


**ID:** 532429
**Sample Name:** UioA2E9DBG.dll
**Cookbook:** default.jbs
**Time:** 09:31:02
**Date:** 02/12/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents

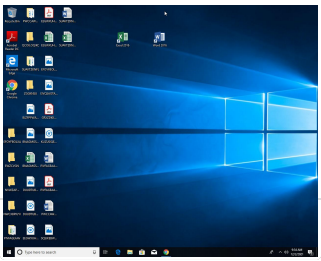
# Windows Analysis Report UioA2E9DBG.dll

## Overview

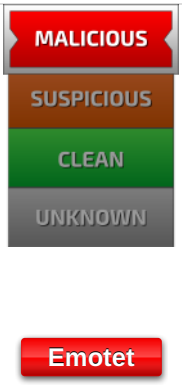
### General Information

| | |
|---|---|
| Sample Name: | UioA2E9DBG.dll |
| Analysis ID: | 532429 |
| MD5: | 6988533cf7cbdcc.. |
| SHA1: | 27836d3e04a315.. |
| SHA256: | 8d6912a12fdccb3.. |
| Tags: | 32 dll exe |
| Infos: | |

Most interesting Screenshot:



### Detection



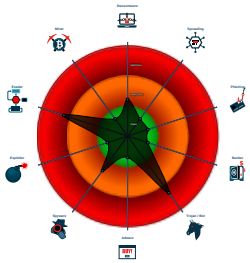

Emotet

| | |
|---|---|
| Score: | 76 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Found malware configuration
- Yara detected Emotet
- Multi AV Scanner detection for subm…
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Creates a DirectInput object (often fo…
- Uses 32bit PE files
- Sample file is different than original …
- PE file contains an invalid checksum
- Contains functionality to check if a d…
- Contains functionality to query locale…

### Classification



## Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 4828 cmdline: loaddll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 7044 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 7148 cmdline: rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6704 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7120 cmdline: rundll32.exe C:\Users\user\Desktop\UioA2E9DBG.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6856 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Uteaesuoyewsu\kffdjmqicgbnmom.ioj",ArlfCURNcI MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4752 cmdline: rundll32.exe C:\Users\user\Desktop\UioA2E9DBG.dll,agrwqhxohbh MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 3880 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5760 cmdline: rundll32.exe C:\Users\user\Desktop\UioA2E9DBG.dll,aoydsyidkopcdbcv MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 4436 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2944 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 4972 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

## Malware Configuration

### Threatname: Emotet

```
{
  "C2 list": [
    "46.55.222.11:443",
    "104.245.52.73:8080",
    "41.76.108.46:8080",
    "103.8.26.103:8080",
    "185.184.25.237:8080",
    "103.8.26.102:8080",
    "203.114.109.124:443",
    "45.118.115.99:8080",
    "178.79.147.66:8080",
    "58.227.42.236:80",
    "45.118.135.203:7080",
    "103.75.201.2:443",
    "195.154.133.20:443",
    "45.142.114.231:8080",
    "212.237.5.209:443",
    "207.38.84.195:8080",
    "104.251.214.46:8080",
    "212.237.17.99:8080",
    "212.237.56.116:7080",
    "216.158.226.206:443",
    "110.232.117.186:8080",
    "158.69.222.101:443",
    "107.182.225.142:8080",
    "176.104.106.96:8080",
    "81.0.236.90:443",
    "50.116.54.215:443",
    "138.185.72.26:8080",
    "51.68.175.8:8080",
    "210.57.217.132:8080"
  ],
  "Public Key": [
    "RUNTMSAAAABAX3S2xNjcDD0fBno33Ln5t71eii+mofIPoXkNFOX1MeiwCh48iz97kB0mJjGGZXwardnDXKxI8GCHGNl0PFj5",
    "RUNLMSAAAADzozW1Di4r9DVWzQpMKT588RDdy7BPILP6AiDOTLYMHkSWvrQO5slbmr1OvZ2Pz+AQWzRMggQmAtO6rPH7nyx2"
  ]
}
```


# Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000005.00000002.626711178.0000000002ADA000.00000004.00000020.sdmp | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| 00000005.00000002.626631642.0000000002790000.00000040.00000010.sdmp | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| 00000000.00000002.627609391.0000000000A8B000.00000004.00000020.sdmp | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| 00000002.00000002.625242397.0000000002E96000.00000004.00000020.sdmp | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| 00000003.00000002.609722465.0000000002875000.00000004.00000020.sdmp | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| Click to see the 5 entries | | | | |

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 4.2.rundll32.exe.3084270.1.unpack | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| 0.2.loaddll32.exe.aaeef0.1.unpack | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| 3.2.rundll32.exe.27a0000.0.raw.unpack | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| 2.2.rundll32.exe.2cc0000.0.unpack | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| 5.2.rundll32.exe.2790000.0.raw.unpack | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| Click to see the 11 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**

## Networking:

**C2 URLs / IPs found in malware configuration**

## E-Banking Fraud:

**Yara detected Emotet**

## Hooking and other Techniques for Hiding and Protection:

**Hides that the sample has been downloaded from the Internet (zone.identifier)**

## Malware Analysis System Evasion:

**Tries to detect virtualization through RDTSC time measurements**

## Stealing of Sensitive Information:

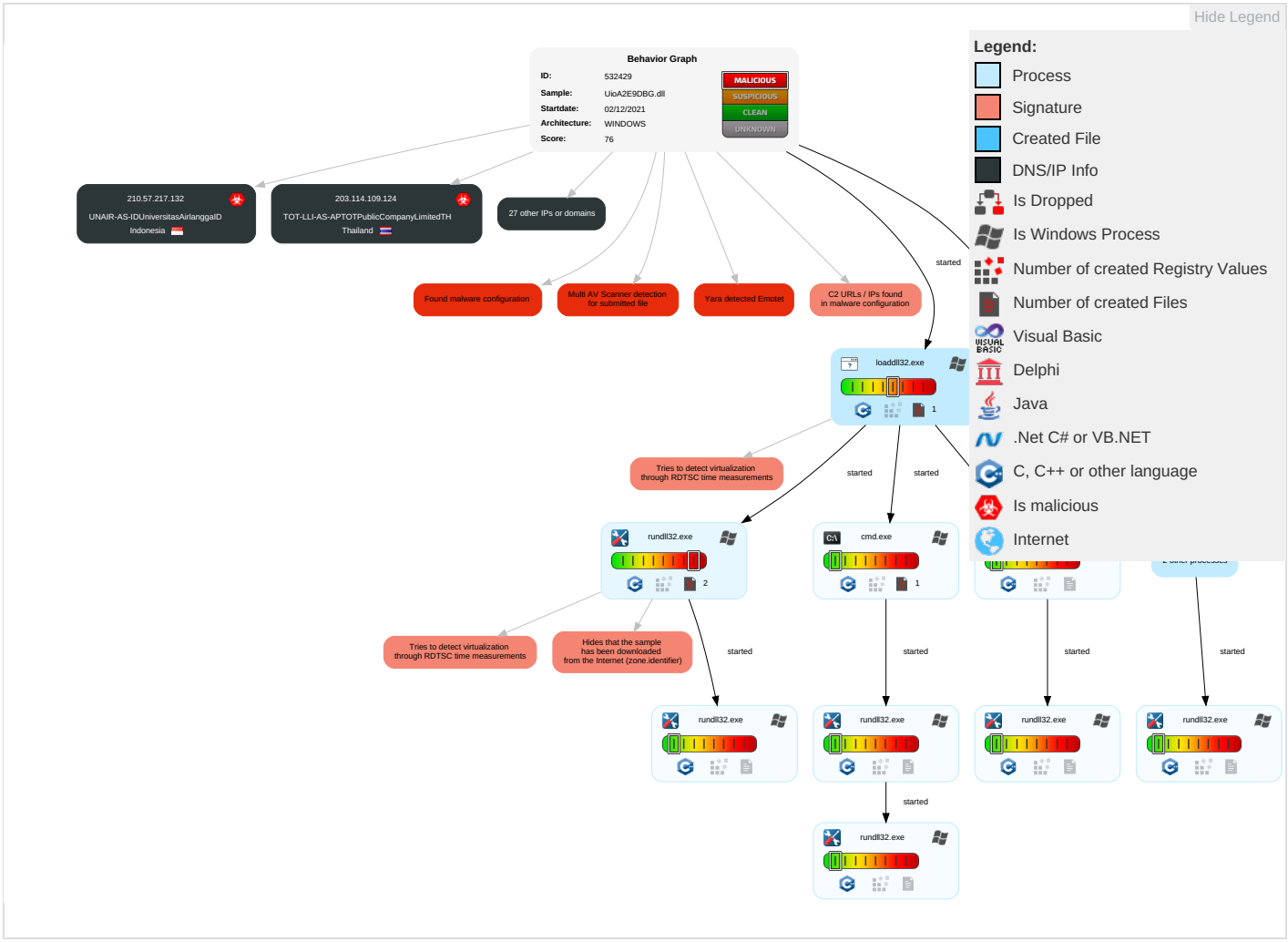
**Yara detected Emotet**

# Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | F S E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation | Path Interception | Process Injection 1 2 | Masquerading 2 | Input Capture 1 | System Time Discovery 1 | Remote Services | Input Capture 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eavesdrop on Insecure Network Communication | F T V A |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Process Injection 1 2 | LSASS Memory | Security Software Discovery 1 3 | Remote Desktop Protocol | Archive Collected Data 1 | Exfiltration Over Bluetooth | Application Layer Protocol 1 | Exploit SS7 to Redirect Phone Calls/SMS | F V A |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Deobfuscate/Decode Files or Information 1 | Security Account Manager | Process Discovery 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Steganography | Exploit SS7 to Track Device Location | C D C E |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Hidden Files and Directories 1 | NTDS | File and Directory Discovery 2 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Obfuscated Files or Information 2 | LSA Secrets | System Information Discovery 1 2 3 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication | |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Rundll32 1 | Cached Domain Credentials | System Owner/User Discovery | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service | |

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | F S E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| External Remote Services | Scheduled Task | Startup Items | Startup Items | File Deletion 1 | DCSync | Network Sniffing | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port | Rogue Wi-Fi Access Points | |

## 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 |
|---|---|---|---|---|
| UioA2E9DBG.dll | 23% | Virustotal | | Browse |
| UioA2E9DBG.dll | 30% | ReversingLabs | Win32.Trojan.Fragtor | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 0.2.loaddll32.exe.830000.0.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |
| 4.2.rundll32.exe.2db0000.0.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |
| 2.2.rundll32.exe.2cc0000.0.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |
| 5.2.rundll32.exe.2790000.0.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |
| 3.2.rundll32.exe.27a0000.0.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |

### Domains

No Antivirus matches

### URLs

No Antivirus matches

# Domains and IPs

## Contacted Domains

No contacted domains info

## Contacted IPs

### Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 195.154.133.20 | unknown | France | | 12876 | OnlineSASFR | true |
| 212.237.17.99 | unknown | Italy | | 31034 | ARUBA-ASNIT | true |
| 110.232.117.186 | unknown | Australia | | 56038 | RACKCORP-APRackCorpAU | true |
| 104.245.52.73 | unknown | United States | | 63251 | METRO-WIRELESSUS | true |
| 138.185.72.26 | unknown | Brazil | | 264343 | EmpasoftLtdaMeBR | true |
| 81.0.236.90 | unknown | Czech Republic | | 15685 | CASABLANCA-ASInternetCollocationProviderCZ | true |
| 45.118.115.99 | unknown | Indonesia | | 131717 | IDNIC-CIFO-AS-IDPTCitraJelajahInformatikalD | true |
| 103.75.201.2 | unknown | Thailand | | 133496 | CDNPLUSCOLTD-AS-APCDNPLUSCOLTDTH | true |
| 216.158.226.206 | unknown | United States | | 19318 | IS-AS-1US | true |
| 107.182.225.142 | unknown | United States | | 32780 | HOSTINGSERVICES-INCUS | true |
| 45.118.135.203 | unknown | Japan | | 63949 | LINODE-APLinodeLLCUS | true |
| 50.116.54.215 | unknown | United States | | 63949 | LINODE-APLinodeLLCUS | true |
| 51.68.175.8 | unknown | France | | 16276 | OVHFR | true |
| 103.8.26.102 | unknown | Malaysia | | 132241 | SKSATECH1-MYSKSATECHNOLOGYSDNBHDMY | true |
| 46.55.222.11 | unknown | Bulgaria | | 34841 | BALCHIKNETBG | true |
| 41.76.108.46 | unknown | South Africa | | 327979 | DIAMATRIXZA | true |
| 103.8.26.103 | unknown | Malaysia | | 132241 | SKSATECH1-MYSKSATECHNOLOGYSDNBHDMY | true |
| 178.79.147.66 | unknown | United Kingdom | | 63949 | LINODE-APLinodeLLCUS | true |
| 212.237.5.209 | unknown | Italy | | 31034 | ARUBA-ASNIT | true |
| 176.104.106.96 | unknown | Serbia | | 198371 | NINETRS | true |
| 207.38.84.195 | unknown | United States | | 30083 | AS-30083-GO-DADDY-COM-LLCUS | true |
| 212.237.56.116 | unknown | Italy | | 31034 | ARUBA-ASNIT | true |
| 45.142.114.231 | unknown | Germany | | 44066 | DE-FIRSTCOLOwwwfirst-colonetDE | true |
| 203.114.109.124 | unknown | Thailand | | 131293 | TOT-LLI-AS-APTOTPublicCompanyLimitedTH | true |
| 210.57.217.132 | unknown | Indonesia | | 38142 | UNAIR-AS-IDUniversitasAirlanggaID | true |
| 58.227.42.236 | unknown | Korea Republic of | | 9318 | SKB-ASSKBroadbandCoLtdKR | true |
| 185.184.25.237 | unknown | Turkey | | 209711 | MUVHOSTTR | true |
| 158.69.222.101 | unknown | Canada | | 16276 | OVHFR | true |
| 104.251.214.46 | unknown | United States | | 54540 | INCERO-HVVCUS | true |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 532429 |
| Start date: | 02.12.2021 |
| Start time: | 09:31:02 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 9m 25s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | UioA2E9DBG.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 |
| Run name: | Run with higher sleep bypass |
| Number of analysed new started processes analysed: | 16 |
| 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: | mal76.troj.evad.winDLL@22/0@0/29 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 14.1% (good quality ratio 13.5%)<br>• Quality average: 71.8%<br>• Quality standard deviation: 25.2% |
| HCA Information: | • Successful, ratio: 70%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Sleeps bigger than 120000ms are automatically reduced to 1000ms<br>• Found application associated with file extension: .dll |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

**No simulations**

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 195.154.133.20 | 916Q89rlYD.dll | Get hash | malicious | Browse | |
| | 9izNuvE61W.dll | Get hash | malicious | Browse | |
| | P5LROPCURK.dll | Get hash | malicious | Browse | |
| | TYLNb8VvnmYA.dll | Get hash | malicious | Browse | |
| | TYLNb8VvnmYA.dll | Get hash | malicious | Browse | |
| | snBYiBAMB2.dll | Get hash | malicious | Browse | |
| | 6zAcNlJXo7.dll | Get hash | malicious | Browse | |
| | 6zAcNlJXo7.dll | Get hash | malicious | Browse | |
| | mal.dll | Get hash | malicious | Browse | |
| | mal2.dll | Get hash | malicious | Browse | |
| | mal.dll | Get hash | malicious | Browse | |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | mal2.dll | Get hash | malicious | Browse | |
| | 2gyA5uNl6VPQUA.dll | Get hash | malicious | Browse | |
| | 2gyA5uNl6VPQUA.dll | Get hash | malicious | Browse | |
| | 9sQccNfqAR.dll | Get hash | malicious | Browse | |
| | FILE_464863409880121918.xlsm | Get hash | malicious | Browse | |
| | 9sQccNfqAR.dll | Get hash | malicious | Browse | |
| | t3XtgyQEoe.dll | Get hash | malicious | Browse | |
| | t3XtgyQEoe.dll | Get hash | malicious | Browse | |
| 212.237.17.99 | UioA2E9DBG.dll | Get hash | malicious | Browse | |
| | 916Q89rlYD.dll | Get hash | malicious | Browse | |
| | 9izNuvE61W.dll | Get hash | malicious | Browse | |
| | P5LROPCURK.dll | Get hash | malicious | Browse | |
| | TYLNb8VvnmYA.dll | Get hash | malicious | Browse | |
| | TYLNb8VvnmYA.dll | Get hash | malicious | Browse | |
| | snBYiBAMB2.dll | Get hash | malicious | Browse | |
| | 6zAcNlJXo7.dll | Get hash | malicious | Browse | |
| | 6zAcNlJXo7.dll | Get hash | malicious | Browse | |
| | mal.dll | Get hash | malicious | Browse | |
| | mal2.dll | Get hash | malicious | Browse | |
| | mal.dll | Get hash | malicious | Browse | |
| | mal2.dll | Get hash | malicious | Browse | |
| | 2gyA5uNl6VPQUA.dll | Get hash | malicious | Browse | |
| | 2gyA5uNl6VPQUA.dll | Get hash | malicious | Browse | |
| | 9sQccNfqAR.dll | Get hash | malicious | Browse | |
| | FILE_464863409880121918.xlsm | Get hash | malicious | Browse | |
| | 9sQccNfqAR.dll | Get hash | malicious | Browse | |
| | t3XtgyQEoe.dll | Get hash | malicious | Browse | |
| | t3XtgyQEoe.dll | Get hash | malicious | Browse | |

## Domains

**No context**

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| ARUBA-ASNIT | UioA2E9DBG.dll | Get hash | malicious | Browse | • 212.237.56.116 |
| | 916Q89rlYD.dll | Get hash | malicious | Browse | • 212.237.56.116 |
| | 9izNuvE61W.dll | Get hash | malicious | Browse | • 212.237.56.116 |
| | P5LROPCURK.dll | Get hash | malicious | Browse | • 212.237.56.116 |
| | zTGtLv4pTO.dll | Get hash | malicious | Browse | • 94.177.217.88 |
| | zTGtLv4pTO.dll | Get hash | malicious | Browse | • 94.177.217.88 |
| | TYLNb8VvnmYA.dll | Get hash | malicious | Browse | • 212.237.56.116 |
| | TYLNb8VvnmYA.dll | Get hash | malicious | Browse | • 212.237.56.116 |
| | snBYiBAMB2.dll | Get hash | malicious | Browse | • 212.237.56.116 |
| | 6zAcNlJXo7.dll | Get hash | malicious | Browse | • 212.237.56.116 |
| | 6zAcNlJXo7.dll | Get hash | malicious | Browse | • 212.237.56.116 |
| | DHL DOCUMENT FOR #504.exe | Get hash | malicious | Browse | • 62.149.128.40 |
| | RqgAGRvHNwhoreniggagay.dll | Get hash | malicious | Browse | • 94.177.217.88 |
| | RqgAGRvHNwhoreniggagay.dll | Get hash | malicious | Browse | • 94.177.217.88 |
| | dFUOuTxFQrXAwhoreniggagay.dll | Get hash | malicious | Browse | • 94.177.217.88 |
| | RbrKCqqjDPUwhoreniggagay.dll | Get hash | malicious | Browse | • 94.177.217.88 |
| | dFUOuTxFQrXAwhoreniggagay.dll | Get hash | malicious | Browse | • 94.177.217.88 |
| | RbrKCqqjDPUwhoreniggagay.dll | Get hash | malicious | Browse | • 94.177.217.88 |
| | mal.dll | Get hash | malicious | Browse | • 212.237.56.116 |
| | mal2.dll | Get hash | malicious | Browse | • 212.237.56.116 |
| OnlineSASFR | UioA2E9DBG.dll | Get hash | malicious | Browse | • 195.154.133.20 |
| | 916Q89rlYD.dll | Get hash | malicious | Browse | • 195.154.133.20 |
| | 9izNuvE61W.dll | Get hash | malicious | Browse | • 195.154.133.20 |
| | P5LROPCURK.dll | Get hash | malicious | Browse | • 195.154.133.20 |
| | GlobalfoundriesINV33-45776648.htm | Get hash | malicious | Browse | • 51.15.17.195 |
| | TYLNb8VvnmYA.dll | Get hash | malicious | Browse | • 195.154.133.20 |
| | TYLNb8VvnmYA.dll | Get hash | malicious | Browse | • 195.154.133.20 |
| | snBYiBAMB2.dll | Get hash | malicious | Browse | • 195.154.133.20 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | 6zAcNlJXo7.dll | Get hash | malicious | Browse | • 195.154.133.20 |
| | 6zAcNlJXo7.dll | Get hash | malicious | Browse | • 195.154.133.20 |
| | mal.dll | Get hash | malicious | Browse | • 195.154.133.20 |
| | mal2.dll | Get hash | malicious | Browse | • 195.154.133.20 |
| | mal.dll | Get hash | malicious | Browse | • 195.154.133.20 |
| | mal2.dll | Get hash | malicious | Browse | • 195.154.133.20 |
| | 2gyA5uNl6VPQUA.dll | Get hash | malicious | Browse | • 195.154.133.20 |
| | 2gyA5uNl6VPQUA.dll | Get hash | malicious | Browse | • 195.154.133.20 |
| | spZRMihlrkFGqYq1f.dll | Get hash | malicious | Browse | • 195.154.146.35 |
| | spZRMihlrkFGqYq1f.dll | Get hash | malicious | Browse | • 195.154.146.35 |
| | AtlanticareINV25-67431254.htm | Get hash | malicious | Browse | • 51.15.17.195 |
| | 9sQccNfqAR.dll | Get hash | malicious | Browse | • 195.154.133.20 |

### JA3 Fingerprints

**No context**

### Dropped Files

**No context**

## Created / dropped Files

**No created / dropped files found**

## Static File Info

### General

| | |
|---|---|
| File type: | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| Entropy (8bit): | 7.196240298834973 |
| TrID: | • Win32 Dynamic Link Library (generic) (1002004/3) 99.60%<br>• Generic Win/DOS Executable (2004/3) 0.20%<br>• DOS Executable Generic (2002/1) 0.20%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | UioA2E9DBG.dll |
| File size: | 473600 |
| MD5: | 6988533cf7cbdccd0ea429571e0441a9 |
| SHA1: | 27836d3e04a31548fa09ec8537ba50777a73a42a |
| SHA256: | 8d6912a12fdccb3d6d55980c3b1fd20cc97a2736d3381e315657a3d6f2f8d1b3 |
| SHA512: | 2d48c1b8ef38ad9d0a68650896b5ee69bdcea2caeddfe5e8cadd7b5f411311a8a43a09ce33ca5d6b5e341f38f30fbe41a0aa91048a8b2c5a2a663013f8b1e40 |
| SSDEEP: | 12288:mFyGBDytNZAR5Myju+qQuj/J+7C6Dg8stHb1h:mF92e/jEk7zDg8stJh |
| File Content Preview: | MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....A~.. ... ... ...F... ...F..D ...U... ...U... ...U... ...F... ...F... ...F... ... ..< ..TU... ..TU... ..TU... ... ... ..TU... . |

### File Icon

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

### Static PE Info

## General

| | |
|---|---|
| Entrypoint: | 0x10014c2e |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x10000000 |
| Subsystem: | windows gui |
| Image File Characteristics: | 32BIT_MACHINE, EXECUTABLE_IMAGE, DLL |
| DLL Characteristics: | DYNAMIC_BASE, NX_COMPAT |
| Time Stamp: | 0x61A7B2E7 [Wed Dec 1 17:37:43 2021 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| OS Version Major: | 6 |
| OS Version Minor: | 0 |
| File Version Major: | 6 |
| File Version Minor: | 0 |
| Subsystem Version Major: | 6 |
| Subsystem Version Minor: | 0 |
| Import Hash: | 057d91f9747659ff50a0558e0aed5a44 |

## Entrypoint Preview

## Data Directories

## Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x385cc | 0x38600 | False | 0.542072304601 | data | 6.65370681685 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rdata | 0x3a000 | 0x12520 | 0x12600 | False | 0.497967155612 | data | 5.51962067899 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0x4d000 | 0x23d4 | 0x1600 | False | 0.2265625 | data | 3.93138515856 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x50000 | 0x24448 | 0x24600 | False | 0.788874570447 | data | 7.67571153778 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0x75000 | 0x2d78 | 0x2e00 | False | 0.740913722826 | data | 6.57934659057 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

## Resources

## Imports

## Exports

## Version Infos

## Possible Origin

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

# Network Behavior

**No network behavior found**

# Code Manipulations

# Statistics

## Behavior

Click to jump to process

# System Behavior

## Analysis Process: loaddll32.exe PID: 4828 Parent PID: 5688

### General

| | |
|---|---|
| Start time: | 09:31:58 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\System32\loaddll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | loaddll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll" |
| Imagebase: | 0x120000 |
| File size: | 893440 bytes |
| MD5 hash: | 72FCD8FB0ADC38ED9050569AD673650E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.627609391.0000000000A8B000.00000004.00000020.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.627509669.0000000000830000.00000040.00000010.sdmp, Author: Joe Security |
| Reputation: | high |

### File Activities

Show Windows behavior

## Analysis Process: cmd.exe PID: 7044 Parent PID: 4828

### General

| | |
|---|---|
| Start time: | 09:31:58 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | cmd.exe /C rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",#1 |
| Imagebase: | 0xd80000 |
| 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: 7120 Parent PID: 4828

### General

| | |
|---|---|
| Start time: | 09:31:58 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\UioA2E9DBG.dll,Control_RunDLL |
| Imagebase: | 0x370000 |
| 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_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.625242397.0000000002E96000.00000004.00000020.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.625153138.0000000002CC0000.00000040.00000010.sdmp, Author: Joe Security |
| Reputation: | high |

### File Activities

Show Windows behavior

## Analysis Process: rundll32.exe PID: 7148 Parent PID: 7044

### General

| | |
|---|---|
| Start time: | 09:31:58 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",#1 |
| Imagebase: | 0x370000 |
| 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_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.609722465.0000000002875000.00000004.00000020.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.609690193.00000000027A0000.00000040.00000010.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: 4752 Parent PID: 4828

### General

| | |
|---|---|
| Start time: | 09:32:03 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\UioA2E9DBG.dll,agrwqhxohbh |
| Imagebase: | 0x370000 |
| 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_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.611321700.000000000306A000.00000004.00000020.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.611275948.0000000002DB0000.00000040.00000010.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: 5760 Parent PID: 4828

### General

| | |
|---|---|
| Start time: | 09:32:10 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\UioA2E9DBG.dll,aoydsyidkopcdbcv |
| Imagebase: | 0x370000 |
| 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_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.626711178.0000000002ADA000.00000004.00000020.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.626631642.0000000002790000.00000040.00000010.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: 6704 Parent PID: 7148

### General

| | |
|---|---|
| Start time: | 09:34:16 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",Control_RunDLL |
| Imagebase: | 0x370000 |
| 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: 6856 Parent PID: 7120

### General

| | |
|---|---|
| Start time: | 09:34:17 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |

| | |
|---|---|
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Uteaesuoyewsu\kffdjmqicgbnmom.ioj",ArlfCURNcI |
| Imagebase: | 0x370000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: 3880 Parent PID: 4752

### General

| | |
|---|---|
| Start time: | 09:34:28 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",Control_RunDLL |
| Imagebase: | 0x370000 |
| 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: 4436 Parent PID: 5760

### General

| | |
|---|---|
| Start time: | 09:34:35 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",Control_RunDLL |
| Imagebase: | 0x370000 |
| 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: 2944 Parent PID: 4828

### General

| | |
|---|---|
| Start time: | 09:34:36 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |

| | |
|---|---|
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\UioA2E9DBG.dll",Control_RunDLL |
| Imagebase: | 0x370000 |
| 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: svchost.exe PID: 4972 Parent PID: 572

### General

| | |
|---|---|
| Start time: | 09:34:38 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\System32\svchost.exe -k netsvcs -p |
| Imagebase: | 0x7ff70d6e0000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| 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