


**ID:** 445164
**Sample Name:** 5.dll
**Cookbook:** default.jbs
**Time:** 10:40:23
**Date:** 07/07/2021
**Version:** 32.0.0 Black Diamond

# Table of Contents

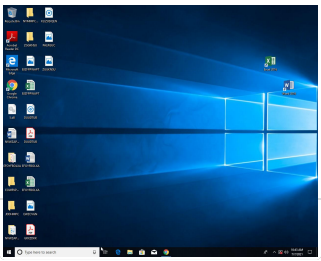
# Windows Analysis Report 5.dll

## Overview

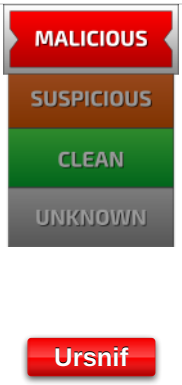
### General Information

| | |
|---|---|
| Sample Name: | 5.dll |
| Analysis ID: | 445164 |
| MD5: | fceb6a51be4205d. |
| SHA1: | 0abb60d37fac499. |
| SHA256: | c521dd937ce9b2.. |
| Tags: | dll |
| Infos: | |

Most interesting Screenshot:



### Detection

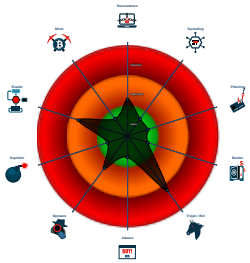



| | |
|---|---|
| Score: | 84 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected Ursnif
- Machine Learning detection for samp…
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Contains functionality to call native f…
- Contains functionality to check if a d…
- Contains functionality to check if a d…
- Contains functionality to dynamically…
- Contains functionality to query CPU …

### Classification



## Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 2248 cmdline: loaddll32.exe 'C:\Users\user\Desktop\5.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 5484 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\5.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 452 cmdline: rundll32.exe 'C:\Users\user\Desktop\5.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1716 cmdline: rundll32.exe C:\Users\user\Desktop\5.dll,Clockcondition MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2940 cmdline: rundll32.exe C:\Users\user\Desktop\5.dll,Dogwhen MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3904 cmdline: rundll32.exe C:\Users\user\Desktop\5.dll,Sing MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5580 cmdline: rundll32.exe C:\Users\user\Desktop\5.dll,Wholegray MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 1900 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 3220 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1900 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5264 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1900 CREDAT:17418 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

## Malware Configuration

### Threatname: Ursnif


```
{
  "RSA Public Key":
"ovNAU+HRorLZmwnDvbYFDY7UA+FTIAnF2uJSQd0M+N3ep6CVEhoDrEXACstP09QHK7cBl9nMAaFI1as0K4aXOQKngdScIQbDa3MQ98Ce9MYRMvxGUI05fSIRRFzMYffOXQr97vVUUUPjsYgfkDWS2eKPxSe5dz/pF0mjA0T8ibOLzHmV
Ms4vVv+nwVAw0xpD",
  "c2_domain": [
    "outlook.com",
    "auredosite.club",
    "vuredosite.club"
  ],
  "botnet": "8877",
  "server": "12",
  "serpent_key": "30218409ILPAJDUR",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0",
  "DGA_count": "10"
}
```

# Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000003.00000003.451946137.0000000004D18000.00000004.00000040.sdmp | JoeSecurity_Ursnif | Yara detected Ursnif | Joe Security | |
| 00000003.00000003.452051043.0000000004D18000.00000004.00000040.sdmp | JoeSecurity_Ursnif | Yara detected Ursnif | Joe Security | |
| 00000000.00000002.496928044.0000000003328000.00000004.00000040.sdmp | JoeSecurity_Ursnif | Yara detected Ursnif | Joe Security | |
| 00000000.00000003.445570350.0000000003328000.00000004.00000040.sdmp | JoeSecurity_Ursnif | Yara detected Ursnif | Joe Security | |
| 00000003.00000003.452023874.0000000004D18000.00000004.00000040.sdmp | JoeSecurity_Ursnif | Yara detected Ursnif | Joe Security | |
| Click to see the 15 entries | | | | |

# Sigma Overview

**No Sigma rule has matched**

# Jbx Signature Overview

Click to jump to signature section

## AV Detection:

**Found malware configuration**

**Multi AV Scanner detection for submitted file**

**Machine Learning detection for sample**

## Networking:

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

## Key, Mouse, Clipboard, Microphone and Screen Capturing:

**Yara detected Ursnif**

## E-Banking Fraud:

**Yara detected Ursnif**

## System Summary:

**Writes or reads registry keys via WMI**

**Writes registry values via WMI**

## Hooking and other Techniques for Hiding and Protection:

**Yara detected Ursnif**

**Stealing of Sensitive Information:**

**Yara detected Ursnif**

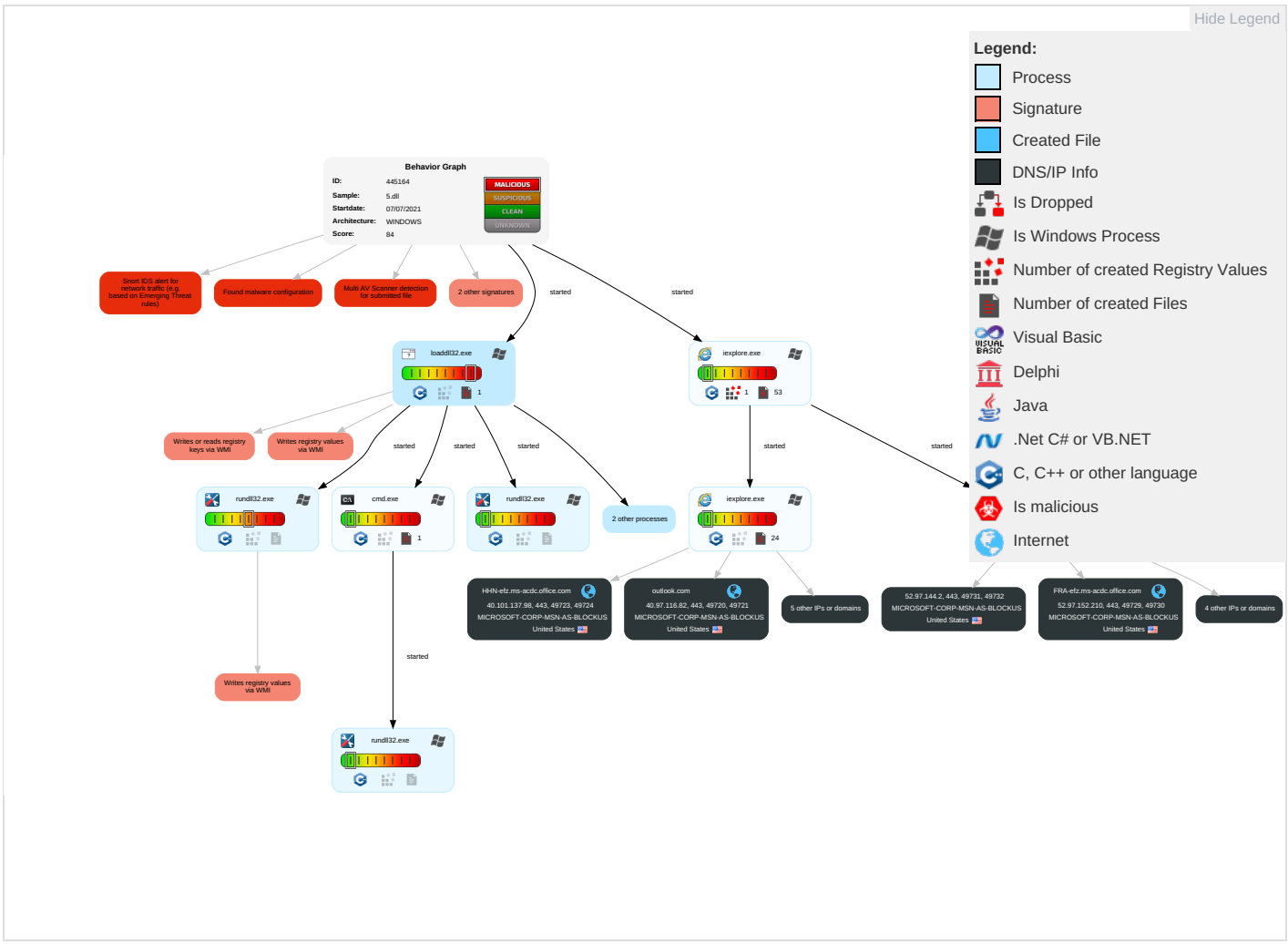
**Remote Access Functionality:**

**Yara detected Ursnif**

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation 2 | Path Interception | Process Injection 1 2 | Masquerading 1 | OS Credential Dumping | System Time Discovery 1 | Remote Services | Archive Collected Data 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 2 | Eavesdrop on Insecure Network Communication |
| Default Accounts | Native API 1 | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Process Injection 1 2 | LSASS Memory | Query Registry 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Ingress Tool Transfer 1 | Exploit SS7 to Redirect Phone Calls/SMS |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Deobfuscate/Decode Files or Information 1 | Security Account Manager | Security Software Discovery 3 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Non-Application Layer Protocol 2 | Exploit SS7 to Track Device Location |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Obfuscated Files or Information 2 1 | NTDS | Process Discovery 2 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Application Layer Protocol 3 | SIM Card Swap |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Rundll32 1 | LSA Secrets | Account Discovery 1 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Software Packing 1 | Cached Domain Credentials | System Owner/User 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 | Compile After Delivery | DCSync | File and Directory Discovery 1 | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port | Rogue Wi-Fi Access Points |
| Drive-by Compromise | Command and Scripting Interpreter | Scheduled Task/Job | Scheduled Task/Job | Indicator Removal from Tools | Proc Filesystem | System Information Discovery 2 3 | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Application Layer Protocol | Downgrade to Insecure Protocols |

## Behavior Graph




# Screenshots

## Thumbnails

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


## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| 5.dll | 22% | Virustotal | | Browse |
| 5.dll | 100% | Joe Sandbox ML | | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 0.2.loaddll32.exe.c30000.0.unpack | 100% | Avira | HEUR/AGEN.1108168 | | Download File |
| 3.2.rundll32.exe.2a70000.1.unpack | 100% | Avira | HEUR/AGEN.1108168 | | Download File |

### Domains

No Antivirus matches

### URLs

No Antivirus matches

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| outlook.com | 40.97.116.82 | true | false | | high |
| HHN-efz.ms-acdc.office.com | 40.101.137.98 | true | false | | high |
| FRA-efz.ms-acdc.office.com | 52.97.152.210 | true | false | | high |
| www.outlook.com | unknown | unknown | false | | high |
| outlook.office365.com | unknown | unknown | false | | high |

## URLs from Memory and Binaries

## Contacted IPs

## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 40.101.137.98 | HHN-efz.ms-acdc.office.com | United States | | 8075 | MICROSOFT-CORP-MSN-AS-BLOCKUS | false |
| 52.97.152.210 | FRA-efz.ms-acdc.office.com | United States | | 8075 | MICROSOFT-CORP-MSN-AS-BLOCKUS | false |
| 52.97.144.2 | unknown | United States | | 8075 | MICROSOFT-CORP-MSN-AS-BLOCKUS | false |
| 52.97.233.2 | unknown | United States | | 8075 | MICROSOFT-CORP-MSN-AS-BLOCKUS | false |
| 40.97.116.82 | outlook.com | United States | | 8075 | MICROSOFT-CORP-MSN-AS-BLOCKUS | false |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 32.0.0 Black Diamond |
| Analysis ID: | 445164 |
| Start date: | 07.07.2021 |
| Start time: | 10:40:23 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 8m 59s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | 5.dll |
| 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: | 31 |
| 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: | mal84.troj.winDLL@18/7@6/5 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 13.4% (good quality ratio 12.6%)<br>• Quality average: 78.7%<br>• Quality standard deviation: 29.5% |

| | |
|---|---|
| HCA Information: | • Successful, ratio: 69%<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: .dll |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 10:42:35 | API Interceptor | 1x Sleep call for process: rundll32.exe modified |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 52.97.152.210 | http://https://r0qp15r0b1rq05rrpbqbrpq5.s3-eu-west-1.amazonaws.com/Ap3dX.html#orderadmin@roku.com | Get hash | malicious | Browse | |
| | loader.exe | Get hash | malicious | Browse | |
| | https:\\bit.ly/2WRZ0S5#joyce.chay@milliken.com | Get hash | malicious | Browse | |
| | http://https://learn4fun.cz/domains/learn4fun.cz/ahgf36894we894jsd/voicemessage/ | Get hash | malicious | Browse | |
| 52.97.144.2 | E848.tmp.exe | Get hash | malicious | Browse | |
| | 0G2gue8shl.exe | Get hash | malicious | Browse | |
| | shipping_doc.exe | Get hash | malicious | Browse | |
| | http://https://immense-bullfrog.10web.me/ | Get hash | malicious | Browse | |
| | http://https://projectcheckg.web.app/#taxes@abrholdings.com | Get hash | malicious | Browse | |
| | ze99HWZnJK.exe | Get hash | malicious | Browse | |
| | http://https://app.upthere.com/elnino/assets/pdfjs/viewer/ce6fefe64453f27791ffdf3afa5bbdadb5d75d7267b297b30b776a371de64e63/45b49d4fce909afc27225208cd0205c692535fc89a07ab840bb78533e2925460?view_id=e28c4043fb3f3e666cddd8b96543302e5bac6c21c762fba5b895a91a251f9b48&branch_id=52a27d4473c90b9b6d624d662ab8a832c97a3c384a2b776927ed4eccc24a1e0a?*35354689209358HvT35W1Sh3509mW81735BbW098QdbK09W1Sh | Get hash | malicious | Browse | |
| | http://https://bradyblocks.com/fob/Pro/onedauth/office/index.php | Get hash | malicious | Browse | |
| | http://https://u10269907.ct.sendgrid.net/wf/click?upn=7TnevfDNdxZp2Q3ysQ7X3oESB0-2FDPAHHGrCSuhANFl0RilaXTQqc14zMc-2FpX9M8w_fxDop4UK-2FXWtvz-2Fo4SgBilCRDsINTKa-2BV6WoX7TCamBzN4Y3OFVxfYIFnMjo2oF0yanJFKyei-2FKbXVFZy2wWdw2BISVfQ0uuj040ducQ3e4x0ReqX-2BeavUyA3qBOBoptIxux6KHZnY0imx8tUJ6aPUBf7V4AQsKN3qI-2FJUs5ka5TGYo3JtEVvh56ieL-2BftMts8GVieoN5pgiQgMOSfl-2FS3as8UhjMRUwml-2Btsxw6bkw-3D | Get hash | malicious | Browse | |
| 52.97.233.2 | http://https://deatee00.z13.web.core.windows.net/#guyb@thomas.co | Get hash | malicious | Browse | |
| 40.97.116.82 | 2790000.dll | Get hash | malicious | Browse | |
| | 2770174.dll | Get hash | malicious | Browse | |
| | 60e40fb428612.dll | Get hash | malicious | Browse | |
| | zHUScMPOlZ.dll | Get hash | malicious | Browse | |
| | nT5pUwoJSS.dll | Get hash | malicious | Browse | |
| | .exe | Get hash | malicious | Browse | |
| | 82attachmen.exe | Get hash | malicious | Browse | |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | 62lette.exe | Get hash | malicious | Browse | |
| | 5transcrip.exe | Get hash | malicious | Browse | |
| | 1message.exe | Get hash | malicious | Browse | |
| | 49instructio.exe | Get hash | malicious | Browse | |
| | .exe | Get hash | malicious | Browse | |
| | 52DOCUMEN.exe | Get hash | malicious | Browse | |
| | 25messag.exe | Get hash | malicious | Browse | |
| | fuck.exe | Get hash | malicious | Browse | |

## Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| HHN-efz.ms-acdc.office.com | PreOrder.exe | Get hash | malicious | Browse | • 52.97.201.2 |
| | 2790000.dll | Get hash | malicious | Browse | • 52.97.201.50 |
| | 2770174.dll | Get hash | malicious | Browse | • 52.98.175.18 |
| | 60e40fb428612.dll | Get hash | malicious | Browse | • 52.97.201.18 |
| | zHUScMPOlZ.dll | Get hash | malicious | Browse | • 40.101.136.242 |
| | SwiftDocument.HTML | Get hash | malicious | Browse | • 40.101.136.18 |
| | Xerox scan.html | Get hash | malicious | Browse | • 52.98.151.226 |
| | r.dll | Get hash | malicious | Browse | • 40.101.137.2 |
| | a9FUs89dWy.dll | Get hash | malicious | Browse | • 52.98.171.226 |
| | 60b49bdd63509.dll | Get hash | malicious | Browse | • 40.101.137.50 |
| | nT5pUwoJSS.dll | Get hash | malicious | Browse | • 52.97.201.34 |
| | nT5pUwoJSS.dll | Get hash | malicious | Browse | • 52.97.233.66 |
| | kZcCqvNtWa.dll | Get hash | malicious | Browse | • 52.98.171.226 |
| | A5uTdwOwJ1.dll | Get hash | malicious | Browse | • 40.101.138.210 |
| | FuiZSHt8Hx.dll | Get hash | malicious | Browse | • 52.98.151.242 |
| | 609a460e94791.tiff.dll | Get hash | malicious | Browse | • 52.97.201.34 |
| | iJdlvBxhYu.dll | Get hash | malicious | Browse | • 52.97.150.2 |
| | 8OKQ6ogGRx.dll | Get hash | malicious | Browse | • 40.101.138.2 |
| | 609110f2d14a6.dll | Get hash | malicious | Browse | • 40.101.137.34 |
| | New%20order%20contract.html | Get hash | malicious | Browse | • 52.98.175.2 |
| outlook.com | oEE058tCoG.exe | Get hash | malicious | Browse | • 40.93.207.1 |
| | 2Bmv1UZL2m.exe | Get hash | malicious | Browse | • 52.101.24.0 |
| | oS4iWYYsx7.exe | Get hash | malicious | Browse | • 104.47.53.36 |
| | P4SRvI1baM.exe | Get hash | malicious | Browse | • 104.47.54.36 |
| | 051y0i7M8q.exe | Get hash | malicious | Browse | • 40.93.207.0 |
| | lEbR9gFgLr.exe | Get hash | malicious | Browse | • 104.47.54.36 |
| | 0OvBoFRzgC.exe | Get hash | malicious | Browse | • 104.47.54.36 |
| | A1qhcbngFV.exe | Get hash | malicious | Browse | • 104.47.54.36 |

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| MICROSOFT-CORP-MSN-AS-BLOCKUS | sud-life-mobcast.apk | Get hash | malicious | Browse | • 104.45.180.93 |
| | sud-life-outwork.apk | Get hash | malicious | Browse | • 104.45.180.93 |
| | Flwphoptcdyxlxhpejlfjgmsyzqkhoqweu.exe | Get hash | malicious | Browse | • 20.80.30.45 |
| | 2790000.dll | Get hash | malicious | Browse | • 40.101.136.2 |
| | 2770174.dll | Get hash | malicious | Browse | • 40.101.136.2 |
| | 60e40fb428612.dll | Get hash | malicious | Browse | • 52.97.201.18 |
| | 9cYXsscTTT.exe | Get hash | malicious | Browse | • 104.42.151.234 |
| | TestTakerSBBrowser.exe | Get hash | malicious | Browse | • 137.117.66.167 |
| | mJSDCeNxFi.exe | Get hash | malicious | Browse | • 40.88.32.150 |
| | oEE058tCoG.exe | Get hash | malicious | Browse | • 40.93.212.0 |
| | zHUScMPOlZ.dll | Get hash | malicious | Browse | • 40.97.116.82 |
| | hsIF8b0YX1.msi | Get hash | malicious | Browse | • 191.235.71.131 |
| | x86_x64_setup.exe | Get hash | malicious | Browse | • 104.43.193.48 |
| | h3hlbLDpl8.exe | Get hash | malicious | Browse | • 13.64.90.137 |
| | PAYMENT.HTML | Get hash | malicious | Browse | • 13.71.84.154 |
| | JOB-in.line e.K.- Purchase Order 19600396 & 19600397.xlsx.exe | Get hash | malicious | Browse | • 13.82.24.228 |
| | y3sBoQe6u7.exe | Get hash | malicious | Browse | • 52.170.189.162 |
| | NC46O8xw5Z.exe | Get hash | malicious | Browse | • 52.170.189.162 |
| | input.06.21.doc | Get hash | malicious | Browse | • 52.109.32.41 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | PaymentConfirmation.pdf.exe | Get hash | malicious | Browse | • 13.90.75.180 |

## JA3 Fingerprints

No context

## Dropped Files

No context

# Created / dropped Files

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{BD6AF35A-DF4A-11EB-90E5-ECF4BB570DC9}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 50344 |
| Entropy (8bit): | 2.003853863777815 |
| Encrypted: | false |
| SSDEEP: | 96:ryZlZW2OWEtfbfOq5KMvhqUhQAoxhHS7c3MVs7c8w7Uksw7UONvjaUntvHaaI1v8:ryZlZW2OWEtDfONMgbzJMj/N1tw/o7og |
| MD5: | 1B2C08B04283EF2331ACDE91B8BBCB4D |
| SHA1: | 43A807C8569A26885E912103F9D6D63547638D07 |
| SHA-256: | 77E5A7867B6DA6BC138D8896ACB6DE61361F526F8CA51CE601A9E68DC95E6992 |
| SHA-512: | 9FA7CD627AAEC7EF1B91992798BE68E7E8FA91E5D9390CD925E2E8457F3EF83B37C7EFCD81CDF11BA26FFBEE205828C74B771815C9A970451DC2178837BE0C9 |
| Malicious: | false |
| Reputation: | low |
| Preview: | .....R.o.o.t. .E.n.t.r.y..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{BD6AF35C-DF4A-11EB-90E5-ECF4BB570DC9}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 27384 |
| Entropy (8bit): | 1.848069425899241 |
| Encrypted: | false |
| SSDEEP: | 96:rBZqQ+6sBSdj32DWuMyywBSlHGd9sRwBSlHGd9gSlZA:rBZqQ+6skdj32DWuMyyw2HK+Rw2HKLZA |
| MD5: | ABBBABDCEF013C7360EF262DA94D0BB1 |
| SHA1: | 7886E7C0D416567109ED45A58EB4C63AEC4DA13D |
| SHA-256: | 5F82BCE7575218FED78D6771274A7CE3F2F9450019B37CA1A44043E2DE1B67AD |
| SHA-512: | 8291D7D23C35B5B0F5B6A61C70D230968DBD70E0E1700EBC282F4B3F5291DBC87FEB2363F03A2E152C70AC4ADF2691F1F493798A41BB960CD8A6D3EF3CC31B4 |
| Malicious: | false |
| Preview: | .....R.o.o.t. .E.n.t.r.y..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{BD6AF35E-DF4A-11EB-90E5-ECF4BB570DC9}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 27376 |
| Entropy (8bit): | 1.8498140810925014 |
| Encrypted: | false |
| SSDEEP: | 96:rnZfQj6tBSHjp2BWBMXa6lBlfcFXgxlBlfcFXAl4A:rnZfQj6tkHjp2BWBMXa6lzfHxlzfb4A |
| MD5: | E314AEEF8885724C4F91A74CBF288AAE |
| SHA1: | C299E34AFACD5E67A2748443AE4F3D71D1213174 |
| SHA-256: | 3DC9BB6E88346FF7285AA2B7BE18C8FA94331C42DD48253FBC3436DFB8BF4F00 |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{BD6AF35E-DF4A-11EB-90E5-ECF4BB570DC9}.dat | |
|---|---|
| SHA-512: | 5F8250CF15954ABC4BB60ACB1ACF7952D010260D8235530CE4EFD02F30391E33C9E2F50CB2997E1F86CD442A7F660D2FF01C482CEF93D11C50606E1598ECEC |
| Malicious: | false |
| Preview: | ..... ..... .....R.o.o.t. .E.n.t.r. y..... ..... |

| C:\Users\user\AppData\Local\Temp\JavaDeployReg.log | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | modified |
| Size (bytes): | 89 |
| Entropy (8bit): | 4.429518442893874 |
| Encrypted: | false |
| SSDEEP: | 3:oVXUdUbXIyB8JOGXnEdUbXIy6j+n:o9UVQqEVi |
| MD5: | 7551EDFC2A095038308DE03A979AEA3B |
| SHA1: | 28A3E4408ABBD841E14B80C82D712894D7480A73 |
| SHA-256: | FD0B2F23730CC3AAAFEB969CE5AFF07BAD4CA1EDA987671346FE6513CB7AFDD6 |
| SHA-512: | 96F41AF45753FAFA2DAA35022B02841153EE8C98894ED530A8F16C72B5FC7774FDEF2C0A8211843F4059E613087DB806F685CE058F6B9C782AAB30614607EA12 |
| Malicious: | false |
| Preview: | [2021/07/07 10:42:49.331] Latest deploy version: ..[2021/07/07 10:42:49.331] 11.211.2 .. |

| C:\Users\user\AppData\Local\Temp\~DF3A99C7AD2702480D.TMP | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 39649 |
| Entropy (8bit): | 0.5767042893555584 |
| Encrypted: | false |
| SSDEEP: | 96:kBqoxKAuvScS+NTRwzRlBlfcFX2lBlfcFX+lBlfcFX3:kBqoxKAuqR+NTRwzRlzfrlzf3lzf8 |
| MD5: | 5E4E8D633EEC37451CA584FB977CD2A3 |
| SHA1: | F2FDC159F116F1F666876081CD57C21FF4D6F629 |
| SHA-256: | 54912DA24BE3C7F0278AFF9A7FA3748F20BB70B7A444BB6D36219E8F5BAF910E |
| SHA-512: | 7E54E62E35EB7DF22657B5BD7374BF2634C9C0DBFFD8497175740591CB19AE20193A72555931D96A1B958AC9333606CE6D4A9264F4B10EC2A5DB786A015AF97 |
| Malicious: | false |
| Preview: | .....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ..... ..... ..... |

| C:\Users\user\AppData\Local\Temp\~DF48F8DB99852E5824.TMP | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 13237 |
| Entropy (8bit): | 0.6015770581866133 |
| Encrypted: | false |
| SSDEEP: | 24:c9lLh9lLh9lIn9lIn9lo59loZ9lWN5iG5PA:kBqoIC8N5iG5PA |
| MD5: | 48DB8549900DAE5BC2552D048ED02C3F |
| SHA1: | 6C535A402C05BF8FEFC3500973D9F4393FC67277 |
| SHA-256: | 3DB755B3A9C5F18FE0694056E963504C59603244F11C801A72991E62CA219BC6 |
| SHA-512: | 0792497457374046404D96816FCA01748D62D3CC87FA6E5AC22B3593D55E707E89A2EE3FEA72DC7C07A6ED6D27944FF062C781B334E06C7A871A88AFBF41889 |
| Malicious: | false |
| Preview: | .....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ..... ..... ..... |

| C:\Users\user\AppData\Local\Temp\~DFBADD8EC8FEBD51BA.TMP | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 39665 |
| Entropy (8bit): | 0.576637477758457 |

| C:\Users\user\AppData\Local\Temp\~DFBADD8EC8FEBD51BA.TMP | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 96:kBqoxKAuvScS+uoCLYewBSlHGd9uwBSlHGd9+wBSlHGd93:kBqoxKAuqR+uoCLYew2HK0w2HK0w2HK1 |
| MD5: | 3252CDAF94741DE42A0C2C0887F7B2AA |
| SHA1: | 917057587119E9A2610A30B1F1538C94B99E6179 |
| SHA-256: | DBDD2E68C5A55AD1E178E0860709F5D0AB2205E30D8D0FF184B95D39DD820087 |
| SHA-512: | 15321A223617B5C9296F57B79AAF13884F8427488F380BE084BA9A19BF9EBA0C4B0518D6D9F4D0B3EEE6C3FD31795D593F8DBD107ADB8C865CABA1F13C9B188<br>7 |
| Malicious: | false |
| Preview: | .....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....<br>.....<br>.....<br>..... |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed |
| Entropy (8bit): | 7.907972335888756 |
| TrID: | • Win32 Dynamic Link Library (generic) (1002004/3) 96.66%<br>• UPX compressed Win32 Executable (30571/9) 2.95%<br>• Generic Win/DOS Executable (2004/3) 0.19%<br>• DOS Executable Generic (2002/1) 0.19%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | 5.dll |
| File size: | 227342 |
| MD5: | fceb6a51be4205d11be1491f6e263cae |
| SHA1: | 0abb60d37fac49912172c5385ff58e049520eb53 |
| SHA256: | c521dd937ce9b2e8bda2fa915bae5b5be0e150a8b82e3b2bfb1cdbc60a8326c4 |
| SHA512: | 0dd278f5499a28f3ae536fd1870cbedbfb1da34f07d9210f09b86c5167d04be4f0eb1ffbcb922d3b01afe83cf9cd9f620e5c4abf0a27a569c954e6d7cc9451e7 |
| SSDEEP: | 3072:Ndmt0uTpBxy1mXhKvuE3GThWccntEvAJjHPLpvLHMwsJyV/vl5PX8J/g9vN:N85ykhKWE3UhwmMjjpvjMwskD5f8JsvN |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~@.....D.....Rich.....PE..L.....S... |

## File Icon

| | |
|---|---|
| Icon Hash: | 74f0e4ecccdce0e4 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x10facd0 |
| Entrypoint Section: | UPX1 |
| Digitally signed: | false |
| Imagebase: | 0x1000000 |
| Subsystem: | windows gui |
| Image File Characteristics: | 32BIT_MACHINE, EXECUTABLE_IMAGE, DLL |
| DLL Characteristics: | DYNAMIC_BASE, NX_COMPAT |
| Time Stamp: | 0x5396CBB2 [Tue Jun 10 09:11:14 2014 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| OS Version Major: | 6 |
| OS Version Minor: | 0 |

### General

| | |
|---|---|
| File Version Major: | 6 |
| File Version Minor: | 0 |
| Subsystem Version Major: | 6 |
| Subsystem Version Minor: | 0 |
| Import Hash: | ea5307b4a63215686c0cdc83cff5fcba |

### Entrypoint Preview

### Rich Headers

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| UPX0 | 0x1000 | 0xc3000 | 0x0 | False | 0 | empty | 0.0 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| UPX1 | 0xc4000 | 0x37000 | 0x37000 | False | 0.987744140625 | data | 7.91565633635 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0xfb000 | 0x1000 | 0x400 | False | 0.490234375 | data | 4.47756536718 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Exports

### Possible Origin

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

# Network Behavior

## Snort IDS Alerts

| Timestamp | Protocol | SID | Message | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|---|---|---|
| 07/07/21-10:42:51.274973 | TCP | 2033204 | ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) | 49721 | 80 | 192.168.2.5 | 40.97.116.82 |
| 07/07/21-10:42:51.274973 | TCP | 2033203 | ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) | 49721 | 80 | 192.168.2.5 | 40.97.116.82 |

## Network Port Distribution

### TCP Packets

### UDP Packets

### DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Jul 7, 2021 10:42:51.021521091 CEST | 192.168.2.5 | 8.8.8.8 | 0xed2a | Standard query (0) | outlook.com | A (IP address) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Jul 7, 2021 10:42:53.333837032 CEST | 192.168.2.5 | 8.8.8.8 | 0x696b | Standard query (0) | www.outlook.com | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:54.000277042 CEST | 192.168.2.5 | 8.8.8.8 | 0xf187 | Standard query (0) | outlook.office365.com | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:56.563894987 CEST | 192.168.2.5 | 8.8.8.8 | 0x2e0a | Standard query (0) | outlook.com | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:57.276827097 CEST | 192.168.2.5 | 8.8.8.8 | 0x6302 | Standard query (0) | www.outlook.com | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:57.526649952 CEST | 192.168.2.5 | 8.8.8.8 | 0x49fa | Standard query (0) | outlook.office365.com | A (IP address) | IN (0x0001) |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Jul 7, 2021 10:42:51.070379019 CEST | 8.8.8.8 | 192.168.2.5 | 0xed2a | No error (0) | outlook.com | | 40.97.116.82 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:51.070379019 CEST | 8.8.8.8 | 192.168.2.5 | 0xed2a | No error (0) | outlook.com | | 40.97.161.50 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:51.070379019 CEST | 8.8.8.8 | 192.168.2.5 | 0xed2a | No error (0) | outlook.com | | 40.97.160.2 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:51.070379019 CEST | 8.8.8.8 | 192.168.2.5 | 0xed2a | No error (0) | outlook.com | | 40.97.148.226 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:51.070379019 CEST | 8.8.8.8 | 192.168.2.5 | 0xed2a | No error (0) | outlook.com | | 40.97.164.146 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:51.070379019 CEST | 8.8.8.8 | 192.168.2.5 | 0xed2a | No error (0) | outlook.com | | 40.97.128.194 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:51.070379019 CEST | 8.8.8.8 | 192.168.2.5 | 0xed2a | No error (0) | outlook.com | | 40.97.156.114 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:51.070379019 CEST | 8.8.8.8 | 192.168.2.5 | 0xed2a | No error (0) | outlook.com | | 40.97.153.146 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:53.382605076 CEST | 8.8.8.8 | 192.168.2.5 | 0x696b | No error (0) | www.outlook.com | outlook.office365.com | | CNAME (Canonical name) | IN (0x0001) |
| Jul 7, 2021 10:42:53.382605076 CEST | 8.8.8.8 | 192.168.2.5 | 0x696b | No error (0) | outlook.office365.com | outlook.ha.office365.com | | CNAME (Canonical name) | IN (0x0001) |
| Jul 7, 2021 10:42:53.382605076 CEST | 8.8.8.8 | 192.168.2.5 | 0x696b | No error (0) | outlook.ha.office365.com | outlook.ms-acdc.office.com | | CNAME (Canonical name) | IN (0x0001) |
| Jul 7, 2021 10:42:53.382605076 CEST | 8.8.8.8 | 192.168.2.5 | 0x696b | No error (0) | outlook.ms-acdc.office.com | HHN-efz.ms-acdc.office.com | | CNAME (Canonical name) | IN (0x0001) |
| Jul 7, 2021 10:42:53.382605076 CEST | 8.8.8.8 | 192.168.2.5 | 0x696b | No error (0) | HHN-efz.ms-acdc.office.com | | 40.101.137.98 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:53.382605076 CEST | 8.8.8.8 | 192.168.2.5 | 0x696b | No error (0) | HHN-efz.ms-acdc.office.com | | 52.98.175.18 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:53.382605076 CEST | 8.8.8.8 | 192.168.2.5 | 0x696b | No error (0) | HHN-efz.ms-acdc.office.com | | 52.97.233.34 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:53.382605076 CEST | 8.8.8.8 | 192.168.2.5 | 0x696b | No error (0) | HHN-efz.ms-acdc.office.com | | 52.97.150.2 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:54.047828913 CEST | 8.8.8.8 | 192.168.2.5 | 0xf187 | No error (0) | outlook.office365.com | outlook.ha.office365.com | | CNAME (Canonical name) | IN (0x0001) |
| Jul 7, 2021 10:42:54.047828913 CEST | 8.8.8.8 | 192.168.2.5 | 0xf187 | No error (0) | outlook.ha.office365.com | outlook.ms-acdc.office.com | | CNAME (Canonical name) | IN (0x0001) |
| Jul 7, 2021 10:42:54.047828913 CEST | 8.8.8.8 | 192.168.2.5 | 0xf187 | No error (0) | outlook.ms-acdc.office.com | HHN-efz.ms-acdc.office.com | | CNAME (Canonical name) | IN (0x0001) |
| Jul 7, 2021 10:42:54.047828913 CEST | 8.8.8.8 | 192.168.2.5 | 0xf187 | No error (0) | HHN-efz.ms-acdc.office.com | | 52.97.233.2 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:54.047828913 CEST | 8.8.8.8 | 192.168.2.5 | 0xf187 | No error (0) | HHN-efz.ms-acdc.office.com | | 52.98.171.242 | A (IP address) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Jul 7, 2021 10:42:54.047828913 CEST | 8.8.8.8 | 192.168.2.5 | 0xf187 | No error (0) | HHN-efz.ms-acdc.office.com | | 52.98.151.226 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:54.047828913 CEST | 8.8.8.8 | 192.168.2.5 | 0xf187 | No error (0) | HHN-efz.ms-acdc.office.com | | 52.98.152.162 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:56.612906933 CEST | 8.8.8.8 | 192.168.2.5 | 0x2e0a | No error (0) | outlook.com | | 40.97.116.82 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:56.612906933 CEST | 8.8.8.8 | 192.168.2.5 | 0x2e0a | No error (0) | outlook.com | | 40.97.161.50 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:56.612906933 CEST | 8.8.8.8 | 192.168.2.5 | 0x2e0a | No error (0) | outlook.com | | 40.97.160.2 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:56.612906933 CEST | 8.8.8.8 | 192.168.2.5 | 0x2e0a | No error (0) | outlook.com | | 40.97.148.226 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:56.612906933 CEST | 8.8.8.8 | 192.168.2.5 | 0x2e0a | No error (0) | outlook.com | | 40.97.164.146 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:56.612906933 CEST | 8.8.8.8 | 192.168.2.5 | 0x2e0a | No error (0) | outlook.com | | 40.97.128.194 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:56.612906933 CEST | 8.8.8.8 | 192.168.2.5 | 0x2e0a | No error (0) | outlook.com | | 40.97.156.114 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:56.612906933 CEST | 8.8.8.8 | 192.168.2.5 | 0x2e0a | No error (0) | outlook.com | | 40.97.153.146 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:57.325242996 CEST | 8.8.8.8 | 192.168.2.5 | 0x6302 | No error (0) | www.outlook.com | outlook.office365.com | | CNAME (Canonical name) | IN (0x0001) |
| Jul 7, 2021 10:42:57.325242996 CEST | 8.8.8.8 | 192.168.2.5 | 0x6302 | No error (0) | outlook.office365.com | outlook.ha.office365.com | | CNAME (Canonical name) | IN (0x0001) |
| Jul 7, 2021 10:42:57.325242996 CEST | 8.8.8.8 | 192.168.2.5 | 0x6302 | No error (0) | outlook.ha.office365.com | outlook.ms-acdc.office.com | | CNAME (Canonical name) | IN (0x0001) |
| Jul 7, 2021 10:42:57.325242996 CEST | 8.8.8.8 | 192.168.2.5 | 0x6302 | No error (0) | outlook.ms-acdc.office.com | FRA-efz.ms-acdc.office.com | | CNAME (Canonical name) | IN (0x0001) |
| Jul 7, 2021 10:42:57.325242996 CEST | 8.8.8.8 | 192.168.2.5 | 0x6302 | No error (0) | FRA-efz.ms-acdc.office.com | | 52.97.152.210 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:57.325242996 CEST | 8.8.8.8 | 192.168.2.5 | 0x6302 | No error (0) | FRA-efz.ms-acdc.office.com | | 40.101.19.146 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:57.325242996 CEST | 8.8.8.8 | 192.168.2.5 | 0x6302 | No error (0) | FRA-efz.ms-acdc.office.com | | 40.101.83.194 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:57.574337959 CEST | 8.8.8.8 | 192.168.2.5 | 0x49fa | No error (0) | outlook.office365.com | outlook.ha.office365.com | | CNAME (Canonical name) | IN (0x0001) |
| Jul 7, 2021 10:42:57.574337959 CEST | 8.8.8.8 | 192.168.2.5 | 0x49fa | No error (0) | outlook.ha.office365.com | outlook.ms-acdc.office.com | | CNAME (Canonical name) | IN (0x0001) |
| Jul 7, 2021 10:42:57.574337959 CEST | 8.8.8.8 | 192.168.2.5 | 0x49fa | No error (0) | outlook.ms-acdc.office.com | FRA-efz.ms-acdc.office.com | | CNAME (Canonical name) | IN (0x0001) |
| Jul 7, 2021 10:42:57.574337959 CEST | 8.8.8.8 | 192.168.2.5 | 0x49fa | No error (0) | FRA-efz.ms-acdc.office.com | | 52.97.144.2 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:57.574337959 CEST | 8.8.8.8 | 192.168.2.5 | 0x49fa | No error (0) | FRA-efz.ms-acdc.office.com | | 52.97.163.2 | A (IP address) | IN (0x0001) |
| Jul 7, 2021 10:42:57.574337959 CEST | 8.8.8.8 | 192.168.2.5 | 0x49fa | No error (0) | FRA-efz.ms-acdc.office.com | | 52.97.188.66 | A (IP address) | IN (0x0001) |

## HTTP Request Dependency Graph

- outlook.com

### HTTP Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.5 | 49721 | 40.97.116.82 | 80 | C:\Program Files (x86)\Internet Explorer\iexplore.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jul 7, 2021 10:42:51.274972916 CEST | 1487 | OUT | GET /grower/b1FUosZSinX/D_2FTo28i4eES3/o1nX6HvoNr7JCqEB2TBDy/3reac2cOKkFxPa3C/uHqcEARrcPcZDk3/M6E_2BTZS_2BVaLqj4/34AYxwikF/REm_2FMb1QNTSjBFb_2F/tvRFv4olV4RM6PFjWcs/Yxi4zCvrQiijB3JFDfkmao/_2Ff4LrwOirbu/dGY1O2o_/2BPYCJyNgelsd4Jc6x2/N.grow HTTP/1.1<br>Accept: text/html, application/xhtml+xml, image/jxr, */*<br>Accept-Language: en-US<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Accept-Encoding: gzip, deflate<br>Host: outlook.com<br>Connection: Keep-Alive |
| Jul 7, 2021 10:42:51.455990076 CEST | 1488 | IN | HTTP/1.1 301 Moved Permanently<br>Cache-Control: no-cache<br>Pragma: no-cache<br>Location: https://outlook.com/grower/b1FUosZSinX/D_2FTo28i4eES3/o1nX6HvoNr7JCqEB2TBDy/3reac2cOKkFxPa3C/uHqcEARrcPcZDk3/M6E_2BTZS_2BVaLqj4/34AYxwikF/REm_2FMb1QNTSjBFb_2F/tvRFv4olV4RM6PFjWcs/Yxi4zCvrQiijB3JFDfkmao/_2Ff4LrwOirbu/dGY1O2o_/2BPYCJyNgelsd4Jc6x2/N.grow<br>Server: Microsoft-IIS/10.0<br>request-id: 52e0a7cb-8602-91df-81c1-2dcb70efe4dd<br>X-FEServer: MWHPR13CA0006<br>X-RequestId: 2526dedc-1dff-46a1-8916-d76af6eb2525<br>X-Powered-By: ASP.NET<br>X-FEServer: MWHPR13CA0006<br>Date: Wed, 07 Jul 2021 08:42:51 GMT<br>Connection: close<br>Content-Length: 0 |

## Code Manipulations

## Statistics

### Behavior

Click to jump to process

## System Behavior

### Analysis Process: loaddll32.exe PID: 2248 Parent PID: 5648

#### General

| | |
|---|---|
| Start time: | 10:41:12 |
| Start date: | 07/07/2021 |
| Path: | C:\Windows\System32\loaddll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | loaddll32.exe 'C:\Users\user\Desktop\5.dll' |
| Imagebase: | 0x1170000 |
| File size: | 116736 bytes |
| MD5 hash: | 542795ADF7CC08EFCF675D65310596E8 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

| | |
|---|---|
| Yara matches: | • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.496928044.0000000003328000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.445570350.0000000003328000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.445487547.0000000003328000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.445636875.0000000003328000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.445602533.0000000003328000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.445524931.0000000003328000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.445456909.0000000003328000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.445424230.0000000003328000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.445650161.0000000003328000.00000004.00000040.sdmp, Author: Joe Security |
| Reputation: | high |

**File Activities** Show Windows behavior

## Analysis Process: cmd.exe PID: 5484 Parent PID: 2248

### General

| | |
|---|---|
| Start time: | 10:41:12 |
| Start date: | 07/07/2021 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\5.dll',#1 |
| 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** Show Windows behavior

## Analysis Process: rundll32.exe PID: 1716 Parent PID: 2248

### General

| | |
|---|---|
| Start time: | 10:41:13 |
| Start date: | 07/07/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\5.dll,Clockcondition |
| Imagebase: | 0x960000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## File Activities

Show Windows behavior

## Analysis Process: rundll32.exe PID: 452 Parent PID: 5484

### General

| | |
|---|---|
| Start time: | 10:41:13 |
| Start date: | 07/07/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe 'C:\Users\user\Desktop\5.dll',#1 |
| Imagebase: | 0x960000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.451946137.0000000004D18000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.452051043.0000000004D18000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.452023874.0000000004D18000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.452000205.0000000004D18000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.451869538.0000000004D18000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.452038744.0000000004D18000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.498068878.0000000004D18000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.451977445.0000000004D18000.00000004.00000040.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.451921011.0000000004D18000.00000004.00000040.sdmp, Author: Joe Security |
| Reputation: | high |

## File Activities

Show Windows behavior

## Analysis Process: rundll32.exe PID: 2940 Parent PID: 2248

### General

| | |
|---|---|
| Start time: | 10:41:17 |
| Start date: | 07/07/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\5.dll,Dogwhen |
| Imagebase: | 0x960000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## File Activities

Show Windows behavior

## Analysis Process: rundll32.exe PID: 3904 Parent PID: 2248

### General

| | |
|---|---|
| Start time: | 10:41:23 |
| Start date: | 07/07/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\5.dll,Sing |
| Imagebase: | 0x960000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

Show Windows behavior

## Analysis Process: rundll32.exe PID: 5580 Parent PID: 2248

### General

| | |
|---|---|
| Start time: | 10:41:28 |
| Start date: | 07/07/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\5.dll,Wholegray |
| Imagebase: | 0x960000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

Show Windows behavior

## Analysis Process: iexplore.exe PID: 1900 Parent PID: 792

### General

| | |
|---|---|
| Start time: | 10:42:47 |
| Start date: | 07/07/2021 |
| Path: | C:\Program Files\internet explorer\iexplore.exe |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding |
| Imagebase: | 0x7ff762e70000 |
| File size: | 823560 bytes |
| MD5 hash: | 6465CB92B25A7BC1DF8E01D8AC5E7596 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

Show Windows behavior

Registry Activities — Show Windows behavior

## Analysis Process: iexplore.exe PID: 3220 Parent PID: 1900

### General

| | |
|---|---|
| Start time: | 10:42:48 |
| Start date: | 07/07/2021 |
| Path: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1900 CREDAT:17410 /prefetch:2 |
| Imagebase: | 0xf40000 |
| File size: | 822536 bytes |
| MD5 hash: | 071277CC2E3DF41EEEA8013E2AB58D5A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

File Activities — Show Windows behavior

## Analysis Process: iexplore.exe PID: 5264 Parent PID: 1900

### General

| | |
|---|---|
| Start time: | 10:42:53 |
| Start date: | 07/07/2021 |
| Path: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1900 CREDAT:17418 /prefetch:2 |
| Imagebase: | 0xf40000 |
| File size: | 822536 bytes |
| MD5 hash: | 071277CC2E3DF41EEEA8013E2AB58D5A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

File Activities — Show Windows behavior

# Disassembly

## Code Analysis