

JOeSandbox Cloud BASIC



**ID:** 620140

**Sample Name:**

62724e14c3203.dll

**Cookbook:** default.jbs

**Time:** 12:06:42

**Date:** 04/05/2022

**Version:** 34.0.0 Boulder Opal

# Table of Contents

|                                                           |    |
|-----------------------------------------------------------|----|
| Table of Contents                                         | 2  |
| Windows Analysis Report 62724e14c3203.dll                 | 4  |
| Overview                                                  | 4  |
| General Information                                       | 4  |
| Detection                                                 | 4  |
| Signatures                                                | 4  |
| Classification                                            | 4  |
| Process Tree                                              | 4  |
| Malware Configuration                                     | 4  |
| Yara Signatures                                           | 4  |
| Initial Sample                                            | 4  |
| Sigma Signatures                                          | 4  |
| Snort Signatures                                          | 5  |
| Joe Sandbox Signatures                                    | 5  |
| AV Detection                                              | 5  |
| Key, Mouse, Clipboard, Microphone and Screen Capturing    | 5  |
| E-Banking Fraud                                           | 5  |
| Hooking and other Techniques for Hiding and Protection    | 5  |
| Malware Analysis System Evasion                           | 5  |
| Anti Debugging                                            | 5  |
| Stealing of Sensitive Information                         | 5  |
| Remote Access Functionality                               | 5  |
| Mitre Att&ck Matrix                                       | 5  |
| Behavior Graph                                            | 6  |
| Screenshots                                               | 6  |
| Thumbnails                                                | 6  |
| Antivirus, Machine Learning and Genetic Malware Detection | 7  |
| Initial Sample                                            | 7  |
| Dropped Files                                             | 8  |
| Unpacked PE Files                                         | 8  |
| Domains                                                   | 8  |
| URLs                                                      | 8  |
| Domains and IPs                                           | 8  |
| Contacted Domains                                         | 8  |
| URLs from Memory and Binaries                             | 8  |
| World Map of Contacted IPs                                | 8  |
| General Information                                       | 8  |
| Warnings                                                  | 9  |
| Simulations                                               | 9  |
| Behavior and APIs                                         | 9  |
| Joe Sandbox View / Context                                | 9  |
| IPs                                                       | 9  |
| Domains                                                   | 9  |
| ASNs                                                      | 9  |
| JA3 Fingerprints                                          | 9  |
| Dropped Files                                             | 9  |
| Created / dropped Files                                   | 10 |
| Static File Info                                          | 10 |
| General                                                   | 10 |
| File Icon                                                 | 10 |
| Static PE Info                                            | 10 |
| General                                                   | 10 |
| Entrypoint Preview                                        | 10 |
| Rich Headers                                              | 12 |
| Data Directories                                          | 12 |
| Sections                                                  | 12 |
| Imports                                                   | 13 |
| Exports                                                   | 13 |
| Network Behavior                                          | 13 |
| Statistics                                                | 13 |
| Behavior                                                  | 13 |
| System Behavior                                           | 13 |
| Analysis Process: loadll32.exePID: 1560, Parent PID: 3892 | 13 |
| General                                                   | 14 |
| File Activities                                           | 14 |
| Analysis Process: cmd.exePID: 4392, Parent PID: 1560      | 14 |
| General                                                   | 14 |
| File Activities                                           | 14 |
| Analysis Process: regsvr32.exePID: 5616, Parent PID: 1560 | 14 |
| General                                                   | 14 |
| Analysis Process: rundll32.exePID: 5244, Parent PID: 4392 | 15 |
| General                                                   | 15 |
| Analysis Process: rundll32.exePID: 5016, Parent PID: 1560 | 15 |
| General                                                   | 15 |



# Windows Analysis Report

62724e14c3203.dll

## Overview

### General Information

Sample Name:

62724e14c3203.dll

Analysis ID:

620140

MD5:

d8b1d46801506b.

SHA1:

af58e06fafcf944...

SHA256:

ac633cc57571ff5..

Tags:

dll

enel

enelenergia

gozi

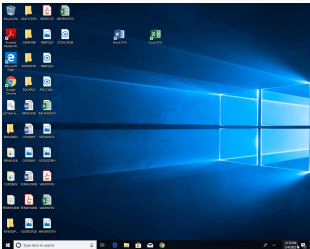
isfb

ita

ursnif

Infos:





### Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Ursnif

Score:

72

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

### Signatures

Multi AV Scanner detection for subm...

Yara detected Ursnif

Tries to detect sandboxes and other...

Query firmware table information (lik...

Tries to detect sandboxes / dynamic...

Machine Learning detection for sam...

Uses 32bit PE files

PE file contains an invalid checksum

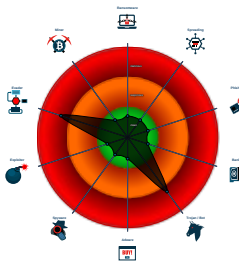
Tries to load missing DLLs

May sleep (evasive loops) to hinder...

PE file contains sections with non-s...

Contains capabilities to detect virtua...

### Classification



## Process Tree

System is w10x64

loaddll32.exe

(PID: 1560 cmdline: loaddll32.exe "C:\Users\user\Desktop\62724e14c3203.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)

cmd.exe

(PID: 4392 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\62724e14c3203.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)

rundll32.exe

(PID: 5244 cmdline: rundll32.exe "C:\Users\user\Desktop\62724e14c3203.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)

regsvr32.exe

(PID: 5616 cmdline: regsvr32.exe /s C:\Users\user\Desktop\62724e14c3203.dll MD5: 426E7499F6A7346F0410DEAD0805586B)

rundll32.exe

(PID: 5016 cmdline: rundll32.exe C:\Users\user\Desktop\62724e14c3203.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)

cleanup

## Malware Configuration

No configs have been found

## Yara Signatures

| Initial Sample    |                      |                      |              |         |
|-------------------|----------------------|----------------------|--------------|---------|
| Source            | Rule                 | Description          | Author       | Strings |
| 62724e14c3203.dll | JoeSecurity_Ursnif_1 | Yara detected Ursnif | Joe Security |         |

## Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2022

Page 4 of 15

## Snort Signatures

⛔ No Snort rule has matched

## Joe Sandbox Signatures

### AV Detection



Multi AV Scanner detection for submitted file

Machine Learning detection for sample

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



Yara detected Ursnif

### E-Banking Fraud



Yara detected Ursnif

### Hooking and other Techniques for Hiding and Protection



Yara detected Ursnif

### Malware Analysis System Evasion



Query firmware table information (likely to detect VMs)

Tries to detect sandboxes / dynamic malware analysis system (registry check)

### Anti Debugging



Tries to detect sandboxes and other dynamic analysis tools (window names)

### Stealing of Sensitive Information



Yara detected Ursnif

### Remote Access Functionality



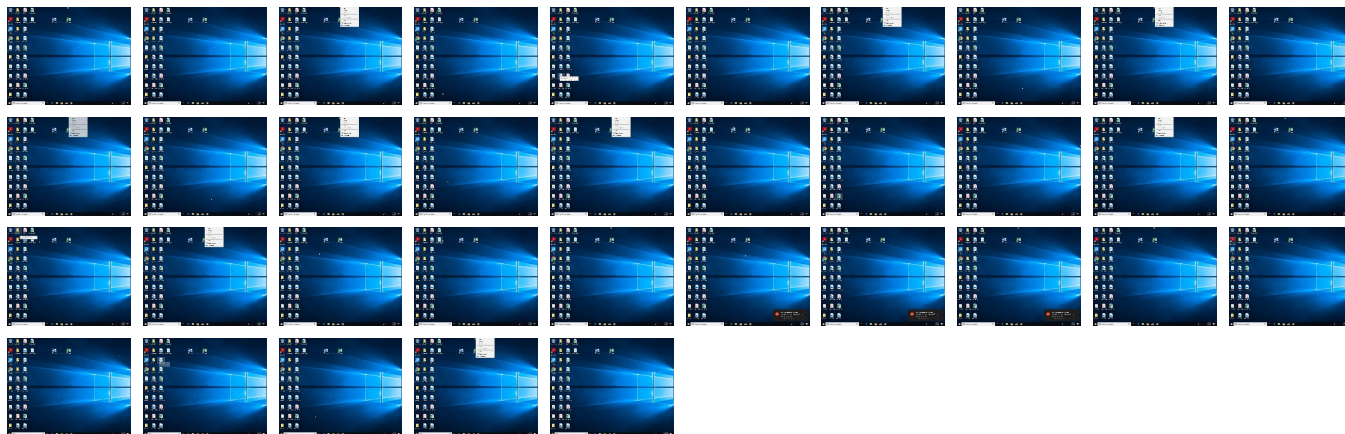
Yara detected Ursnif

## Mitre Att&ck Matrix

| Initial Access | Execution                          | Persistence        | Privilege Escalation  | Defense Evasion | Credential Access     | Discovery                       | Lateral Movement | Collection             | Exfiltration                           | Command and Control | Network Effects                             | Remote Service Effects                      | Impact                  |
|----------------|------------------------------------|--------------------|-----------------------|-----------------|-----------------------|---------------------------------|------------------|------------------------|----------------------------------------|---------------------|---------------------------------------------|---------------------------------------------|-------------------------|
| Valid Accounts | Windows Management Instrumentation | 1 DLL Side-Loading | 1 1 Process Injection | 1 Regsvr32      | OS Credential Dumping | 3 1 Security Software Discovery | Remote Services  | Data from Local System | Exfiltration Over Other Network Medium | Data Obfuscation    | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modify System Partition |



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                   |
|-------------------|-----------|----------------|-------------------------|------------------------|
| 62724e14c3203.dll | 29%       | Virustotal     |                         | <a href="#">Browse</a> |
| 62724e14c3203.dll | 29%       | ReversingLabs  | Win32.Trojan.Ursni<br>f |                        |
| 62724e14c3203.dll | 100%      | Joe Sandbox ML |                         |                        |

## Dropped Files

 No Antivirus matches

## Unpacked PE Files

 No Antivirus matches

## Domains

 No Antivirus matches

## URLs

| Source                       | Detection | Scanner        | Label | Link |
|------------------------------|-----------|----------------|-------|------|
| http://pki-ocsp.symauth.com0 | 0%        | URL Reputation | safe  |      |

## Domains and IPs

### Contacted Domains

 No contacted domains info

### URLs from Memory and Binaries

| Name                                                                                                 | Source            | Malicious | Antivirus Detection    | Reputation |
|------------------------------------------------------------------------------------------------------|-------------------|-----------|------------------------|------------|
| http://pki-crl.symauth.com/offlineca/TheInstituteofElectricalandElectronicsEngineersInclEEERootCA.cr | 62724e14c3203.dll | false     |                        | high       |
| http://pki-ocsp.symauth.com0                                                                         | 62724e14c3203.dll | false     | • URL Reputation: safe | unknown    |
| http://pki-crl.symauth.com/ca_d409a5cb737dc0768fd08ed5256f3633/LatestCRL.crl07                       | 62724e14c3203.dll | false     |                        | high       |

### World Map of Contacted IPs

 No contacted IP infos

## General Information

|                                                    |                                                                                                                     |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Joe Sandbox Version:                               | 34.0.0 Boulder Opal                                                                                                 |
| Analysis ID:                                       | 620140                                                                                                              |
| Start date and time: 04/05/202212:06:42            | 2022-05-04 12:06:42 +02:00                                                                                          |
| Joe Sandbox Product:                               | CloudBasic                                                                                                          |
| Overall analysis duration:                         | 0h 5m 31s                                                                                                           |
| Hypervisor based Inspection enabled:               | false                                                                                                               |
| Report type:                                       | light                                                                                                               |
| Sample file name:                                  | 62724e14c3203.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: | 32                                                                                                                  |
| 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:         | <ul style="list-style-type: none"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>                                                                                                    |
| Analysis Mode:        | default                                                                                                                                                                                                                             |
| Analysis stop reason: | Timeout                                                                                                                                                                                                                             |
| Detection:            | MAL                                                                                                                                                                                                                                 |
| Classification:       | mal72.troj.evad.winDLL@9/0@0/0                                                                                                                                                                                                      |
| EGA Information:      | Failed                                                                                                                                                                                                                              |
| HDC Information:      | Failed                                                                                                                                                                                                                              |
| HCA Information:      | <ul style="list-style-type: none"><li>• Successful, ratio: 100%</li><li>• Number of executed functions: 0</li><li>• Number of non-executed functions: 0</li></ul>                                                                   |
| Cookbook Comments:    | <ul style="list-style-type: none"><li>• Found application associated with file extension: .dll</li><li>• Adjust boot time</li><li>• Enable AMSI</li><li>• Sleeps bigger than 120000ms are automatically reduced to 1000ms</li></ul> |

### Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, ctdl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target loadll32.exe, PID 1560 because there are no executed function
- Not all processes where analyzed, report is missing behavior information

### Simulations

#### Behavior and APIs

| Time     | Type            | Description                                      |
|----------|-----------------|--------------------------------------------------|
| 12:07:48 | API Interceptor | 1x Sleep call for process: regsvr32.exe modified |
| 12:07:48 | API Interceptor | 2x Sleep call for process: rundll32.exe modified |
| 12:07:52 | API Interceptor | 1x Sleep call for process: loadll32.exe modified |

### Joe Sandbox View / Context

#### IPs

 No context

#### Domains

 No context

#### ASNs

 No context

#### 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):       | 6.015061702913002                                                                                                                                                                                                                                                                |
| TrID:                 | <ul style="list-style-type: none"><li>Win32 Dynamic Link Library (generic) (1002004/3) 99.60%</li><li>Generic Win/DOS Executable (2004/3) 0.20%</li><li>DOS Executable Generic (2002/1) 0.20%</li><li>Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%</li></ul> |
| File name:            | 62724e14c3203.dll                                                                                                                                                                                                                                                                |
| File size:            | 3735060                                                                                                                                                                                                                                                                          |
| MD5:                  | d8b1d46801506b84938f864365bc7c81                                                                                                                                                                                                                                                 |
| SHA1:                 | af58e06fafcf944e800ac5029b5a40ce5326db3e                                                                                                                                                                                                                                         |
| SHA256:               | ac633cc57571ff54a72dd8cac9236cddef488af8074e08a3b17b53983d3f0733                                                                                                                                                                                                                 |
| SHA512:               | 672ae9a31d0d5a6c6c724d5ca22a408938a15729e8abc93036575062b6ea078e64f7ecd7d4ca2aece79b69520ade7727c0351bb7d6e904212d38f56dc20c30af                                                                                                                                                 |
| SSDEEP:               | 49152:3TeGCEZ8YnAM+OxCYxsk2GVybVpr7Vt+S/zl:3TBCEZXAM+O4msk2GV4Vprxt+SL/                                                                                                                                                                                                          |
| TLSH:                 | 36065AE1760AA5CFD09A5AF89813CF026B3C53F94A115D13EDA9787F6D63CC13289E24                                                                                                                                                                                                           |
| File Content Preview: | MZ.....@.....!..L!This program cannot be run in DOS<br>mode...\$.....\0.....V.....W.....V.....V.....Rich.....PE..L....Chb...                                                                                                                                                     |

### File Icon



|            |                 |
|------------|-----------------|
| Icon Hash: | 74f0e4ecccde0e4 |
|------------|-----------------|

## Static PE Info

### General

|                             |                                           |
|-----------------------------|-------------------------------------------|
| Entrypoint:                 | 0x10394000                                |
| Entrypoint Section:         | .taggant                                  |
| Digitally signed:           | false                                     |
| Imagebase:                  | 0x10000000                                |
| Subsystem:                  | windows gui                               |
| Image File Characteristics: | 32BIT_MACHINE, EXECUTABLE_IMAGE, DLL      |
| DLL Characteristics:        |                                           |
| Time Stamp:                 | 0x626843F2 [Tue Apr 26 19:11:46 2022 UTC] |
| TLS Callbacks:              |                                           |
| CLR (.Net) Version:         |                                           |
| OS Version Major:           | 5                                         |
| OS Version Minor:           | 0                                         |
| File Version Major:         | 5                                         |
| File Version Minor:         | 0                                         |
| Subsystem Version Major:    | 5                                         |
| Subsystem Version Minor:    | 0                                         |
| Import Hash:                | c846031d91edf5130318f0a56b358ac5          |

### Entrypoint Preview

| Instruction                 |
|-----------------------------|
| jmp 00007FC1049834DAh       |
| pmaxub mm7, qword ptr [eax] |
| add byte ptr [eax], al      |
| add byte ptr [eax], al      |
| add cl, ch                  |

| Instruction                              |
|------------------------------------------|
| add byte ptr [eax], ah                   |
| add byte ptr [eax], al                   |
| push esp                                 |
| inc ecx                                  |
| inc edi                                  |
| inc edi                                  |
| add byte ptr [eax], ah                   |
| add byte ptr [eax], al                   |
| loop 00007FC1049834DEh                   |
| add byte ptr [eax], al                   |
| add dword ptr [eax], eax                 |
| xor byte ptr [edx+0906DE0Ch], al         |
| sub al, byte ptr [esi+0DF78648h]         |
| add dword ptr [edi], eax                 |
| add ah, byte ptr [eax+30CF0C82h]         |
| or byte ptr [ebx+ecx*8], 00000002h       |
| add dword ptr [ecx], eax                 |
| xor dword ptr [09060B30h], ecx           |
| pushad                                   |
| xchg byte ptr [eax+01h], cl              |
| add eax, dword ptr [edx+eax]             |
| add dword ptr [eax], esi                 |
| and ecx, 862A0906h                       |
| dec eax                                  |
| xchg bh, dh                              |
| or eax, A0010701h                        |
| adc ebx, D0D08104h                       |
| add byte ptr [ecx], al                   |
| add byte ptr [ecx], al                   |
| sal dword ptr [ecx+000003A1h], 00000000h |
| add byte ptr [eax], al                   |
| add byte ptr [eax], al                   |
| add byte ptr [eax], al                   |
| add byte ptr [ecx], al                   |
| add byte ptr [ecx+60h], bh               |
| xchg dword ptr [edx+edi*2], ebp          |
| xor byte ptr [edi-0Ch], ch               |
| insd                                     |
| jnbe 00007FC104983521h                   |
| pushfd                                   |
| push eax                                 |
| les esi, esp                             |
| cmp dword ptr [1EFF9DD7h], eax           |
| stosd                                    |
| mov al, byte ptr [5C67BBA0h]             |
| cli                                      |
| pop ecx                                  |
| xor bh, bh                               |
| add byte ptr [ecx], al                   |
| add byte ptr [ecx], 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                   |

| Instruction                    |
|--------------------------------|
| 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 [esi+edi*8], dl   |
| cmp byte ptr [eax], al         |
| add byte ptr [eax], al         |
| add byte ptr [eax], al         |
| sub al, byte ptr [eax]         |
| add al, byte ptr [eax]         |
| add dword ptr [eax], eax       |
| imul ebp, dword ptr [edx], F0h |

| Rich Headers                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div> <div>Programming Language:</div> <div> <ul style="list-style-type: none"> <li>[ASM] VS2008 SP1 build 30729</li> <li>[LNK] VS2008 SP1 build 30729</li> <li>[IMP] VS2008 SP1 build 30729</li> <li>[EXP] VS2008 SP1 build 30729</li> </ul> </div> </div> |

| Data Directories                     |                 |              |               |
|--------------------------------------|-----------------|--------------|---------------|
| Name                                 | Virtual Address | Virtual Size | Is in Section |
| IMAGE_DIRECTORY_ENTRY_EXPORT         | 0xe000          | 0x4c         | .exports      |
| IMAGE_DIRECTORY_ENTRY_IMPORT         | 0xf07b          | 0x6c         | .imports      |
| IMAGE_DIRECTORY_ENTRY_RESOURCE       | 0x0             | 0x0          |               |
| 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   | 0x0             | 0x0          |               |
| IMAGE_DIRECTORY_ENTRY_IAT            | 0x0             | 0x0          |               |
| 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          | 0x16b7       | 0x1800   | False    | 0.700846354167  | data      | 6.45396003483  | IMAGE_SCN_MEM_EXECUT<br>E, IMAGE_SCN_CNT_CODE,<br>IMAGE_SCN_MEM_READ              |
| .rdata   | 0x3000          | 0x59c        | 0x600    | False    | 0.185546875     | data      | 1.83732227468  | IMAGE_SCN_CNT_INITIALIZ<br>ED_DATA,<br>IMAGE_SCN_MEM_READ                         |
| .data    | 0x4000          | 0x25c        | 0x200    | False    | 0.08984375      | data      | 0.369416603835 | IMAGE_SCN_CNT_INITIALIZ<br>ED_DATA,<br>IMAGE_SCN_MEM_WRITE,<br>IMAGE_SCN_MEM_READ |
| .bss     | 0x5000          | 0x2dc        | 0x400    | False    | 0.7626953125    | data      | 6.25781926122  | IMAGE_SCN_CNT_INITIALIZ<br>ED_DATA,<br>IMAGE_SCN_MEM_WRITE,<br>IMAGE_SCN_MEM_READ |
| .reloc   | 0x6000          | 0x8000       | 0x7200   | False    | 0.970086348684  | data      | 7.85482039795  | IMAGE_SCN_CNT_INITIALIZ<br>ED_DATA,<br>IMAGE_SCN_MEM_READ                         |
| .exports | 0xe000          | 0x1000       | 0x200    | False    | 0.140625        | data      | 0.781993247616 | IMAGE_SCN_CNT_INITIALIZ<br>ED_DATA,<br>IMAGE_SCN_MEM_READ                         |

| Name     | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type            | Entropy       | Characteristics                                                                                                                |
|----------|-----------------|--------------|----------|----------|-----------------|----------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------|
| .imports | 0xf000          | 0x1000       | 0x200    | False    | 0.26171875      | data                 | 2.01907876474 | IMAGE_SCN_CNT_INITIALIZED_DATA,<br>IMAGE_SCN_MEM_WRITE,<br>IMAGE_SCN_MEM_READ                                                  |
| .themida | 0x10000         | 0x384000     | 0x384000 | unknown  | unknown         | unknown              | unknown       | IMAGE_SCN_MEM_EXECUTE,<br>IMAGE_SCN_CNT_INITIALIZED_DATA,<br>IMAGE_SCN_MEM_WRITE,<br>IMAGE_SCN_CNT_CODE,<br>IMAGE_SCN_MEM_READ |
| .taggant | 0x394000        | 0x2200       | 0x2014   | False    | 0.32976132489   | DOS executable (COM) | 3.88631067097 | IMAGE_SCN_MEM_EXECUTE,<br>IMAGE_SCN_CNT_INITIALIZED_DATA,<br>IMAGE_SCN_CNT_CODE,<br>IMAGE_SCN_MEM_READ                         |

| Imports      |                                                      |
|--------------|------------------------------------------------------|
| DLL          | Import                                               |
| kernel32.dll | GetModuleHandleA                                     |
| ntdll.dll    | _snwprintf                                           |
| ADVAPI32.dll | ConvertStringSecurityDescriptorToSecurityDescriptorA |

| Exports           |         |            |
|-------------------|---------|------------|
| Name              | Ordinal | Address    |
| DllRegisterServer | 1       | 0x100011c2 |

Network Behavior

 No network behavior found

Statistics

Behavior

loaddll32.exe  
cmd.exe  
regsvr32.exe  
rundll32.exe  
rundll32.exe

 Click to jump to process

System Behavior

Analysis Process: loaddll32.exe    PID: 1560, Parent PID: 3892

| General                       |                                                         |
|-------------------------------|---------------------------------------------------------|
| Target ID:                    | 0                                                       |
| Start time:                   | 12:07:43                                                |
| Start date:                   | 04/05/2022                                              |
| Path:                         | C:\Windows\System32\loaddll32.exe                       |
| Wow64 process (32bit):        | true                                                    |
| Commandline:                  | loaddll32.exe "C:\Users\user\Desktop\62724e14c3203.dll" |
| Imagebase:                    | 0xfc0000                                                |
| File size:                    | 116736 bytes                                            |
| MD5 hash:                     | 7DEB5DB86C0AC789123DEC286286B938                        |
| Has elevated privileges:      | true                                                    |
| Has administrator privileges: | true                                                    |
| Programmed in:                | C, C++ or other language                                |
| Reputation:                   | high                                                    |

| File Activities                                                                     |        |            |         |            |       |                |        |  |
|-------------------------------------------------------------------------------------|--------|------------|---------|------------|-------|----------------|--------|--|
| There is hidden Windows Behavior. Click on <b>Show Windows Behavior</b> to show it. |        |            |         |            |       |                |        |  |
| File Path                                                                           | Access | Attributes | Options | Completion | Count | Source Address | Symbol |  |

| Analysis Process: cmd.exe    PID: 4392, Parent PID: 1560 |                                                                      |
|----------------------------------------------------------|----------------------------------------------------------------------|
| General                                                  |                                                                      |
| Target ID:                                               | 1                                                                    |
| Start time:                                              | 12:07:44                                                             |
| Start date:                                              | 04/05/2022                                                           |
| Path:                                                    | C:\Windows\SysWOW64\cmd.exe                                          |
| Wow64 process (32bit):                                   | true                                                                 |
| Commandline:                                             | cmd.exe /C rundll32.exe "C:\Users\user\Desktop\62724e14c3203.dll",#1 |
| Imagebase:                                               | 0x1190000                                                            |
| 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                                                                     |        |            |         |            |       |                |        |  |
|-------------------------------------------------------------------------------------|--------|------------|---------|------------|-------|----------------|--------|--|
| There is hidden Windows Behavior. Click on <b>Show Windows Behavior</b> to show it. |        |            |         |            |       |                |        |  |
| File Path                                                                           | Access | Attributes | Options | Completion | Count | Source Address | Symbol |  |

| Analysis Process: regsvr32.exe    PID: 5616, Parent PID: 1560 |                                                         |
|---------------------------------------------------------------|---------------------------------------------------------|
| General                                                       |                                                         |
| Target ID:                                                    | 2                                                       |
| Start time:                                                   | 12:07:44                                                |
| Start date:                                                   | 04/05/2022                                              |
| Path:                                                         | C:\Windows\SysWOW64\regsvr32.exe                        |
| Wow64 process (32bit):                                        | true                                                    |
| Commandline:                                                  | regsvr32.exe /s C:\Users\user\Desktop\62724e14c3203.dll |
| Imagebase:                                                    | 0x9e0000                                                |
| File size:                                                    | 20992 bytes                                             |
| MD5 hash:                                                     | 426E7499F6A7346F0410DEAD0805586B                        |
| Has elevated privileges:                                      | true                                                    |
| Has administrator privileges:                                 | true                                                    |

|                |                          |
|----------------|--------------------------|
| Programmed in: | C, C++ or other language |
| Reputation:    | high                     |

**Analysis Process: rundll32.exe**    PID: 5244, Parent PID: 4392

**General**

|                               |                                                           |
|-------------------------------|-----------------------------------------------------------|
| Target ID:                    | 3                                                         |
| Start time:                   | 12:07:44                                                  |
| Start date:                   | 04/05/2022                                                |
| Path:                         | C:\Windows\SysWOW64\rundll32.exe                          |
| Wow64 process (32bit):        | true                                                      |
| Commandline:                  | rundll32.exe "C:\Users\user\Desktop\62724e14c3203.dll",#1 |
| Imagebase:                    | 0xde0000                                                  |
| 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: 5016, Parent PID: 1560

**General**

|                               |                                                                        |
|-------------------------------|------------------------------------------------------------------------|
| Target ID:                    | 4                                                                      |
| Start time:                   | 12:07:44                                                               |
| Start date:                   | 04/05/2022                                                             |
| Path:                         | C:\Windows\SysWOW64\rundll32.exe                                       |
| Wow64 process (32bit):        | true                                                                   |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\62724e14c3203.dll,DllRegisterServer |
| Imagebase:                    | 0xde0000                                                               |
| File size:                    | 61952 bytes                                                            |
| MD5 hash:                     | D7CA562B0DB4F4DD0F03A89A1FDAD63D                                       |
| Has elevated privileges:      | true                                                                   |
| Has administrator privileges: | true                                                                   |
| Programmed in:                | C, C++ or other language                                               |
| Reputation:                   | high                                                                   |

**Disassembly**

 No disassembly