


**ID:** 483640
**Sample Name:**
TPJX2QwEdXs5sTV.exe
**Cookbook:** default.jbs
**Time:** 10:37:40
**Date:** 15/09/2021
**Version:** 33.0.0 White Diamond

# Table of Contents

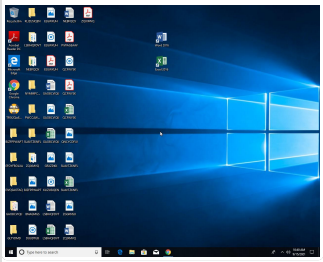
# Windows Analysis Report TPJX2QwEdXs5sTV.exe

## Overview

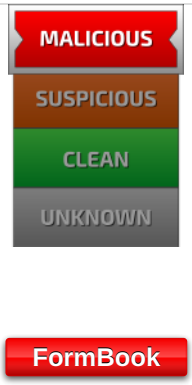
### General Information

| | |
|---|---|
| Sample Name: | TPJX2QwEdXs5sTV.exe |
| Analysis ID: | 483640 |
| MD5: | ce556ce97ea23c… |
| SHA1: | cc2bdaefa2f0ac1… |
| SHA256: | 7c3d5ebd2c417a.. |
| Tags: | exe Formbook xloader |
| Infos: | |

Most interesting Screenshot:



### Detection



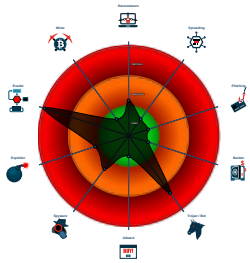

FormBook

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

### Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Sigma detected: Bad Opsec Default…
- Writes to foreign memory regions
- Tries to detect sandboxes and other…
- Performs DNS queries to domains w…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Queues an APC in another process …

### Classification



## Process Tree

- **System is w10x64**
- TPJX2QwEdXs5sTV.exe (PID: 5056 cmdline: 'C:\Users\user\Desktop\TPJX2QwEdXs5sTV.exe' MD5: CE556CE97EA23CBC2940F2AAD45D468F)
  - RegSvcs.exe (PID: 5192 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
  - RegSvcs.exe (PID: 4036 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
    - explorer.exe (PID: 3292 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - cmd.exe (PID: 3608 cmdline: C:\Windows\SysWOW64\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - cmd.exe (PID: 4572 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 4116 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

## Malware Configuration

### Threatname: FormBook

```
{
  "C2 list": [
    "www.438451.com/t75f/"
  ],
  "decoy": [
    "ice-lemon.pro",
    "ar3spro.cloud",
    "9055837.com",
    "fucksociety.net",
    "prettyofficialx.com",
    "mfxw.xyz",
    "relationshipquiz.info",
    "customia.xyz",
    "juanayjuan.com",
    "zidiankj.com",
    "facture-booking.com",
    "secondmining.store",
    "aboutyou.club",
    "gongxichen.com",
    "laurabraincreative.com",
    "pierrot-bros.com",
    "saintpaulaccountingservices.com",
    "dom-maya.com",
    "garderobamarzen.net",
    "la-salamandre-assurances.com",
    "pearmanprep.com",
    "telfarcontrol.com",
    "productsshareco.com",
    "cirf2021.online",
    "purchasevip.com",
    "cakewalkvision.com",
    "pointrenewables.com",
    "groups4n.com",
    "swnegce.xyz",
    "tjapro.com",
    "packagedesign.biz",
    "services-govgr.cloud",
    "shopgrassfedbeef.com",
    "tquilaint.com",
    "templetreemontessori.com",
    "munortiete.com",
    "nothingbutspotlesss.com",
    "fanpaixiu.xyz",
    "fr-site-amazon.com",
    "salartfinance.com",
    "beachers-shop.com",
    "friskvardaportalen.online",
    "pinsanova.site",
    "lemonvinyl.online",
    "indianadogeavaxsite.site",
    "styphon.com",
    "open24review-service.com",
    "bdjh9.xyz",
    "cocodiesel.com",
    "fortmyersfl.deals",
    "dsdtourism.com",
    "phone-il.net",
    "learningfactoryus.com",
    "incentreward.xyz",
    "travellerfund.com",
    "changcheng.pro",
    "cryptowalletts.com",
    "tradopplst.xyz",
    "autonomoustechnologyinc.com",
    "assessmentdna.xyz",
    "denicon-th.com",
    "dib5so.com",
    "genwealthbuilders.store",
    "delnetitcilo.net"
  ]
}
```


# Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000008.00000000.342627286.000000000E07 7000.00000040.00020000.sdmp | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000008.00000000.342627286.000000000E07 7000.00000040.00020000.sdmp | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x4695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x4181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x4797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0x33fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0x9b87:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0xac2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00 |
| 00000008.00000000.342627286.000000000E07 7000.00000040.00020000.sdmp | Formbook | detect Formbook in memory | JPCERT/CC Incident Response Group | • 0x6ab9:$sqlite3step: 68 34 1C 7B E1<br>• 0x6bcc:$sqlite3step: 68 34 1C 7B E1<br>• 0x6ae8:$sqlite3text: 68 38 2A 90 C5<br>• 0x6c0d:$sqlite3text: 68 38 2A 90 C5<br>• 0x6afb:$sqlite3blob: 68 53 D8 7F 8C<br>• 0x6c23:$sqlite3blob: 68 53 D8 7F 8C |
| 00000017.00000002.514970004.0000000002D9 0000.00000040.00020000.sdmp | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 00000017.00000002.514970004.0000000002D9 0000.00000040.00020000.sdmp | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x19b87:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1ac2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| Click to see the 27 entries | | | | |

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 6.2.RegSvcs.exe.400000.0.unpack | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 6.2.RegSvcs.exe.400000.0.unpack | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x18d87:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x19e2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| 6.2.RegSvcs.exe.400000.0.unpack | Formbook | detect Formbook in memory | JPCERT/CC Incident Response Group | • 0x15cb9:$sqlite3step: 68 34 1C 7B E1<br>• 0x15dcc:$sqlite3step: 68 34 1C 7B E1<br>• 0x15ce8:$sqlite3text: 68 38 2A 90 C5<br>• 0x15e0d:$sqlite3text: 68 38 2A 90 C5<br>• 0x15cfb:$sqlite3blob: 68 53 D8 7F 8C<br>• 0x15e23:$sqlite3blob: 68 53 D8 7F 8C |
| 1.2.TPJX2QwEdXs5sTV.exe.4175e30.1.raw.unpack | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 1.2.TPJX2QwEdXs5sTV.exe.4175e30.1.raw.unpack | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x68418:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x687a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x744b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x73fa1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x745b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x7472f:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0x691ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x7321c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0x69f32:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x799a7:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x7aa4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| Click to see the 4 entries | | | | |

# Sigma Overview

## System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Possible Applocker Bypass

# Jbx Signature Overview

Click to jump to signature section

## AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

## Networking:

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

Performs DNS queries to domains with low reputation

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 potential unpacker

## 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

## HIPS / PFW / Operating System Protection Evasion:

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Writes to foreign memory regions

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

## Stealing of Sensitive Information:

Yara detected FormBook

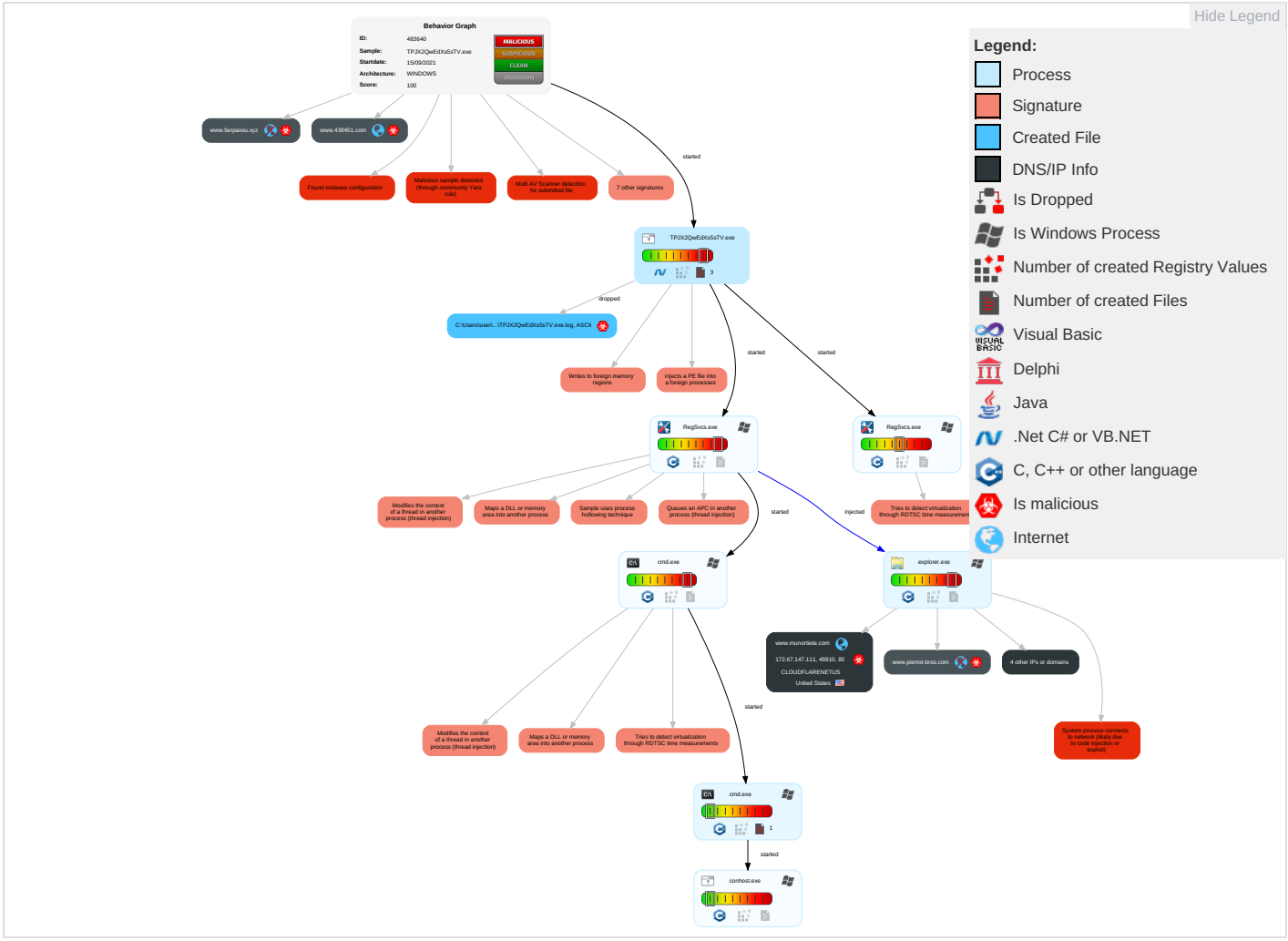
**Remote Access Functionality:**

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 1 | Shared Modules 1 | Valid Accounts 1 | Valid Accounts 1 | Masquerading 1 | Input Capture 1 | System Time Discovery 1 | Remote Services | Input Capture 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eavesdrop c Insecure Network Communica |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Access Token Manipulation 1 | Valid Accounts 1 | LSASS Memory | Security Software Discovery 2 4 1 | Remote Desktop Protocol | Archive Collected Data 1 1 | Exfiltration Over Bluetooth | Ingress Tool Transfer 1 | Exploit SS7 Redirect Phc Calls/SMS |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Process Injection 7 1 2 | Access Token Manipulation 1 | Security Account Manager | Process Discovery 2 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Non-Application Layer Protocol 2 | Exploit SS7 Track Devic Location |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Disable or Modify Tools 1 | NTDS | Virtualization/Sandbox Evasion 3 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Application Layer Protocol 1 2 | SIM Card Swap |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Virtualization/Sandbox Evasion 3 1 | LSA Secrets | Remote System Discovery 1 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communica |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Process Injection 7 1 2 | Cached Domain Credentials | File and Directory Discovery 1 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | Deobfuscate/Decode Files or Information 1 1 | DCSync | System Information Discovery 1 2 5 | 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 | Obfuscated Files or Information 4 | Proc Filesystem | Network Service Scanning | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Application Layer Protocol | Downgrade Insecure Protocols |
| Exploit Public-Facing Application | PowerShell | At (Linux) | At (Linux) | Software Packing 1 3 | /etc/passwd and /etc/shadow | System Network Connections Discovery | Software Deployment Tools | Data Staged | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | Web Protocols | Rogue Cellu Base Statior |

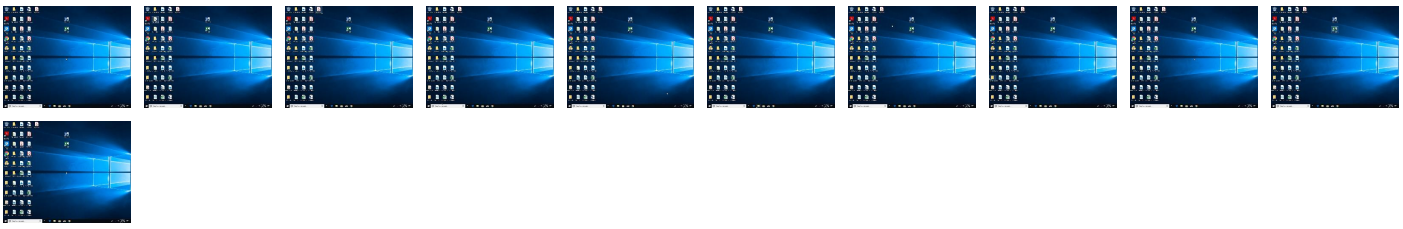
## Behavior Graph




## 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 |
|---|---|---|---|---|
| TPJX2QwEdXs5sTV.exe | 18% | ReversingLabs | ByteCode-MSIL.Spyware.Noon | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 6.2.RegSvcs.exe.400000.0.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen | | Download File |

### Domains

No Antivirus matches

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.zhongyicts.com.cnue | 0% | URL Reputation | safe | |
| http://www.carterandcone.comTCd | 0% | Avira URL Cloud | safe | |

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.carterandcone.comypoC | 0% | Avira URL Cloud | safe | |
| http://www.founder.com.cn/cn/bThe | 0% | URL Reputation | safe | |
| http://www.carterandcone.comak | 0% | Avira URL Cloud | safe | |
| http://www.carterandcone.com-se | 0% | Avira URL Cloud | safe | |
| http://www.carterandcone.com0 | 0% | Avira URL Cloud | safe | |
| http://www.tiro.com | 0% | URL Reputation | safe | |
| http://www.zhongyicts.com.cn0 | 0% | Avira URL Cloud | safe | |
| http://www.carterandcone.coml-g | 0% | Avira URL Cloud | safe | |
| http://www.goodfont.co.kr | 0% | URL Reputation | safe | |
| http://www.carterandcone.com | 0% | URL Reputation | safe | |
| http://www.carterandcone.com) | 0% | Avira URL Cloud | safe | |
| http://www.sajatypeworks.com | 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.galapagosdesign.com/staff/dennis.htm | 0% | URL Reputation | safe | |
| http://fontfabrik.com | 0% | URL Reputation | safe | |
| http://www.carterandcone.com? | 0% | Avira URL Cloud | safe | |
| http://www.zhongyicts.com.cncom | 0% | Avira URL Cloud | safe | |
| http://www.carterandcone.comue | 0% | URL Reputation | safe | |
| http://www.carterandcone.comMic | 0% | Avira URL Cloud | safe | |
| http://www.goodfont.co.krV | 0% | Avira URL Cloud | safe | |
| http://www.galapagosdesign.com/DPlease | 0% | URL Reputation | safe | |
| http://www.carterandcone.como._ | 0% | Avira URL Cloud | safe | |
| http://www.indianadogeavaxsite.site/t75f/?IL3h=sM7Ty9CQqazxDsp1L2wp1X0yz6j8iZQMubl0W4soZskD9oW6nOghj7d5yalvsy0iKmR0GSiRBw==&_hN0=5jFT8RbH3tHLZn | 0% | Avira URL Cloud | safe | |
| http://www.sandoll.co.kr | 0% | URL Reputation | safe | |
| http://www.urwpp.deDPlease | 0% | URL Reputation | safe | |
| http://www.carterandcone.coml-se | 0% | Avira URL Cloud | safe | |
| http://www.urwpp.de | 0% | URL Reputation | safe | |
| http://www.zhongyicts.com.cn | 0% | URL Reputation | safe | |
| http://fontfabrik.comj | 0% | Avira URL Cloud | safe | |
| http://www.sakkal.com | 0% | URL Reputation | safe | |
| http://www.goodfont.co.kr-cY | 0% | Avira URL Cloud | safe | |
| http://www.carterandcone.coma | 0% | URL Reputation | safe | |
| http://www.carterandcone.comexc | 0% | URL Reputation | safe | |
| http://www.tiro.comw | 0% | Avira URL Cloud | safe | |
| http://www.carterandcone.comd | 0% | URL Reputation | safe | |
| http://www.sajatypeworks.comt | 0% | URL Reputation | safe | |
| http://www.zhongyicts.com.cno.U | 0% | Avira URL Cloud | safe | |
| http://www.urwpp.deA | 0% | Avira URL Cloud | safe | |
| http://www.zhongyicts.com.cno.E | 0% | Avira URL Cloud | safe | |
| http://en.w | 0% | URL Reputation | safe | |
| http://www.sakkal.com9 | 0% | Avira URL Cloud | safe | |
| http://www.carterandcone.coml | 0% | URL Reputation | safe | |
| http://www.zhongyicts.com.cnk | 0% | Avira URL Cloud | safe | |
| www.438451.com/t75f/ | 0% | Avira URL Cloud | safe | |
| http://www.founder.com.cn/cn/ | 0% | URL Reputation | safe | |
| http://www.carterandcone.comof | 0% | Avira URL Cloud | safe | |
| http://www.founder.com.cn/cn | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cn0 | 0% | URL Reputation | safe | |
| http://www.sakkal.com3 | 0% | Avira URL Cloud | safe | |
| http://www.founder.com.cn/cncom | 0% | Avira URL Cloud | safe | |
| http://www.monotype. | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/ | 0% | URL Reputation | safe | |
| http://https://www.438451.com/t75f/?IL3h=1BeMm2dWByn9xv9J99R2XzKkk0MJMO8GKUMNYM3ZZNvYMz7ACarE0KIXHaUrAW4HLV | 0% | Avira URL Cloud | safe | |
| http://www.carterandcone.comona | 0% | URL Reputation | safe | |
| http://www.ascendercorp.com/typedesigners.htmlh | 0% | Avira URL Cloud | safe | |
| http://www.founder.com.cn/cnicr | 0% | URL Reputation | safe | |
| http://www.goodfont.co.kX | 0% | Avira URL Cloud | safe | |
| http://www.sandoll.co.kra-e# | 0% | Avira URL Cloud | safe | |
| http://www.founder.com.cn/cn( | 0% | URL Reputation | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| www.munortiete.com | 172.67.147.111 | true | true | | unknown |
| www.438451.com | 160.202.170.147 | true | true | | unknown |
| domains.readymag.com | 54.194.41.141 | true | false | | high |
| www.fanpaixiu.xyz | unknown | unknown | true | | unknown |
| www.ice-lemon.pro | unknown | unknown | true | | unknown |
| www.pierrot-bros.com | unknown | unknown | true | | unknown |
| www.indianadogeavaxsite.site | unknown | unknown | true | | unknown |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://www.indianadogeavaxsite.site/t75f/?IL3h=sM7Ty9CQqazxDsp1L2wp1X0yz6j8iZQMubl0W4soZskD9oW6nOghj7d5yalvsy0iKmR0GSiRBw==&_hN0=5jFT8RbH3tHLZn | true | • Avira URL Cloud: safe | unknown |
| www.438451.com/t75f/ | true | • Avira URL Cloud: safe | low |

## URLs from Memory and Binaries

## Contacted IPs

## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 54.194.41.141 | domains.readymag.com | United States | | 16509 | AMAZON-02US | false |
| 172.67.147.111 | www.munortiete.com | United States | | 13335 | CLOUDFLARENETUS | true |

## Private

| IP |
|---|
| 192.168.2.1 |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 483640 |
| Start date: | 15.09.2021 |
| Start time: | 10:37:40 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 11m 44s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | TPJX2QwEdXs5sTV.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: | 28 |
| 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@10/1@7/3 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 9.2% (good quality ratio 8.8%)<br>• Quality average: 77%<br>• Quality standard deviation: 26% |
| HCA Information: | • Successful, ratio: 99%<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 |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 10:38:48 | API Interceptor | 1x Sleep call for process: TPJX2QwEdXs5sTV.exe modified |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 54.194.41.141 | PO889876.pdf.exe | Get hash | malicious | Browse | • www.malee v.design/a7dr/?NTots 4J=R9ptnxQ NB44VdMlga vxu7aNuHoy YBwaJO8KVH Tec7XFz9L8 vbWf1S3lhR tFZGNrBr39 p&Ch9De=9r j01Zg0 |
| | DHL Receipt_AWB811470484778.exe | Get hash | malicious | Browse | • www.malee v.design/a7dr/?vT=R9 ptnxQNB44V dMlgavxu7a NuHoyYBwaJ O8KVHTec7X Fz9L8vbWf1 S3lhRtFZGN rBr39p&S0G l9T=RPHlpD KhNf_x |
| | Nigj57ar4W.exe | Get hash | malicious | Browse | • www.zuluf orest.com/ g050/?QZ3d 8rFH=51f9L teLSLtZ/KE FFUFc6GczS QZWKxJptRV R4rE3mzWWL USWQ1nFrlc 8EIzEiz7hG 4yH&3fnDH= hpvPaByp64 GpMl8p |

## Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| domains.readymag.com | PO889876.pdf.exe | Get hash | malicious | Browse | • 54.194.41.141 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | DHL Receipt_AWB811470484778.exe | Get hash | malicious | Browse | • 54.194.41.141 |

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| AMAZON-02US | tgamf4XuLa.exe | Get hash | malicious | Browse | • 99.83.154.118 |
| | SRMETALINDUSTRIES.exe | Get hash | malicious | Browse | • 44.227.65.245 |
| | PI L032452021xxls.exe | Get hash | malicious | Browse | • 99.83.154.118 |
| | Unpaid invoice.exe | Get hash | malicious | Browse | • 99.83.154.118 |
| | FaxGUO65DE.391343-Faa.html | Get hash | malicious | Browse | • 3.139.50.24 |
| | FaxGUO65DE.391343-Faa.html | Get hash | malicious | Browse | • 3.139.50.24 |
| | Elon Musk Club - 024705 .htm | Get hash | malicious | Browse | • 13.226.156.103 |
| | PGQBjDmDZ4 | Get hash | malicious | Browse | • 34.249.145.219 |
| | m5DozqUO2t | Get hash | malicious | Browse | • 54.70.167.99 |
| | avxeC9Wssi | Get hash | malicious | Browse | • 13.52.148.225 |
| | Wh3hrPWbBG | Get hash | malicious | Browse | • 34.249.145.219 |
| | re2.x86 | Get hash | malicious | Browse | • 184.77.232.100 |
| | re2.arm7 | Get hash | malicious | Browse | • 63.32.132.1 |
| | Fourlokov9.x86 | Get hash | malicious | Browse | • 34.249.145.219 |
| | re2.x86 | Get hash | malicious | Browse | • 54.96.126.50 |
| | re2.arm | Get hash | malicious | Browse | • 18.226.174.198 |
| | XbvAoRKnFm.exe | Get hash | malicious | Browse | • 52.218.0.168 |
| | Enclosed.xlsx | Get hash | malicious | Browse | • 13.238.159.178 |
| | HBW PAYMENT LIST FOR 2021,20210809.xlsx | Get hash | malicious | Browse | • 3.139.183.122 |
| | debit.xlsx | Get hash | malicious | Browse | • 52.77.232.215 |

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

| C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TPJX2QwEdXs5sTV.exe.log | |
|---|---|
| Process: | C:\Users\user\Desktop\TPJX2QwEdXs5sTV.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1216 |
| Entropy (8bit): | 5.355304211458859 |
| Encrypted: | false |
| SSDEEP: | 24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr |
| MD5: | FED34146BF2F2FA59DCF8702FCC8232E |
| SHA1: | B03BFEA175989D989850CF06FE5E7BBF56EAA00A |
| SHA-256: | 123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C |
| SHA-512: | 1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6 |
| Malicious: | **true** |
| Reputation: | high, very likely benign file |
| Preview: | 1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21 |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Entropy (8bit): | 7.724399427496627 |
| TrID: | • Win32 Executable (generic) Net Framework (10011505/4) 49.83%<br>• Win32 Executable (generic) a (10002005/4) 49.78%<br>• Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36%<br>• Generic Win/DOS Executable (2004/3) 0.01%<br>• DOS Executable Generic (2002/1) 0.01% |
| File name: | TPJX2QwEdXs5sTV.exe |
| File size: | 671232 |
| MD5: | ce556ce97ea23cbc2940f2aad45d468f |
| SHA1: | cc2bdaefa2f0ac108e2f456e42a42e8258580cf4 |
| SHA256: | 7c3d5ebd2c417a52b2a0b98dee95b5a7f283816f6a2453ceeffd31becc140882 |
| SHA512: | 82d4d71aeb5118d600394c64eb127ca4a87d7b83702feb4f9c5b0a0d98a597f812ebfd16784cbde54b9f4b1c87d3c7eaf57fb1c86b9720df95419887fc13f77b |
| SSDEEP: | 12288:cC2l/yzQs2TaIpIBykIwoL18/kdfskxRXP6erdH2fQiZ8uXpIe:cOMIpIBG/CUqRXP64gf5Ie |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L... .Aa.....n....."....  .....@.. .....@..... |

## File Icon

| | |
|---|---|
| Icon Hash: | f1f0f4d0eecccc71 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x49ed22 |
| 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: | 0x61419020 [Wed Sep 15 06:18:08 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 | 0x9cd28 | 0x9ce00 | False | 0.870889877988 | data | 7.79647412085 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .reloc | 0xa0000 | 0xc | 0x200 | False | 0.044921875 | data | 0.101910425663 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .rsrc | 0xa2000 | 0x6b3c | 0x6c00 | False | 0.441261574074 | data | 5.13425944435 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Version Infos

# Network Behavior

## Snort IDS Alerts

| Timestamp | Protocol | SID | Message | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|---|---|---|
| 09/15/21-10:40:22.963692 | TCP | 1201 | ATTACK-RESPONSES 403 Forbidden | 80 | 49809 | 54.194.41.141 | 192.168.2.7 |
| 09/15/21-10:40:30.779091 | ICMP | 402 | ICMP Destination Unreachable Port Unreachable | | | 192.168.2.7 | 8.8.8.8 |

## Network Port Distribution

### TCP Packets

### UDP Packets

### ICMP Packets

### DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Sep 15, 2021 10:40:17.770468950 CEST | 192.168.2.7 | 8.8.8.8 | 0x3f3c | Standard query (0) | www.ice-lemon.pro | A (IP address) | IN (0x0001) |
| Sep 15, 2021 10:40:22.819891930 CEST | 192.168.2.7 | 8.8.8.8 | 0x424a | Standard query (0) | www.indianadogeavaxsite.site | A (IP address) | IN (0x0001) |
| Sep 15, 2021 10:40:27.972635031 CEST | 192.168.2.7 | 8.8.8.8 | 0x4193 | Standard query (0) | www.pierrot-bros.com | A (IP address) | IN (0x0001) |
| Sep 15, 2021 10:40:28.970036983 CEST | 192.168.2.7 | 8.8.8.8 | 0x4193 | Standard query (0) | www.pierrot-bros.com | A (IP address) | IN (0x0001) |
| Sep 15, 2021 10:40:34.846492052 CEST | 192.168.2.7 | 8.8.8.8 | 0x5287 | Standard query (0) | www.munortiete.com | A (IP address) | IN (0x0001) |
| Sep 15, 2021 10:40:44.972348928 CEST | 192.168.2.7 | 8.8.8.8 | 0x14a0 | Standard query (0) | www.438451.com | A (IP address) | IN (0x0001) |
| Sep 15, 2021 10:40:50.800831079 CEST | 192.168.2.7 | 8.8.8.8 | 0xc584 | Standard query (0) | www.fanpaixiu.xyz | A (IP address) | IN (0x0001) |

### DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Sep 15, 2021 10:40:17.801754951 CEST | 8.8.8.8 | 192.168.2.7 | 0x3f3c | Server failure (2) | www.ice-lemon.pro | none | none | A (IP address) | IN (0x0001) |
| Sep 15, 2021 10:40:22.864661932 CEST | 8.8.8.8 | 192.168.2.7 | 0x424a | No error (0) | www.indianadogeavaxsite.site | domains.readymag.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 15, 2021 10:40:22.864661932 CEST | 8.8.8.8 | 192.168.2.7 | 0x424a | No error (0) | domains.readymag.com | | 54.194.41.141 | A (IP address) | IN (0x0001) |
| Sep 15, 2021 10:40:29.799778938 CEST | 8.8.8.8 | 192.168.2.7 | 0x4193 | Server failure (2) | www.pierrot-bros.com | none | none | A (IP address) | IN (0x0001) |
| Sep 15, 2021 10:40:30.778945923 CEST | 8.8.8.8 | 192.168.2.7 | 0x4193 | Server failure (2) | www.pierrot-bros.com | none | none | A (IP address) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Sep 15, 2021 10:40:34.879271030 CEST | 8.8.8.8 | 192.168.2.7 | 0x5287 | No error (0) | www.munortiete.com | | 172.67.147.111 | A (IP address) | IN (0x0001) |
| Sep 15, 2021 10:40:34.879271030 CEST | 8.8.8.8 | 192.168.2.7 | 0x5287 | No error (0) | www.munortiete.com | | 104.21.71.167 | A (IP address) | IN (0x0001) |
| Sep 15, 2021 10:40:45.377986908 CEST | 8.8.8.8 | 192.168.2.7 | 0x14a0 | No error (0) | www.438451.com | | 160.202.170.147 | A (IP address) | IN (0x0001) |
| Sep 15, 2021 10:40:51.148735046 CEST | 8.8.8.8 | 192.168.2.7 | 0xc584 | Name error (3) | www.fanpaixiu.xyz | none | none | A (IP address) | IN (0x0001) |

## HTTP Request Dependency Graph

- www.indianadogeavaxsite.site
- www.munortiete.com

## HTTP Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.7 | 49809 | 54.194.41.141 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Sep 15, 2021 10:40:22.916647911 CEST | 6201 | OUT | GET /t75f/?IL3h=sM7Ty9CQqazxDsp1L2wp1X0yz6j8iZQMubl0W4soZskD9oW6nOghj7d5yalvsy0iKmR0GSiRBw==&_hN0=5jFT8RbH3tHLZn HTTP/1.1<br>Host: www.indianadogeavaxsite.site<br>Connection: close<br>Data Raw: 00 00 00 00 00 00 00 00<br>Data Ascii: |
| Sep 15, 2021 10:40:22.963691950 CEST | 6201 | IN | HTTP/1.1 403 Forbidden<br>Server: nginx<br>Date: Wed, 15 Sep 2021 08:40:22 GMT<br>Content-Type: text/html<br>Content-Length: 118<br>Connection: close<br>Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a<br>Data Ascii: <html><head><title>403 Forbidden</title></head><body> <h1>403 Forbidden</h1> </body></html> |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 1 | 192.168.2.7 | 49810 | 172.67.147.111 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Sep 15, 2021 10:40:34.909507036 CEST | 6203 | OUT | GET /t75f/?IL3h=1LVEWTKjgk7dQQTcgX7ekf6vWGvALEiRfuym9xfNfV6ZlhpaQ60NuXtsMiMogZeeqS9jy4XPVA==&_hN0=5jFT8RbH3tHLZn HTTP/1.1<br>Host: www.munortiete.com<br>Connection: close<br>Data Raw: 00 00 00 00 00 00 00 00<br>Data Ascii: |
| Sep 15, 2021 10:40:34.941842079 CEST | 6204 | IN | HTTP/1.1 301 Moved Permanently<br>Date: Wed, 15 Sep 2021 08:40:34 GMT<br>Transfer-Encoding: chunked<br>Connection: close<br>Cache-Control: max-age=3600<br>Expires: Wed, 15 Sep 2021 09:40:34 GMT<br>Location: https://www.munortiete.com/t75f/?IL3h=1LVEWTKjgk7dQQTcgX7ekf6vWGvALEiRfuym9xfNfV6ZlhpaQ60NuXtsMiMogZeeqS9jy4XPVA==&_hN0=5jFT8RbH3tHLZn<br>Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=tf19gfgwC210LIACe1vV29u1H4wndpzEQechmp6W8NM%2F%2BBin2oGR1mlmAEeHy867OF7b8VWH9BEaP2fn4MX%2Bi29fIOkrR25WYxU0SDHleBOTosji4XBUZ%2Bk08tOt9qjCq1Gz6as%3D"}],"group":"cf-nel","max_age":604800}<br>NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}<br>Server: cloudflare<br>CF-RAY: 68f08d124ee7d6b5-FRA<br>alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400<br>Data Raw: 30 0d 0a 0d 0a<br>Data Ascii: 0 |

# Code Manipulations

# Statistics

## Behavior

Click to jump to process

# System Behavior

## Analysis Process: TPJX2QwEdXs5sTV.exe PID: 5056 Parent PID: 5424

### General

| | |
|---|---|
| Start time: | 10:38:35 |
| Start date: | 15/09/2021 |
| Path: | C:\Users\user\Desktop\TPJX2QwEdXs5sTV.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\TPJX2QwEdXs5sTV.exe' |
| Imagebase: | 0xcd0000 |
| File size: | 671232 bytes |
| MD5 hash: | CE556CE97EA23CBC2940F2AAD45D468F |
| 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: 00000001.00000002.281632826.0000000002FA1000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.282361714.0000000003FA9000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.282361714.0000000003FA9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.282361714.0000000003FA9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.282500066.000000000409E000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.282500066.000000000409E000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.282500066.000000000409E000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Created

#### File Written

#### File Read

## Analysis Process: RegSvcs.exe PID: 5192 Parent PID: 5056

### General

| | |
|---|---|
| Start time: | 10:38:49 |
| Start date: | 15/09/2021 |
| Path: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe |
| Imagebase: | 0x410000 |
| File size: | 45152 bytes |
| MD5 hash: | 2867A3817C9245F7CF518524DFD18F28 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: RegSvcs.exe PID: 4036 Parent PID: 5056

### General

| | |
|---|---|
| Start time: | 10:38:50 |
| Start date: | 15/09/2021 |
| Path: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe |
| Imagebase: | 0x470000 |
| File size: | 45152 bytes |
| MD5 hash: | 2867A3817C9245F7CF518524DFD18F28 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.390262569.00000000009D0000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.390262569.00000000009D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.390262569.00000000009D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.389976608.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.389976608.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.389976608.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.390330954.0000000000A20000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.390330954.0000000000A20000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.390330954.0000000000A20000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | high |

### File Activities

Show Windows behavior

### File Read

## Analysis Process: explorer.exe PID: 3292 Parent PID: 4036

### General

| | |
|---|---|
| Start time: | 10:38:55 |
| Start date: | 15/09/2021 |
| Path: | C:\Windows\explorer.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\Explorer.EXE |
| Imagebase: | 0x7ff662bf0000 |
| File size: | 3933184 bytes |
| MD5 hash: | AD5296B280E8F522A8A897C96BAB0E1D |
| 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: 00000008.00000000.342627286.000000000E077000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.342627286.000000000E077000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.342627286.000000000E077000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.321761934.000000000E077000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.321761934.000000000E077000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.321761934.000000000E077000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | high |

### File Activities

Show Windows behavior

## Analysis Process: cmd.exe PID: 3608 Parent PID: 4036

### General

| | |
|---|---|
| Start time: | 10:39:43 |
| Start date: | 15/09/2021 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\cmd.exe |
| Imagebase: | 0x870000 |
| File size: | 232960 bytes |
| MD5 hash: | F3BDBE3BB6F734E357235F4D5898582D |
| 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: 00000017.00000002.514970004.0000000002D90000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.514970004.0000000002D90000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.514970004.0000000002D90000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.512368731.0000000000940000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.512368731.0000000000940000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.512368731.0000000000940000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.513972990.00000000029D0000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.513972990.00000000029D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.513972990.00000000029D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | high |

### File Activities

Show Windows behavior

### File Read

## Analysis Process: cmd.exe PID: 4572 Parent PID: 3608

### General

| | |
|---|---|
| Start time: | 10:39:45 |
| Start date: | 15/09/2021 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe' |
| Imagebase: | 0x870000 |
| 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

Show Windows behavior

## Analysis Process: conhost.exe PID: 4116 Parent PID: 4572

### General

| | |
|---|---|
| Start time: | 10:39:46 |
| Start date: | 15/09/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff774ee0000 |
| 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