe	Get hash	malicious	Browse	• 199.59.242.153
	mQFXD5FxGT.exe	Get hash	malicious	Browse	• 199.59.242.153
	099898892.exe	Get hash	malicious	Browse	• 199.59.242.153
	ZIPEXT#U007e1.EXE	Get hash	malicious	Browse	• 199.59.242.153
AMAZON-AESUS	win32.exe	Get hash	malicious	Browse	• 52.44.229.95
	order pdf.exe	Get hash	malicious	Browse	• 3.223.115.185
	SecuriteInfo.com.Variant.Zusy.363976.7571.exe	Get hash	malicious	Browse	• 23.21.126.66
	Shipping Documents.doc	Get hash	malicious	Browse	• 54.235.83.248
	gPGTcEMoM1.exe	Get hash	malicious	Browse	• 52.23.148.124
	vA0mtZ7JzJ.exe	Get hash	malicious	Browse	• 3.223.115.185
	8Aobnx1VRi.exe	Get hash	malicious	Browse	• 23.21.76.253
	RFQ-Strip Casting Line.exe	Get hash	malicious	Browse	• 54.235.142.93
	INGNhYonmgtGZ9Updf.exe	Get hash	malicious	Browse	• 3.223.115.185
	NEW ORDER PO 20200909.exe	Get hash	malicious	Browse	• 23.21.252.4
	bin.sh	Get hash	malicious	Browse	• 18.210.13.68
	file.exe	Get hash	malicious	Browse	• 54.225.220.115
	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	• 54.158.2.202
	file.exe	Get hash	malicious	Browse	• 54.225.242.59
	SecuriteInfo.com.Variant.MSILPerseus.224695.13350.exe	Get hash	malicious	Browse	• 23.21.252.4
	1_25_2021 11_20_30 a.m., [Payment 457 CMSupportDev].html	Get hash	malicious	Browse	• 3.218.111.133
	Dropper.xlsm	Get hash	malicious	Browse	• 3.220.8.221
	IDA Pro 7.0 2017 Incl. Hex-Rays Decompilers (LEAKED) [Ny2rogen].exe	Get hash	malicious	Browse	• 54.235.147.252
	recteq_v1.6.3_apkpure.com.apk	Get hash	malicious	Browse	• 34.225.41.153
	recteq_v1.6.3_apkpure.com.apk	Get hash	malicious	Browse	• 54.225.115.255
GOOGLEUS	bXFjrxjRlb.exe	Get hash	malicious	Browse	• 34.102.136.180
	xl2Ml2iNJe.exe	Get hash	malicious	Browse	• 34.102.136.180
	eEXZHxdxFE.exe	Get hash	malicious	Browse	• 35.228.108.144

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	SoPwZKv1Mf.exe	Get hash	malicious	Browse	
	bXFjrxjRlb.exe	Get hash	malicious	Browse	
	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	
	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	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\4NoiNHCNoU.exe.log

Process:	C:\Users\user\Desktop\4NoiNHCNoU.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1873
Entropy (8bit):	5.355036985457214
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjovitHoxHhAHKzvr1qHj:iqXeqm00YqhQnouRqjoKtIxHeqzTwD
MD5:	CDA95282F22F47DA2FDDC9E912B67FEF
SHA1:	67A40582A092B5DF40C3EB61A361A2D336FC69E0
SHA-256:	179E50F31095D0CFA13DCBB9CED6DEE424DFE8CEF8E05BDE1F840273F45E5F49
SHA-512:	1D151D92AE982D2149C2255826C2FFB89A475A1EB9B9FE93DC3706F3016CD6B309743B36A4D7F6D68F48CE25391FDA7A2BAE42061535EEA7862460424A3A2036
Malicious:	**true**

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\4NoiNHCNoU.exe.log	
Reputation:	moderate, very likely benign file
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\4NoiNHCNoU.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%
Joe Sandbox View:	• Filename: SoPwZKv1Mf.exe, Detection: malicious, Browse • Filename: bXFjrxjRlb.exe, Detection: malicious, Browse • 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
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):	5.619586569577208
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:	4NoiNHCNoU.exe
File size:	770560
MD5:	204e0bf841b9900fa03d6dff302857f3
SHA1:	a3b3152dbea14ed71a5e226a123433dfc3ecb60a

General	
SHA256:	2ba9185ecb7b43e54242e560724993fbf5e24c3e1acd57 89ac9dc305e934045
SHA512:	edaae04e2cb167fdb6a07c83994b48cbcd9b084ceecc5f2 558b5f1ce499272364ffc4ed572b171e21b204c5c05846e 42e983297c24943b669c9f7705deb80de3
SSDEEP:	12288:LyooVOHfNbxp8pay/ORjp1C0kCeVxxQqR:Lyoo V2/8SR1Y/h
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......PE..L... Y....................v...J........... ....@.. ....`................................

File Icon

	
Icon Hash:	aaacae8e96a2c0e6

Static PE Info

General	
Entrypoint:	0x4b942e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x7F00759 [Fri Mar 22 07:57:13 1974 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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb93e0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xba000	0x46f2	.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	
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	0xb7434	0xb7600	False	0.557991969155	data	5.60539545404	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xba000	0x46f2	0x4800	False	0.154242621528	data	2.48702752708	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc0000	0xc	0x200	False	0.044921875	data	0.101910425663	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	0x39c	data		
RT_MANIFEST	0xbe508	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

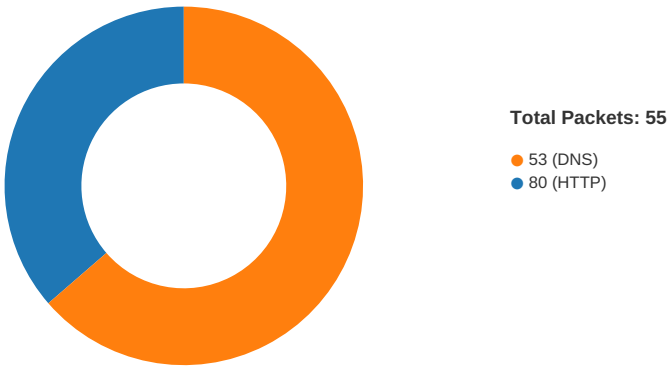
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2005 4;@:9>CF>>5?A@<AE4D4
Assembly Version	1.0.0.0
InternalName	IMG_43016.exe
FileVersion	5.8.10.13
CompanyName	4;@:9>CF>>5?A@<AE4D4

Description	Data
Comments	A7E@4HA4?@7HB;B98GH
ProductName	56:53B29963AH9:F76>A
ProductVersion	5.8.10.13
FileDescription	56:53B29963AH9:F76>A
OriginalFilename	IMG_43016.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 17:08:48.645308018 CET	49761	80	192.168.2.4	216.58.207.179
Jan 26, 2021 17:08:48.687963963 CET	80	49761	216.58.207.179	192.168.2.4
Jan 26, 2021 17:08:48.688122034 CET	49761	80	192.168.2.4	216.58.207.179
Jan 26, 2021 17:08:48.688277960 CET	49761	80	192.168.2.4	216.58.207.179
Jan 26, 2021 17:08:48.730931044 CET	80	49761	216.58.207.179	192.168.2.4
Jan 26, 2021 17:08:48.747661114 CET	80	49761	216.58.207.179	192.168.2.4
Jan 26, 2021 17:08:48.747905016 CET	49761	80	192.168.2.4	216.58.207.179
Jan 26, 2021 17:08:48.748102903 CET	80	49761	216.58.207.179	192.168.2.4
Jan 26, 2021 17:08:48.750555992 CET	49761	80	192.168.2.4	216.58.207.179
Jan 26, 2021 17:08:48.790555954 CET	80	49761	216.58.207.179	192.168.2.4
Jan 26, 2021 17:09:29.897218943 CET	49764	80	192.168.2.4	199.59.242.153
Jan 26, 2021 17:09:30.020919085 CET	80	49764	199.59.242.153	192.168.2.4
Jan 26, 2021 17:09:30.021130085 CET	49764	80	192.168.2.4	199.59.242.153
Jan 26, 2021 17:09:30.021341085 CET	49764	80	192.168.2.4	199.59.242.153
Jan 26, 2021 17:09:30.144951105 CET	80	49764	199.59.242.153	192.168.2.4
Jan 26, 2021 17:09:30.147169113 CET	80	49764	199.59.242.153	192.168.2.4
Jan 26, 2021 17:09:30.147202969 CET	80	49764	199.59.242.153	192.168.2.4
Jan 26, 2021 17:09:30.147219896 CET	80	49764	199.59.242.153	192.168.2.4
Jan 26, 2021 17:09:30.147231102 CET	80	49764	199.59.242.153	192.168.2.4
Jan 26, 2021 17:09:30.147243023 CET	80	49764	199.59.242.153	192.168.2.4
Jan 26, 2021 17:09:30.147464037 CET	49764	80	192.168.2.4	199.59.242.153
Jan 26, 2021 17:09:30.147546053 CET	49764	80	192.168.2.4	199.59.242.153
Jan 26, 2021 17:09:53.305131912 CET	49765	80	192.168.2.4	3.234.181.234
Jan 26, 2021 17:09:53.431636095 CET	80	49765	3.234.181.234	192.168.2.4
Jan 26, 2021 17:09:53.431780100 CET	49765	80	192.168.2.4	3.234.181.234
Jan 26, 2021 17:09:53.431937933 CET	49765	80	192.168.2.4	3.234.181.234
Jan 26, 2021 17:09:53.559004068 CET	80	49765	3.234.181.234	192.168.2.4
Jan 26, 2021 17:09:53.559031963 CET	80	49765	3.234.181.234	192.168.2.4
Jan 26, 2021 17:09:53.559053898 CET	80	49765	3.234.181.234	192.168.2.4
Jan 26, 2021 17:09:53.559077024 CET	80	49765	3.234.181.234	192.168.2.4
Jan 26, 2021 17:09:53.559540033 CET	49765	80	192.168.2.4	3.234.181.234

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 17:09:53.559623003 CET	49765	80	192.168.2.4	3.234.181.234
Jan 26, 2021 17:09:53.685353994 CET	80	49765	3.234.181.234	192.168.2.4
Jan 26, 2021 17:10:13.988073111 CET	49766	80	192.168.2.4	216.24.179.55
Jan 26, 2021 17:10:14.173216105 CET	80	49766	216.24.179.55	192.168.2.4
Jan 26, 2021 17:10:14.173377037 CET	49766	80	192.168.2.4	216.24.179.55
Jan 26, 2021 17:10:14.173506021 CET	49766	80	192.168.2.4	216.24.179.55
Jan 26, 2021 17:10:14.359297991 CET	80	49766	216.24.179.55	192.168.2.4
Jan 26, 2021 17:10:14.359316111 CET	80	49766	216.24.179.55	192.168.2.4
Jan 26, 2021 17:10:14.359328985 CET	80	49766	216.24.179.55	192.168.2.4
Jan 26, 2021 17:10:14.359504938 CET	49766	80	192.168.2.4	216.24.179.55
Jan 26, 2021 17:10:14.359603882 CET	49766	80	192.168.2.4	216.24.179.55
Jan 26, 2021 17:10:14.547630072 CET	80	49766	216.24.179.55	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 17:07:31.394352913 CET	55854	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:07:31.442203045 CET	53	55854	8.8.8.8	192.168.2.4
Jan 26, 2021 17:07:32.286022902 CET	64549	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:07:32.342454910 CET	53	64549	8.8.8.8	192.168.2.4
Jan 26, 2021 17:07:33.203152895 CET	63153	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:07:33.251071930 CET	53	63153	8.8.8.8	192.168.2.4
Jan 26, 2021 17:07:34.250425100 CET	52991	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:07:34.306971073 CET	53	52991	8.8.8.8	192.168.2.4
Jan 26, 2021 17:07:37.835402012 CET	53700	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:07:37.892190933 CET	53	53700	8.8.8.8	192.168.2.4
Jan 26, 2021 17:07:39.025571108 CET	51726	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:07:39.073363066 CET	53	51726	8.8.8.8	192.168.2.4
Jan 26, 2021 17:07:40.548142910 CET	56794	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:07:40.606688023 CET	53	56794	8.8.8.8	192.168.2.4
Jan 26, 2021 17:07:41.933109999 CET	56534	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:07:41.989626884 CET	53	56534	8.8.8.8	192.168.2.4
Jan 26, 2021 17:07:43.245419025 CET	56627	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:07:43.296118975 CET	53	56627	8.8.8.8	192.168.2.4
Jan 26, 2021 17:07:44.217037916 CET	56621	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:07:44.267735004 CET	53	56621	8.8.8.8	192.168.2.4
Jan 26, 2021 17:07:45.158593893 CET	63116	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:07:45.208209038 CET	53	63116	8.8.8.8	192.168.2.4
Jan 26, 2021 17:07:46.156187057 CET	64078	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:07:46.209414005 CET	53	64078	8.8.8.8	192.168.2.4
Jan 26, 2021 17:07:48.044967890 CET	64801	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:07:48.101473093 CET	53	64801	8.8.8.8	192.168.2.4
Jan 26, 2021 17:07:59.689146042 CET	61721	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:07:59.737143040 CET	53	61721	8.8.8.8	192.168.2.4
Jan 26, 2021 17:08:12.337807894 CET	51255	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:08:12.398538113 CET	53	51255	8.8.8.8	192.168.2.4
Jan 26, 2021 17:08:20.700083017 CET	61522	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:08:20.760898113 CET	53	61522	8.8.8.8	192.168.2.4
Jan 26, 2021 17:08:28.058864117 CET	52337	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:08:28.115331888 CET	53	52337	8.8.8.8	192.168.2.4
Jan 26, 2021 17:08:28.916161060 CET	55046	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:08:28.972858906 CET	53	55046	8.8.8.8	192.168.2.4
Jan 26, 2021 17:08:29.858624935 CET	49612	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:08:29.914983034 CET	53	49612	8.8.8.8	192.168.2.4
Jan 26, 2021 17:08:30.348535061 CET	49285	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:08:30.404861927 CET	53	49285	8.8.8.8	192.168.2.4
Jan 26, 2021 17:08:30.866511106 CET	50601	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:08:30.925765038 CET	53	50601	8.8.8.8	192.168.2.4
Jan 26, 2021 17:08:31.452265024 CET	60875	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:08:31.511481047 CET	53	60875	8.8.8.8	192.168.2.4
Jan 26, 2021 17:08:31.663589954 CET	56448	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:08:31.737837076 CET	53	56448	8.8.8.8	192.168.2.4
Jan 26, 2021 17:08:32.115817070 CET	59172	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:08:32.177277088 CET	53	59172	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 17:08:33.000488043 CET	62420	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:08:33.061288118 CET	53	62420	8.8.8.8	192.168.2.4
Jan 26, 2021 17:08:34.165752888 CET	60579	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:08:34.222181082 CET	53	60579	8.8.8.8	192.168.2.4
Jan 26, 2021 17:08:34.715773106 CET	50183	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:08:34.772411108 CET	53	50183	8.8.8.8	192.168.2.4
Jan 26, 2021 17:08:37.264513016 CET	61531	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:08:37.325027943 CET	53	61531	8.8.8.8	192.168.2.4
Jan 26, 2021 17:08:48.502526045 CET	49228	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:08:48.636364937 CET	53	49228	8.8.8.8	192.168.2.4
Jan 26, 2021 17:09:09.497134924 CET	59794	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:09:09.572475910 CET	53	59794	8.8.8.8	192.168.2.4
Jan 26, 2021 17:09:16.022726059 CET	55916	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:09:16.070733070 CET	53	55916	8.8.8.8	192.168.2.4
Jan 26, 2021 17:09:18.174031973 CET	52752	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:09:18.241321087 CET	53	52752	8.8.8.8	192.168.2.4
Jan 26, 2021 17:09:29.752019882 CET	60542	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:09:29.895988941 CET	53	60542	8.8.8.8	192.168.2.4
Jan 26, 2021 17:09:53.156522989 CET	60689	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:09:53.303366899 CET	53	60689	8.8.8.8	192.168.2.4
Jan 26, 2021 17:10:13.778407097 CET	64206	53	192.168.2.4	8.8.8.8
Jan 26, 2021 17:10:13.987082958 CET	53	64206	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2021 17:08:48.502526045 CET	192.168.2.4	8.8.8.8	0x3c82	Standard query (0)	www.hull3dprints.com	A (IP address)	IN (0x0001)
Jan 26, 2021 17:09:09.497134924 CET	192.168.2.4	8.8.8.8	0x737e	Standard query (0)	www.cookiefoo.com	A (IP address)	IN (0x0001)
Jan 26, 2021 17:09:29.752019882 CET	192.168.2.4	8.8.8.8	0xa910	Standard query (0)	www.artdonline.com	A (IP address)	IN (0x0001)
Jan 26, 2021 17:09:53.156522989 CET	192.168.2.4	8.8.8.8	0xe9fc	Standard query (0)	www.milkandmemories.com	A (IP address)	IN (0x0001)
Jan 26, 2021 17:10:13.778407097 CET	192.168.2.4	8.8.8.8	0xd548	Standard query (0)	www.monalizacos.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 17:08:48.636364937 CET	8.8.8.8	192.168.2.4	0x3c82	No error (0)	www.hull3dprints.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 17:08:48.636364937 CET	8.8.8.8	192.168.2.4	0x3c82	No error (0)	ghs.googlehosted.com		216.58.207.179	A (IP address)	IN (0x0001)
Jan 26, 2021 17:09:09.572475910 CET	8.8.8.8	192.168.2.4	0x737e	Name error (3)	www.cookiefoo.com	none	none	A (IP address)	IN (0x0001)
Jan 26, 2021 17:09:29.895988941 CET	8.8.8.8	192.168.2.4	0xa910	No error (0)	www.artdonline.com		199.59.242.153	A (IP address)	IN (0x0001)
Jan 26, 2021 17:09:53.303366899 CET	8.8.8.8	192.168.2.4	0xe9fc	No error (0)	www.milkandmemories.com	comingsoon.namebright.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 17:09:53.303366899 CET	8.8.8.8	192.168.2.4	0xe9fc	No error (0)	comingsoon.namebright.com	nbparking-lb1-e8979d80a94bc16b.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2021 17:09:53.303366899 CET	8.8.8.8	192.168.2.4	0xe9fc	No error (0)	nbparking-lb1-e8979d80a94bc16b.elb.us-east-1.amazonaws.com		3.234.181.234	A (IP address)	IN (0x0001)
Jan 26, 2021 17:10:13.987082958 CET	8.8.8.8	192.168.2.4	0xd548	No error (0)	www.monalizacos.com		216.24.179.55	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.hull3dprints.com
- www.artdonline.com
- www.milkandmemories.com
- www.monalizacos.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49761	216.58.207.179	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 17:08:48.688277960 CET	4798	OUT	GET /wdva/?CTvp=fvUh_lYhi2Qtqn&YP7HsZXp=dtwHAOGjt/+zpbp36VfwrlpLqx9PqTyEssCs5akk3XqA2N3Rg4iBrIryvB1IVPRuISQ2 HTTP/1.1 Host: www.hull3dprints.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 26, 2021 17:08:48.747661114 CET	4799	IN	HTTP/1.1 301 Moved Permanently Location: https://www.etsy.com/shop/Hull3DPrints Date: Tue, 26 Jan 2021 16:08:48 GMT Content-Type: text/html; charset=UTF-8 Server: ghs Content-Length: 235 X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN Connection: close Data Raw: 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 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 3c 54 49 54 4c 45 3e 33 30 31 20 4d 6f 76 65 64 3c 2f 54 49 54 4c 45 3e 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 33 30 31 20 4d 6f 76 65 64 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 0a 3c 41 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 65 74 73 79 2e 63 6f 6d 2f 73 68 6f 70 2f 48 75 6c 6c 33 44 50 72 69 6e 74 73 22 3e 68 65 72 65 3c 2f 41 3e 2e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8"><TITLE>301 Moved</TITLE></HEAD><BODY><H1>301 Moved</H1>The document has moved<A HREF="https://www.etsy.com/shop/Hull3DPrints">here</A>.</BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49764	199.59.242.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 17:09:30.021341085 CET	4837	OUT	GET /wdva/?CTvp=fvUh_lYhi2Qtqn&YP7HsZXp=xHc9ODtVxj0eUWmi3yu1PHJO+9FS2s4H+8Xc5Nf8URN5DAD0y+vEo6QceVJID6bTGhq7 HTTP/1.1 Host: www.artdonline.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 17:09:30.147169113 CET	4838	IN	HTTP/1.1 200 OK Server: openresty Date: Tue, 26 Jan 2021 16:09:30 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oY OeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_rOHYb9Z6Wy9T1+v+/2OiI1DBd5wjCInqR5Zn 6XhVNf2Hb9ATyIElVxP9iU+iEhAeHIpde7JKlMccR/geMyf+aw== Data Raw: 65 65 34 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 44 72 70 32 6c 7a 37 41 4f 6d 41 44 61 4e 38 74 41 35 30 4c 73 57 63 6a 4c 46 79 51 46 63 62 2f 50 32 54 78 63 35 38 6f 59 4f 65 49 4c 62 33 76 42 77 37 4a 36 66 34 70 61 6d 6b 41 51 56 53 51 75 71 59 73 4b 78 33 59 7a 64 55 48 43 76 62 56 5a 76 46 55 73 43 41 77 45 41 41 51 3d 3d 5f 72 4f 48 59 62 39 5a 36 57 79 39 54 31 2b 76 2b 2f 32 4f 69 49 31 44 42 64 35 77 6a 43 49 6e 71 52 35 5a 6e 36 58 68 56 4e 66 32 48 62 39 41 54 79 49 45 6c 56 78 50 39 69 55 2b 69 45 68 41 65 48 49 70 64 65 37 4a 4b 6c 4d 63 63 52 2f 67 65 4d 79 66 2b 61 77 3d 3d 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 3c 74 69 74 6c 65 3e 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 53 65 65 20 72 65 6c 61 74 65 64 20 6c 69 6e 6b 73 20 74 6f 20 77 68 61 74 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 2e 22 2f 3e 3c 2f 68 65 61 64 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 36 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 36 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 37 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 37 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 38 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 38 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 39 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 39 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 28 67 74 20 49 45 20 39 29 7c 21 28 49 45 29 5d 3e 20 2d 2d 3e 3c 62 6f 64 79 3e 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 67 5f 70 62 3d 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 0a 44 54 3d 64 6f 63 75 6d 65 6e 74 2c 61 7a 78 3d 6c 6f 63 61 74 69 6f 6e 2c 44 44 3d 44 54 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 2c 61 41 43 3d 66 61 6c 73 65 2c 4c 55 3b 44 44 2e 64 65 66 65 72 3d 74 72 75 65 3b 44 44 2e 61 73 79 6e 63 3d 74 72 75 65 3b 44 44 2e 73 72 63 3d 22 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 61 64 73 65 6e 73 65 2f 64 6f 6d 61 69 6e 73 2f 63 61 66 2e 6a 73 22 3b 44 44 2e 6f 6e 65 Data Ascii: ee4<!DOCTYPE html><html data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp 2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ= =_rOHYb9Z6Wy9T1+v+/2OiI1DBd5wjCInqR5Zn6XhVNf2Hb9ATyIElVxP9iU+iEhAeHIpde7JKlMccR/geMyf+aw==><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8"><title></title><meta name="viewport" content= "width=device-width, initial-scale=1"><meta name="description" content="See related links to what you are looking for."/> </head>...[if IE 6]><body class="ie6"><![endif]-->...[if IE 7]><body class="ie7"><![endif]-->...[if IE 8]><body class="ie8"><! [endif]-->...[if IE 9]><body class="ie9"><![endif]-->...[if (gt IE 9)|!(IE)]> --><body>...<![endif]--><script type="text/javascri pt">g_pb=(function(){varDT=document,azx=location,DD=DT.createElement('script'),aAC=false,LU;DD.defer=true;DD.a sync=true;DD.src="//www.google.com/adsense/domains/caf.js";DD.one

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49765	3.234.181.234	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 17:09:53.431937933 CET	4843	OUT	GET /wdva/?YP7HsZXp=aeYSUm77/4pN8ZT/uXkxszyZjPiqX70cnyvz0SpaHLBaMQqGqlwCHFzYALKMdCUG+bHZ&C Tvp=fvUh_lYhi2Qtqn HTTP/1.1 Host: www.milkandmemories.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 17:09:53.559004068 CET	4844	IN	HTTP/1.1 200 OK Cache-Control: private Content-Type: text/html; charset=utf-8 Server: Microsoft-IIS/8.5 X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET Date: Tue, 26 Jan 2021 16:08:59 GMT Connection: close Content-Length: 5044 Data Raw: 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 74 72 61 6e 73 69 74 69 6f 6e 61 6c 2e 64 74 64 22 3e 0d 0a 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 0d 0a 0d 0a 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 20 2f 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 4e 61 6d 65 42 72 69 67 68 74 20 2d 20 43 6f 6d 69 6e 67 20 53 6f 6f 6e 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 64 38 64 38 64 38 20 75 72 6c 28 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6e 61 6d 65 62 72 69 67 68 74 73 74 61 74 69 63 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 67 2e 70 6e 67 29 20 74 6f 70 20 72 65 70 65 61 74 2d 78 3b 7d 0d 0a 20 20 20 20 20 20 20 20 2e 70 61 67 65 42 72 6f 77 73 65 72 45 72 72 6f 72 7b 6d 69 6e 2d 68 65 69 67 68 74 3a 20 36 30 30 70 78 3b 7d 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 7b 6d 61 72 67 69 6e 3a 20 30 20 61 75 74 6f 3b 77 69 64 74 68 3a 20 39 32 32 70 78 3b 7d 0d 0a 20 20 20 20 20 20 20 20 2e 73 68 61 64 6f 77 5f 6c 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 31 30 70 78 3b 7d 0d 0a 20 20 20 20 20 20 20 20 2f 2a 2e 73 68 61 64 6f 77 5f 72 7b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 31 30 70 78 3b 7d 2a 2f 0d 0a 20 20 20 20 20 20 20 20 2e 6d 61 69 6e 5f 62 67 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 66 66 66 3b 7d 0d 0a 20 20 20 20 20 20 20 20 23 68 65 61 64 65 72 7b 70 61 64 64 69 6e 67 3a 20 30 20 32 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 66 66 66 3b 7d 0d 0a 20 20 20 20 20 20 20 20 23 68 65 61 64 65 72 2e 68 65 61 64 65 72 53 68 6f 72 74 7b 68 65 69 67 68 74 3a 20 36 35 70 78 3b 7d 0d 0a 20 20 20 20 20 20 20 20 23 68 65 61 64 65 72 20 2e 68 65 61 64 65 72 5f 69 6e 7b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 20 31 34 70 78 3b 68 65 69 67 68 74 3a 20 31 34 35 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 20 68 69 64 64 65 6e 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 20 75 72 6c 28 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6e 61 6d 65 62 72 69 67 68 74 73 74 61 74 69 63 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 68 65 61 64 65 72 5f 62 67 2e 70 6e 67 29 20 74 6f 70 20 72 65 70 65 61 74 2d 78 3b 7d 0d 0a 20 20 20 20 20 20 20 20 23 68 65 61 64 65 72 20 2e 68 65 61 64 65 72 5f 74 6f 70 7b 68 65 69 67 68 74 3a 20 36 35 70 78 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 7d 0d 0a 20 20 20 20 20 20 20 20 23 6c 6f 67 6f 20 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 20 75 72 6c 28 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6e 61 6d 65 62 72 69 67 68 74 73 74 61 74 69 63 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 6c 6f 67 6f 5f 6f 66 66 2e 67 69 66 29 20 6e 6f 2d 72 65 70 65 61 74 3b 77 69 64 74 68 3a 20 32 32 35 70 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><title></title> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <title>NameBright - Coming Soon</title> <style type="text/css"> body{background: #d8d8d8 url(https://www.namebrightstatic.com/images/bg.png) top repeat-x;} .pageBrowserError{ min-height: 600px;} .container{margin: 0 auto;width: 922px;} .shadow_l{margin-left: 10px;} /*.shadow_r{margin-right: 10px;}*/ .main_bg{background: #fff;} #header{padding: 0 2px;background: #fff;} #header.headerShort{height: 65px;} #header .header_in{padding-right: 14px;height: 145px;overflow: hidden;background: url(https://www.namebrightstatic.com/images/header_bg.png) top repeat-x;} #header .header_top{height: 65px;overflow:hidden} #logo {background: url(https://www.namebrightstatic.com/images/logo_off.gif) no-repeat;width: 225p

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49766	216.24.179.55	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2021 17:10:14.173506021 CET	4849	OUT	GET /wdva/?CTvp=fvUh_lYhi2Qtqn&YP7HsZXp=hK2+H65jJ6ehVdA52W/5RiHO6KAeaXXnYMVt3i9x6BH/1kcuoogx/NrTS0USn7suDUfO HTTP/1.1 Host: www.monalizacos.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 26, 2021 17:10:14.359316111 CET	4849	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 26 Jan 2021 16:10:14 GMT Content-Type: text/html Content-Length: 162 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body bgcolor="white"> 404 Not Found <hr> nginx </body></html>

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

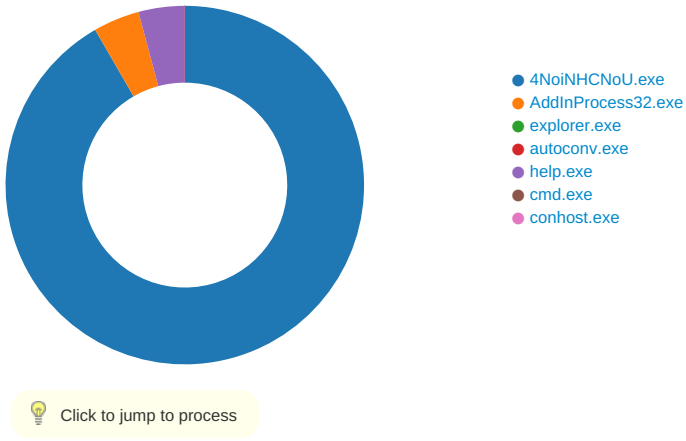
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xEA
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xEA
GetMessageW	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xEA
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xEA

Statistics

Behavior



System Behavior

Analysis Process: 4NoiNHCNoU.exe PID: 6340 Parent PID: 5884

General

Start time:	17:07:36
Start date:	26/01/2021
Path:	C:\Users\user\Desktop\4NoiNHCNoU.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\4NoiNHCNoU.exe'
Imagebase:	0xd20000
File size:	770560 bytes
MD5 hash:	204E0BF841B9900FA03D6DFF302857F3
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: 00000000.00000002.678246488.0000000004BB9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.678246488.0000000004BB9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.678246488.0000000004BB9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.678514440.0000000004D25000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.678514440.0000000004D25000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.678514440.0000000004D25000.00000004.00000001.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	6D38CF06	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	6D38CF06	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	314E11B	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\4NoiNHCNoU.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

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 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	314E11B	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\4NoiNHCNoU.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	6D69C907	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5a e0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationC ore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\d d5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8 c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	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: 6436 Parent PID: 6340

General

Start time:	17:07:42
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:	0xfa0000
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: 00000002.00000002.708829602.0000000001510000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.708829602.0000000001510000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.708829602.0000000001510000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.708860418.0000000001540000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.708860418.0000000001540000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.708860418.0000000001540000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.708551129.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.708551129.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.708551129.0000000000400000.00000040.00000001.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	41A017	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 6436

General

Start time:	17:07:47
Start date:	26/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
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: autoconv.exe PID: 5752 Parent PID: 3424

General

Start time:	17:07:59
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\autoconv.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autoconv.exe
Imagebase:	0x1e0000
File size:	851968 bytes
MD5 hash:	4506BE56787EDCD771A351C10B5AE3B7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: help.exe PID: 6840 Parent PID: 3424

General

Start time:	17:07:59
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\help.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\help.exe
Imagebase:	0x1390000
File size:	10240 bytes
MD5 hash:	09A715036F14D3632AD03B52D1DA6BFF
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: 00000006.00000002.1003763162.00000000005D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.1003763162.00000000005D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.1003763162.00000000005D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.1004298998.0000000000C50000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.1004298998.0000000000C50000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.1004298998.0000000000C50000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.1004347385.0000000000C80000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.1004347385.0000000000C80000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.1004347385.0000000000C80000.00000004.00000001.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	5EA017	NtReadFile

Analysis Process: cmd.exe PID: 6768 Parent PID: 6840

General

Start time:	17:08:03
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:	0x11d0000
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: 6748 Parent PID: 6768

General

Start time:	17:08:03
Start date:	26/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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