


**ID:** 433488
**Sample Name:**
http___192.3.141.164_mal_win32.exe
**Cookbook:** default.jbs
**Time:** 02:05:22
**Date:** 12/06/2021
**Version:** 32.0.0 Black Diamond

# Table of Contents

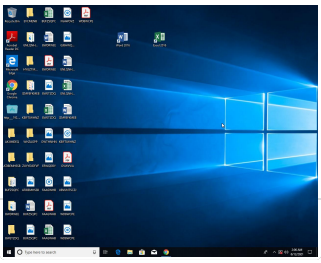
# Analysis Report http___192.3.141.164_mal_win32.exe

## Overview

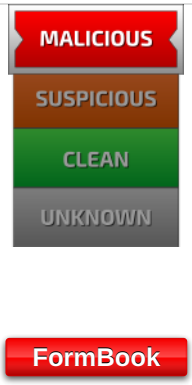
### General Information

| | |
|---|---|
| Sample Name: | http___192.3.141.164_mal_win32.exe |
| Analysis ID: | 433488 |
| MD5: | b9032e2b7b0712.. |
| SHA1: | a06bcdf6aab7fb8.. |
| SHA256: | 120ff2a109c01e3.. |
| Tags: | exe |
| Infos: | |

Most interesting Screenshot:



### Detection



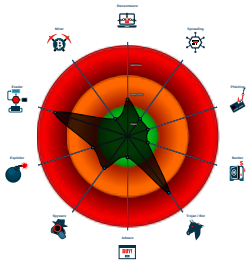

FormBook

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

### Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Yara detected AntiVM3
- Yara detected FormBook
- .NET source code contains method …
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…

### Classification



## Process Tree

- **System is w10x64**
- http___192.3.141.164_mal_win32.exe (PID: 5924 cmdline: 'C:\Users\user\Desktop\http___192.3.141.164_mal_win32.exe' MD5: B9032E2B7B07123F625F5D9E6E4F4796)
  - http___192.3.141.164_mal_win32.exe (PID: 3120 cmdline: C:\Users\user\Desktop\http___192.3.141.164_mal_win32.exe MD5: B9032E2B7B07123F625F5D9E6E4F4796)
- **cleanup**

## Malware Configuration

### Threatname: FormBook

```
{
  "C2 list": [
    "www.dragonpalcenk.com/k8n/"
  ],
  "decoy": [
    "foxynailserie.com",
    "thenoyzees.com",
    "waterrising.xyz",
    "allmister.com",
    "theguyscave.com",
    "erkitap.com",
    "spyder-club.com",
    "raskrutisam.com",
    "giantledlights.com",
    "wowbeautynails.com",
    "youmovies.site",
    "abjms.com",
    "enso-solutions.com",
    "seasonalcampgroundsmn.com",
    "lukeprater.com",
    "mufasacapital.com",
    "idi360.com",
    "mask-cleaner.com",
    "aeruswilmde.com",
    "venkatlifecoach.com",
    "crochetandgabbana.com",
    "onlineshreecollection.com",
    "gwenythportillowightman.com",
    "nexuspropertycare.com",
    "progress.solutions",
    "parkerut.com",
    "achebones.com",
    "jiazhengfu.com",
    "chlamydiadeetz.com",
    "thiele-concept.com",
    "bayareataxattorney.com",
    "geopainterdecorators.com",
    "makemybuild.com",
    "headsleepinstrument.online",
    "finevinum.com",
    "alphaworkoutgear.com",
    "8765pk.com",
    "rikonchat.com",
    "gitchat.net",
    "showy1.net",
    "tellurideminer.com",
    "triliumbrewing.com",
    "fioriapartment.com",
    "salubrigems.com",
    "sctsmney.com",
    "betgobar1.com",
    "thomaspurcell.com",
    "araket.com",
    "parisfilmfestival.online",
    "treepik.com",
    "artemisnaturalhealing.com",
    "littlehouseofhoarders.com",
    "buyselllm.com",
    "levnakava.com",
    "mygolfbetter.com",
    "vinlancer.com",
    "beetalkmobile.press",
    "gocampultralightmattress.com",
    "direk99.net",
    "nivxros.com",
    "cbgdenver.com",
    "datarock.net",
    "docondemand.net",
    "smithvilletexashistory.com"
  ]
}
```


# Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000000.00000002.652273897.0000000003539000.00000004.00000001.sdmp | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000000.00000002.652273897.0000000003539000.00000004.00000001.sdmp | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0xc1268:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0xc14e2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0xcd005:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0xccaf1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0xcd107:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0xcd27f:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0xc1efa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0xcbd6c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xc2bf3:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0xd2ca7:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0xd3caa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| 00000000.00000002.652273897.0000000003539000.00000004.00000001.sdmp | Formbook | detect Formbook in memory | JPCERT/CC Incident Response Group | • 0xcfd89:$sqlite3step: 68 34 1C 7B E1<br>• 0xcfe9c:$sqlite3step: 68 34 1C 7B E1<br>• 0xcfdb8:$sqlite3text: 68 38 2A 90 C5<br>• 0xcfedd:$sqlite3text: 68 38 2A 90 C5<br>• 0xcfdcb:$sqlite3blob: 68 53 D8 7F 8C<br>• 0xcfef3:$sqlite3blob: 68 53 D8 7F 8C |
| 00000000.00000002.652401187.0000000003671000.00000004.00000001.sdmp | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 00000000.00000002.652401187.0000000003671000.00000004.00000001.sdmp | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x17e728:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x17e9a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x18a4c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x189fb1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x18a5c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x18a73f:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0x17f3ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x18922c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0x1800b3:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x190167:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x19116a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| Click to see the 9 entries | | | | |

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 2.2.http___192.3.141.164_mal_win32.exe.400000.0.raw.unpack | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 2.2.http___192.3.141.164_mal_win32.exe.400000.0.raw.unpack | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| 2.2.http___192.3.141.164_mal_win32.exe.400000.0.raw.unpack | Formbook | detect Formbook in memory | JPCERT/CC Incident Response Group | • 0x18409:$sqlite3step: 68 34 1C 7B E1<br>• 0x1851c:$sqlite3step: 68 34 1C 7B E1<br>• 0x18438:$sqlite3text: 68 38 2A 90 C5<br>• 0x1855d:$sqlite3text: 68 38 2A 90 C5<br>• 0x1844b:$sqlite3blob: 68 53 D8 7F 8C<br>• 0x18573:$sqlite3blob: 68 53 D8 7F 8C |
| 2.0.http___192.3.141.164_mal_win32.exe.400000.1.unpack | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 2.0.http___192.3.141.164_mal_win32.exe.400000.1.unpack | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| Click to see the 7 entries | | | | |

## Sigma Overview

No Sigma rule has matched

## Signature Overview

Click to jump to signature section

### AV Detection:

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Machine Learning detection for sample

### Networking:

- C2 URLs / IPs found in malware configuration

### E-Banking Fraud:

- Yara detected FormBook

### System Summary:

- Malicious sample detected (through community Yara rule)

### Data Obfuscation:

- .NET source code contains method to dynamically call methods (often used by packers)

### Malware Analysis System Evasion:

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Tries to detect virtualization through RDTSC time measurements

### Stealing of Sensitive Information:

- Yara detected FormBook

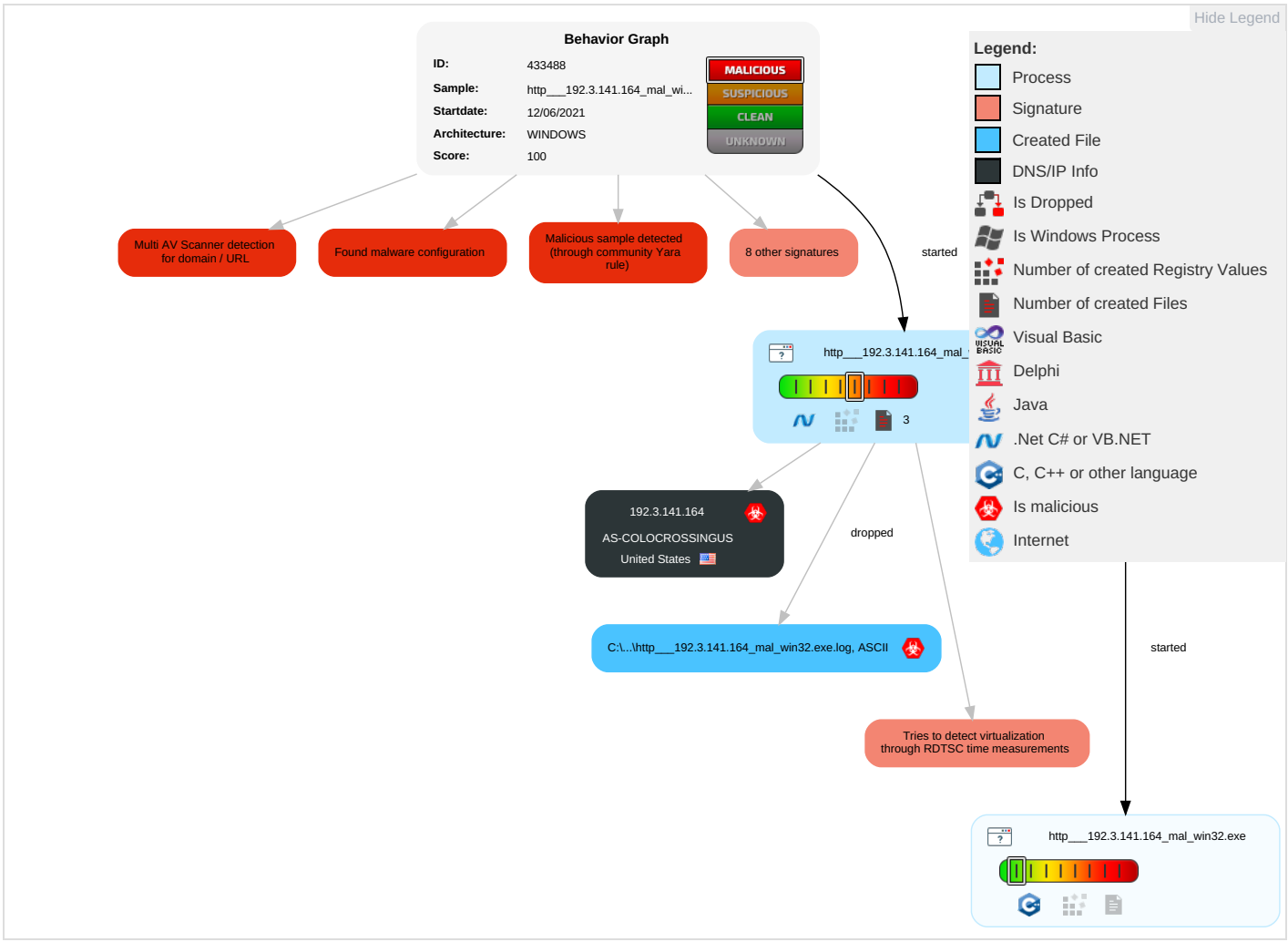
### Remote Access Functionality:

- 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 | Windows Management Instrumentation | Path Interception | Process Injection 1 1 | Masquerading 1 | Input Capture 1 | Security Software Discovery 2 2 1 | Remote Services | Input Capture 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eavesdrop or Insecure Network Communicati |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Disable or Modify Tools 1 | LSASS Memory | Process Discovery 1 | Remote Desktop Protocol | Archive Collected Data 1 1 | Exfiltration Over Bluetooth | Application Layer Protocol 1 | Exploit SS7 t Redirect Phor Calls/SMS |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Virtualization/Sandbox Evasion 3 1 | Security Account Manager | Virtualization/Sandbox Evasion 3 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Steganography | Exploit SS7 t Track Device Location |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Process Injection 1 1 | NTDS | System Information Discovery 1 1 2 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Deobfuscate/Decode Files or Information 1 1 | LSA Secrets | Remote System Discovery | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communicati |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Obfuscated Files or Information 4 | 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 | Software Packing 1 3 | DCSync | Network Sniffing | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port | Rogue Wi-Fi Access Point |

## 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 |
|---|---|---|---|---|
| http___192.3.141.164_mal_win32.exe | 48% | Virustotal | | Browse |
| http___192.3.141.164_mal_win32.exe | 28% | ReversingLabs | ByteCode-MSIL.Trojan.Heracles | |
| http___192.3.141.164_mal_win32.exe | 100% | Joe Sandbox ML | | |

## Dropped Files

**No Antivirus matches**

## Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 2.0.http___192.3.141.164_mal_win32.exe.400000.1.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen | | Download File |
| 2.2.http___192.3.141.164_mal_win32.exe.400000.0.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen | | Download File |

### Domains

No Antivirus matches

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| www.dragonpalcenk.com/k8n/ | 7% | Virustotal | | Browse |
| www.dragonpalcenk.com/k8n/ | 100% | Avira URL Cloud | malware | |

## Domains and IPs

### Contacted Domains

No contacted domains info

### Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| www.dragonpalcenk.com/k8n/ | true | • 7%, Virustotal, Browse<br>• Avira URL Cloud: malware | low |

### URLs from Memory and Binaries

### Contacted IPs

### Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 192.3.141.164 | unknown | United States | | 36352 | AS-COLOCROSSINGUS | true |

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 32.0.0 Black Diamond |
| Analysis ID: | 433488 |
| Start date: | 12.06.2021 |
| Start time: | 02:05:22 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 5m 18s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | http___192.3.141.164_mal_win32.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: | 3 |
| Number of new started drivers analysed: | 0 |
| Number of existing processes analysed: | 0 |
| Number of existing drivers analysed: | 0 |
| Number of injected processes analysed: | 0 |
| Technologies: | • HCA enabled<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |

| | |
|---|---|
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal100.troj.evad.winEXE@3/1@0/1 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 3.3% (good quality ratio 3%)<br>• Quality average: 71.3%<br>• Quality standard deviation: 31% |
| HCA Information: | • Successful, ratio: 98%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .exe<br>• Stop behavior analysis, all processes terminated |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 02:06:10 | API Interceptor | 2x Sleep call for process: http___192.3.141.164_mal_win32.exe modified |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 192.3.141.164 | Swift_Payment.MT103.docx | Get hash | malicious | Browse | • 192.3.141.164/oti/vbc.exe |

## Domains

**No context**

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| AS-COLOCROSSINGUS | Swift_Payment.MT103.docx | Get hash | malicious | Browse | • 192.3.141.164 |
| | WH4OtmG2dO.exe | Get hash | malicious | Browse | • 192.210.198.12 |
| | mPFY2OZSiZ.exe | Get hash | malicious | Browse | • 192.210.198.12 |
| | pXorUvhj09.exe | Get hash | malicious | Browse | • 192.210.198.12 |
| | L2.xlsx | Get hash | malicious | Browse | • 192.210.173.40 |
| | Agency Appointment VSL Tbn-Port-Appointment Letter-2100133.xlsx | Get hash | malicious | Browse | • 192.210.173.40 |
| | Request Letter for Courtesy Call.xlsx | Get hash | malicious | Browse | • 198.12.110.183 |
| | ORDEN 47458.xlsx | Get hash | malicious | Browse | • 198.12.110.183 |
| | Descuentos de hasta el 40%.xlsx | Get hash | malicious | Browse | • 198.12.110.183 |
| | crt9O3URua.exe | Get hash | malicious | Browse | • 198.23.140.76 |
| | _VM0_03064853.HtM | Get hash | malicious | Browse | • 23.94.52.94 |
| | 1LvgZjt4iv.exe | Get hash | malicious | Browse | • 198.46.177.119 |
| | PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx | Get hash | malicious | Browse | • 198.23.221.170 |
| | Purchase Order Price List 061021.xlsx | Get hash | malicious | Browse | • 198.12.127.155 |
| | xYKsdzAUj8.exe | Get hash | malicious | Browse | • 192.210.198.12 |
| | lsQ72VytAw.exe | Get hash | malicious | Browse | • 192.210.198.12 |
| | EDxI6b8IKs.exe | Get hash | malicious | Browse | • 192.210.198.12 |
| | ouGTVjHuUq.exe | Get hash | malicious | Browse | • 192.210.198.12 |
| | vbc.xlsx | Get hash | malicious | Browse | • 107.173.219.35 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | PO.xlsx | Get hash | malicious | Browse | • 198.12.110.183 |

## JA3 Fingerprints

No context

## Dropped Files

No context

# Created / dropped Files

| C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\http___192.3.141.164_mal_win32.exe.log | |
|---|---|
| Process: | C:\Users\user\Desktop\http___192.3.141.164_mal_win32.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1314 |
| Entropy (8bit): | 5.350128552078965 |
| Encrypted: | false |
| SSDEEP: | 24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR |
| MD5: | 1DC1A2DCC9EFAA84EABF4F6D6066565B |
| SHA1: | B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9 |
| SHA-256: | 28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF |
| SHA-512: | 95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7 |
| Malicious: | **true** |
| Reputation: | high, very likely benign file |
| 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): | 7.4991855714039755 |
| TrID: | • Win32 Executable (generic) Net Framework (10011505/4) 49.79%<br>• Win32 Executable (generic) a (10002005/4) 49.75%<br>• Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36%<br>• Windows Screen Saver (13104/52) 0.07%<br>• Win16/32 Executable Delphi generic (2074/23) 0.01% |
| File name: | http___192.3.141.164_mal_win32.exe |
| File size: | 949760 |
| MD5: | b9032e2b7b07123f625f5d9e6e4f4796 |
| SHA1: | a06bcdf6aab7fb82dad340465035549cd853e047 |
| SHA256: | 120ff2a109c01e38da86b9ce61c33906f6ddcea90a2fdf7ea3a67b08a271029c |
| SHA512: | a53309359e78dae4acef870b5c93040e1a851a97a7e6b9a9776ebfd80ca6f097e88cb20b2ac9a3bac7211562efbe552475556209c9372d03a0e1a8555fe211b6 |
| SSDEEP: | 24576:D6kdQhmaxPzRWfydThe6ns3vYETNeBUdt:fMxPzR4YTC5TwBU |

## General

| | |
|---|---|
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... `..... .....@.. ..... @..... |

## File Icon

| | |
|---|---|
| Icon Hash: | 8c8caa8e9692aa00 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x4bf02e |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED |
| DLL Characteristics: | NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT |
| Time Stamp: | 0x60C2A9DE [Fri Jun 11 00:10:06 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

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x2000 | 0xbd034 | 0xbd200 | False | 0.894979190763 | data | 7.84856370561 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .sdata | 0xc0000 | 0x1e8 | 0x200 | False | 0.86328125 | data | 6.60677487515 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0xc2000 | 0x2a3b8 | 0x2a400 | False | 0.124410595414 | data | 4.17274886097 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0xee000 | 0xc | 0x200 | False | 0.044921875 | data | 0.0980041756627 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Version Infos

# Network Behavior

**No network behavior found**

# Code Manipulations

# Statistics

## Behavior

Click to jump to process

# System Behavior

## Analysis Process: http___192.3.141.164_mal_win32.exe PID: 5924 Parent PID: 3028

### General

| | |
|---|---|
| Start time: | 02:06:08 |
| Start date: | 12/06/2021 |
| Path: | C:\Users\user\Desktop\http___192.3.141.164_mal_win32.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\http___192.3.141.164_mal_win32.exe' |
| Imagebase: | 0xe0000 |
| File size: | 949760 bytes |
| MD5 hash: | B9032E2B7B07123F625F5D9E6E4F4796 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Yara matches: | • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.652273897.0000000003539000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.652273897.0000000003539000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.652273897.0000000003539000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.652401187.0000000003671000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.652401187.0000000003671000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.652401187.0000000003671000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.651977772.000000000256F000.00000004.00000001.sdmp, Author: Joe Security |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Created

#### File Written

#### File Read

## Analysis Process: http___192.3.141.164_mal_win32.exe PID: 3120 Parent PID: 5924

## General

| | |
|---|---|
| Start time: | 02:06:11 |
| Start date: | 12/06/2021 |
| Path: | C:\Users\user\Desktop\http___192.3.141.164_mal_win32.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\Desktop\http___192.3.141.164_mal_win32.exe |
| Imagebase: | 0xba0000 |
| File size: | 949760 bytes |
| MD5 hash: | B9032E2B7B07123F625F5D9E6E4F4796 |
| 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: 00000002.00000000.650151759.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.650151759.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.650151759.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.651750558.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.651750558.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.651750558.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | low |

## File Activities

Show Windows behavior

### File Read

# Disassembly

## Code Analysis