

JoeSandbox Cloud BASIC



**ID:** 764036

**Sample Name:** 6k00SOeMjU.dll

**Cookbook:** default.jbs

**Time:** 10:51:12

**Date:** 09/12/2022

**Version:** 36.0.0 Rainbow Opal

# Table of Contents

|                                                           |    |
|-----------------------------------------------------------|----|
| Table of Contents                                         | 2  |
| Windows Analysis Report 6k00SOeMjU.dll                    | 4  |
| Overview                                                  | 4  |
| General Information                                       | 4  |
| Detection                                                 | 4  |
| Signatures                                                | 4  |
| Classification                                            | 4  |
| Process Tree                                              | 4  |
| Malware Configuration                                     | 4  |
| Yara Signatures                                           | 4  |
| Memory Dumps                                              | 4  |
| Unpacked PEs                                              | 5  |
| Sigma Signatures                                          | 5  |
| Snort Signatures                                          | 5  |
| Joe Sandbox Signatures                                    | 5  |
| AV Detection                                              | 6  |
| Networking                                                | 6  |
| System Summary                                            | 6  |
| Hooking and other Techniques for Hiding and Protection    | 6  |
| Malware Analysis System Evasion                           | 6  |
| Anti Debugging                                            | 6  |
| HIPS / PFW / Operating System Protection Evasion          | 6  |
| Stealing of Sensitive Information                         | 6  |
| Remote Access Functionality                               | 6  |
| Mitre Att&ck Matrix                                       | 6  |
| Behavior Graph                                            | 7  |
| Screenshots                                               | 7  |
| Thumbnails                                                | 7  |
| Antivirus, Machine Learning and Genetic Malware Detection | 8  |
| Initial Sample                                            | 8  |
| Dropped Files                                             | 8  |
| Unpacked PE Files                                         | 8  |
| Domains                                                   | 8  |
| URLs                                                      | 9  |
| Domains and IPs                                           | 9  |
| Contacted Domains                                         | 9  |
| URLs from Memory and Binaries                             | 9  |
| World Map of Contacted IPs                                | 9  |
| Public IPs                                                | 9  |
| General Information                                       | 10 |
| Warnings                                                  | 10 |
| Simulations                                               | 10 |
| Behavior and APIs                                         | 10 |
| Joe Sandbox View / Context                                | 10 |
| IPs                                                       | 10 |
| Domains                                                   | 11 |
| ASNs                                                      | 11 |
| JA3 Fingerprints                                          | 11 |
| Dropped Files                                             | 11 |
| Created / dropped Files                                   | 11 |
| Static File Info                                          | 11 |
| General                                                   | 11 |
| File Icon                                                 | 11 |
| Static PE Info                                            | 11 |
| General                                                   | 11 |
| Authenticode Signature                                    | 12 |
| Entrypoint Preview                                        | 12 |
| Data Directories                                          | 13 |
| Sections                                                  | 13 |
| Resources                                                 | 14 |
| Imports                                                   | 14 |
| Exports                                                   | 14 |
| Possible Origin                                           | 14 |
| Network Behavior                                          | 15 |
| TCP Packets                                               | 15 |
| Statistics                                                | 15 |
| Behavior                                                  | 15 |
| System Behavior                                           | 16 |
| Analysis Process: loadll32.exePID: 5288, Parent PID: 3452 | 16 |
| General                                                   | 16 |
| File Activities                                           | 16 |
| Analysis Process: conhost.exePID: 5260, Parent PID: 5288  | 16 |
| General                                                   | 16 |

|                                                           |    |
|-----------------------------------------------------------|----|
| Analysis Process: cmd.exePID: 5316, Parent PID: 5288      | 17 |
| General                                                   | 17 |
| File Activities                                           | 17 |
| Analysis Process: rundll32.exePID: 5448, Parent PID: 5288 | 17 |
| General                                                   | 17 |
| Analysis Process: rundll32.exePID: 5476, Parent PID: 5316 | 17 |
| General                                                   | 17 |
| Analysis Process: rundll32.exePID: 3920, Parent PID: 5288 | 18 |
| General                                                   | 18 |
| Disassembly                                               | 18 |

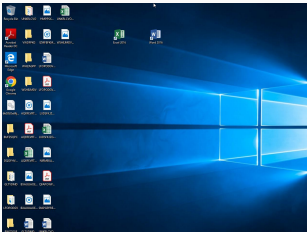
# Windows Analysis Report

6k00S0eMjU.dLL

## Overview

## General Information

|              |                                                                                                                                                                                                                                                                  |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sample Name: | 6k00SOeMjU.dll                                                                                                                                                                                                                                                   |
| Analysis ID: | 764036                                                                                                                                                                                                                                                           |
| MD5:         | 0d079a931e42f5..                                                                                                                                                                                                                                                 |
| SHA1:        | d5f1ab52221019..                                                                                                                                                                                                                                                 |
| SHA256:      | ead2c5aaf92fe07..                                                                                                                                                                                                                                                |
| Tags:        | <div>32 dll exe</div>                                                                                                                                                                                                                                            |
| Infos:       | <div>  </div> |



## Detection

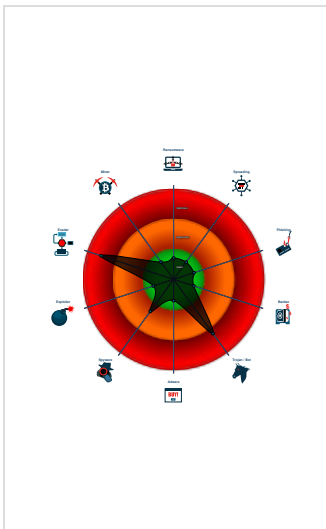
The figure displays a vertical stack of four colored boxes, each containing a threat level label. From top to bottom, the boxes are: red with 'MALICIOUS', brown with 'SUSPICIOUS', green with 'CLEAN', and grey with 'UNKNOWN'. Below this stack is a red box with the text 'SystemBC'. At the bottom of the figure is a table with four rows of security metrics.

|              |         |
|--------------|---------|
| Score:       | 96      |
| Range:       | 0 - 100 |
| Whitelisted: | false   |
| Confidence:  | 100%    |

## Signatures

- System process connects to network...
- Yara detected SystemBC
- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Hides threads from debuggers
- Overwrites code with unconditional j...
- Overwrites code with function prolog...
- Tries to evade analysis by executio...
- Tries to detect virtualization through...
- PE file contains section with specia...
- Creates a DirectInput object (often f...
- Uses 32bit PE files

## Classification



## Process Tree

- System is w10x64
-  **loadaddl32.exe** (PID: 5288 cmdline: loadaddl32.exe "C:\Users\user\Desktop\6k00SOeMjU.dll" MD5: 1F562FBF37040EC6C43C8D5EF619EA39)
-  **conhost.exe** (PID: 5260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C3BBF8A4496)
-  **cmd.exe** (PID: 5316 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\6k00SOeMjU.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
-  **rundll32.exe** (PID: 5476 cmdline: rundll32.exe "C:\Users\user\Desktop\6k00SOeMjU.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
-  **rundll32.exe** (PID: 5448 cmdline: rundll32.exe C:\Users\user\Desktop\6k00SOeMjU.dll,rundll MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
-  **rundll32.exe** (PID: 3920 cmdline: rundll32.exe "C:\Users\user\Desktop\6k00SOeMjU.dll",rundll MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- cleanup

## Malware Configuration

 No configs have been found

## Yara Signatures

## Memory Dumps

| Source                                                                               | Rule                         | Description                                                      | Author                                         | Strings                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------|------------------------------|------------------------------------------------------------------|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 00000005.00000002.764703413.0000000010005000.0000004.00000001.01000000.00000003.sdmp | EXT_MAL_System<br>BC_Mar22_1 | Detects unpacked SystemBC module as used by Emotet in March 2022 | Thomas Barabosch,<br>Deutsche Telekom Security | <ul style="list-style-type: none"><li>• 0x173:\$sx1: -WindowStyle Hidden -ep bypass -file</li><li>• 0x0:\$sx2: BEGINDATA</li><li>• 0x1af:\$sx3: GET %s HTTP/1.0</li><li>• 0x1ca:\$s5: User-Agent:</li><li>• 0x11b:\$s8: ALLUSERSPROFILE</li></ul> |
| 00000003.00000002.764685317.0000000010005000.0000004.00000001.01000000.00000003.sdmp | EXT_MAL_System<br>BC_Mar22_1 | Detects unpacked SystemBC module as used by Emotet in March 2022 | Thomas Barabosch,<br>Deutsche Telekom Security | <ul style="list-style-type: none"><li>• 0x173:\$sx1: -WindowStyle Hidden -ep bypass -file</li><li>• 0x0:\$sx2: BEGINDATA</li><li>• 0x1af:\$sx3: GET %s HTTP/1.0</li><li>• 0x1ca:\$s5: User-Agent:</li><li>• 0x11b:\$s8: ALLUSERSPROFILE</li></ul> |

| Source                                                                               | Rule                     | Description                                                      | Author                                      | Strings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------|--------------------------|------------------------------------------------------------------|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 00000004.00000002.764666285.0000000010005000.0000004.00000001.01000000.00000003.sdmp | EXT_MAL_SystemBC_Mar22_1 | Detects unpacked SystemBC module as used by Emotet in March 2022 | Thomas Barabosch, Deutsche Telekom Security | <ul style="list-style-type: none"><li>0x173:\$sx1: -WindowStyle Hidden -ep bypass -file</li><li>0x0:\$sx2: BEGINDATA</li><li>0x1af:\$sx3: GET %s HTTP/1.0</li><li>0x1ca:\$s5: User-Agent:</li><li>0x11b:\$s8: ALLUSERSPROFILE</li></ul>                                                                                                                                                                                                                                                                                                                                                                      |
| Process Memory Space: rundll32.exe PID: 5448                                         | EXT_MAL_SystemBC_Mar22_1 | Detects unpacked SystemBC module as used by Emotet in March 2022 | Thomas Barabosch, Deutsche Telekom Security | <ul style="list-style-type: none"><li>0x5869:\$sx1: -WindowStyle Hidden -ep bypass -file</li><li>0x5984:\$sx1: -WindowStyle Hidden -ep bypass -file</li><li>0x578f:\$sx2: BEGINDATA</li><li>0x57cc:\$sx2: BEGINDATA</li><li>0x58a5:\$sx3: GET %s HTTP/1.0</li><li>0x59bd:\$sx3: GET %s HTTP/1.0</li><li>0x58c0:\$s5: User-Agent:</li><li>0x662:\$s8: ALLUSERSPROFILE</li><li>0x5811:\$s8: ALLUSERSPROFILE</li><li>0x5933:\$s8: ALLUSERSPROFILE</li><li>0x629f:\$s8: ALLUSERSPROFILE</li><li>0x6b6e:\$s8: ALLUSERSPROFILE</li><li>0x7121:\$s8: ALLUSERSPROFILE</li><li>0x7790:\$s8: ALLUSERSPROFILE</li></ul> |
| Process Memory Space: rundll32.exe PID: 5448                                         | JoeSecurity_SystemBC     | Yara detected SystemBC                                           | Joe Security                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Click to see the 4 entries                                                           |                          |                                                                  |                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Unpacked PEs                       |                             |                                                                  |                                             |                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------|-----------------------------|------------------------------------------------------------------|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source                             | Rule                        | Description                                                      | Author                                      | Strings                                                                                                                                                                                                                                                                                                                                                                                                           |
| 4.2.rundll32.exe.10000000.0.unpack | EXT_MAL_SystemBC_Mar22_1    | Detects unpacked SystemBC module as used by Emotet in March 2022 | Thomas Barabosch, Deutsche Telekom Security | <ul style="list-style-type: none"><li>0x2f54:\$sx1: -WindowStyle Hidden -ep bypass -file</li><li>0x2de1:\$sx2: BEGINDATA</li><li>0x2f90:\$sx3: GET %s HTTP/1.0</li><li>0x2fab:\$s5: User-Agent:</li><li>0x2efc:\$s8: ALLUSERSPROFILE</li></ul>                                                                                                                                                                    |
| 4.2.rundll32.exe.10000000.0.unpack | JoeSecurity_SystemBC        | Yara detected SystemBC                                           | Joe Security                                |                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 4.2.rundll32.exe.10000000.0.unpack | MALWARE_Win_EXEPWSH_DLAgent | Detects SystemBC                                                 | ditekSHen                                   | <ul style="list-style-type: none"><li>0x2f49:\$pwsh: powershell</li><li>0x2f90:\$s1: GET %s HTTP/1</li><li>0x2fab:\$s2: User-Agent:</li><li>0x2f54:\$s3: -WindowStyle Hidden -ep bypass -file "</li><li>0x2f85:\$s4: LdrLoadDll</li><li>0x2de1:\$v1: BEGINDATA</li><li>0x2deb:\$v2: HOST1:</li><li>0x2e1e:\$v2: HOST2:</li><li>0x2e51:\$v3: PORT1:</li><li>0x2e5d:\$v4: TOR:</li><li>0x2ef6:\$v6: start</li></ul> |
| 5.2.rundll32.exe.10000000.0.unpack | EXT_MAL_SystemBC_Mar22_1    | Detects unpacked SystemBC module as used by Emotet in March 2022 | Thomas Barabosch, Deutsche Telekom Security | <ul style="list-style-type: none"><li>0x2f54:\$sx1: -WindowStyle Hidden -ep bypass -file</li><li>0x2de1:\$sx2: BEGINDATA</li><li>0x2f90:\$sx3: GET %s HTTP/1.0</li><li>0x2fab:\$s5: User-Agent:</li><li>0x2efc:\$s8: ALLUSERSPROFILE</li></ul>                                                                                                                                                                    |
| 5.2.rundll32.exe.10000000.0.unpack | JoeSecurity_SystemBC        | Yara detected SystemBC                                           | Joe Security                                |                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Click to see the 4 entries         |                             |                                                                  |                                             |                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Sigma Signatures                                                                    |                           |
|-------------------------------------------------------------------------------------|---------------------------|
|  | No Sigma rule has matched |

| Snort Signatures                                                                    |                           |
|-------------------------------------------------------------------------------------|---------------------------|
|  | No Snort rule has matched |

| Joe Sandbox Signatures |  |
|------------------------|--|
|------------------------|--|

## AV Detection



Multi AV Scanner detection for submitted file

## Networking



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

## System Summary



Malicious sample detected (through community Yara rule)

PE file contains section with special chars

## Hooking and other Techniques for Hiding and Protection



Overwrites code with unconditional jumps - possibly settings hooks in foreign process

Overwrites code with function prologues

## Malware Analysis System Evasion



Tries to evade analysis by execution special instruction (VM detection)

Tries to detect virtualization through RDTSC time measurements

## Anti Debugging



Hides threads from debuggers

## HIPS / PFW / Operating System Protection Evasion



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

## Stealing of Sensitive Information



Yara detected SystemBC

## Remote Access Functionality

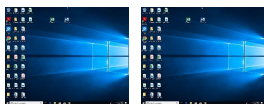


Yara detected SystemBC

## 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 | Path Interception                    | 1 1 1<br>Process Injection           | 1<br>Rundll32                           | 1<br>Credential API Hooking | 3 2 1<br>Security Software Discovery    | Remote Services          | 1<br>Credential API Hooking    | Exfiltration Over Other Network Medium | 1<br>Non-Standard Port | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modify System Partition |
| Default Accounts | Scheduled Task/Job                 | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | 1 2 1<br>Virtualization/Sandbox Evasion | 1<br>Input Capture          | 1<br>Process Discovery                  | Remote Desktop Protocol  | 1<br>Input Capture             | Exfiltration Over Bluetooth            | Junk Data              | Exploit SS7 to Redirect Phone Calls/SMS     | Remotely Wipe Data Without Authorization    | Device Lockout          |
| Domain Accounts  | At (Linux)                         | Logon Script (Windows)               | Logon Script (Windows)               | 1 1 1<br>Process Injection              | Security Account Manager    | 1 2 1<br>Virtualization/Sandbox Evasion | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration                 | Steganography          | Exploit SS7 to Track Device Location        | Obtain Device Cloud Backups                 | Delete Device Data      |





## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source         | Detection | Scanner       | Label                | Link                   |
|----------------|-----------|---------------|----------------------|------------------------|
| 6k00SOeMjU.dll | 23%       | ReversingLabs | Win32.Trojan.Genetic |                        |
| 6k00SOeMjU.dll | 17%       | Virustotal    |                      | <a href="#">Browse</a> |

### Dropped Files

 No Antivirus matches

### Unpacked PE Files

 No Antivirus matches

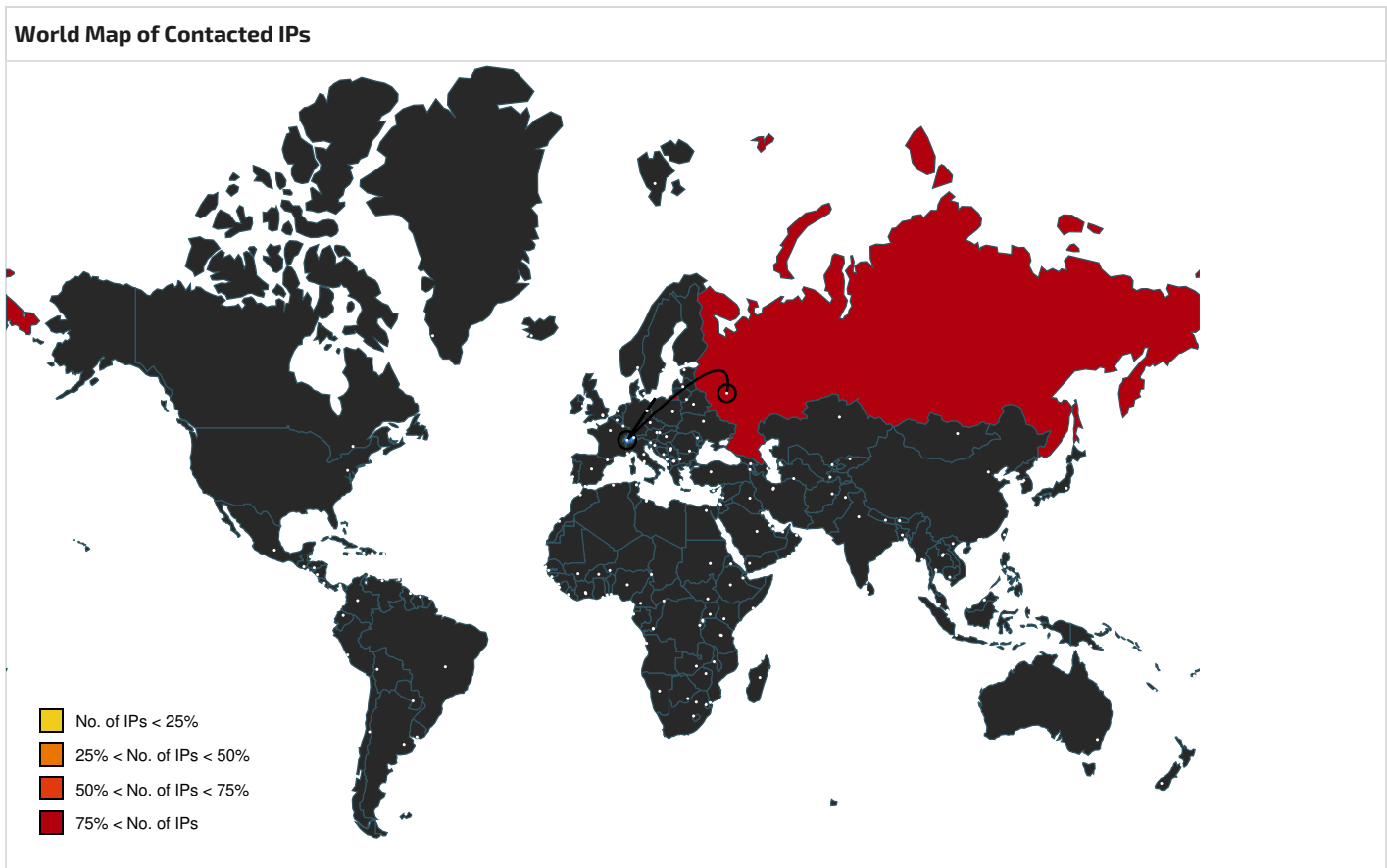
### Domains

 No Antivirus matches

| URLs                                                  |           |                |       |      |
|-------------------------------------------------------|-----------|----------------|-------|------|
| Source                                                | Detection | Scanner        | Label | Link |
| http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t | 0%        | URL Reputation | safe  |      |
| http://https://sectigo.com/CPS0                       | 0%        | URL Reputation | safe  |      |
| http://ocsp.sectigo.com0                              | 0%        | URL Reputation | safe  |      |
| http://www.innosetup.com                              | 0%        | URL Reputation | safe  |      |
| http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0# | 0%        | URL Reputation | safe  |      |

| Domains and IPs                                    |
|----------------------------------------------------|
| <b>Contacted Domains</b>                           |
| <div> <div></div> No contacted domains info </div> |

| URLs from Memory and Binaries                         |                                                                                                                                                                                                                                                                                                                              |           |                                                                        |            |
|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------------------------------------------------------------------------|------------|
| Name                                                  | Source                                                                                                                                                                                                                                                                                                                       | Malicious | Antivirus Detection                                                    | Reputation |
| http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t | 6k00SOeMjU.dll                                                                                                                                                                                                                                                                                                               | false     | <ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul> | unknown    |
| http://https://sectigo.com/CPS0                       | 6k00SOeMjU.dll                                                                                                                                                                                                                                                                                                               | false     | <ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul> | unknown    |
| http://ocsp.sectigo.com0                              | 6k00SOeMjU.dll                                                                                                                                                                                                                                                                                                               | false     | <ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul> | unknown    |
| http://www.innosetup.com                              | rundll32.exe, 00000003.00000002.769805471.0000000010B69000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 00000004.00000002.769805642.0000000010B69000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 00000005.00000002.769803694.000000010B69000.00000002.00000001.01000000.00000003.sdmp, 6k00SOeMjU.dll | false     | <ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul> | unknown    |
| http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0# | 6k00SOeMjU.dll                                                                                                                                                                                                                                                                                                               | false     | <ul style="list-style-type: none"> <li>URL Reputation: safe</li> </ul> | unknown    |



| Public IPs |
|------------|
|------------|

| IP            | Domain  | Country            | Flag                                                                              | ASN    | ASN Name  | Malicious |
|---------------|---------|--------------------|-----------------------------------------------------------------------------------|--------|-----------|-----------|
| 89.22.236.225 | unknown | Russian Federation |  | 197328 | INETLTDTR | true      |

## General Information

|                                                    |                                                                                                                                                                       |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Joe Sandbox Version:                               | 36.0.0 Rainbow Opal                                                                                                                                                   |
| Analysis ID:                                       | 764036                                                                                                                                                                |
| Start date and time:                               | 2022-12-09 10:51:12 +01:00                                                                                                                                            |
| Joe Sandbox Product:                               | CloudBasic                                                                                                                                                            |
| Overall analysis duration:                         | 0h 7m 21s                                                                                                                                                             |
| Hypervisor based Inspection enabled:               | false                                                                                                                                                                 |
| Report type:                                       | light                                                                                                                                                                 |
| Sample file name:                                  | 6k00SOeMjU.dll                                                                                                                                                        |
| Cookbook file name:                                | default.jbs                                                                                                                                                           |
| Analysis system description:                       | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211                                                  |
| Number of analysed new started processes analysed: | 20                                                                                                                                                                    |
| 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:                                    | mal96.troj.evad.winDLL@10/0@0/1                                                                                                                                       |
| 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>• Override analysis time to 240s for rundll32</li> </ul>     |

## Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information

## Simulations

### Behavior and APIs

| Time     | Type            | Description                                      |
|----------|-----------------|--------------------------------------------------|
| 10:52:05 | API Interceptor | 3x Sleep call for process: rundll32.exe modified |
| 10:52:07 | API Interceptor | 1x Sleep call for process: loadll32.exe modified |

## Joe Sandbox View / Context

### IPs

 No context

| Domains                                        |
|------------------------------------------------|
| <div> <div></div> <div>No context</div> </div> |

| ASNs                                           |
|------------------------------------------------|
| <div> <div></div> <div>No context</div> </div> |

| JA3 Fingerprints                               |
|------------------------------------------------|
| <div> <div></div> <div>No context</div> </div> |

| Dropped Files                                  |
|------------------------------------------------|
| <div> <div></div> <div>No context</div> </div> |

| Created / dropped Files                                              |
|----------------------------------------------------------------------|
| <div> <div></div> <div>No created / dropped files found</div> </div> |

Static File Info

General

|                       |                                                                                                                                                                                                                                                                                                                                         |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File type:            | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                 |
| Entropy (8bit):       | 7.976819466268135                                                                                                                                                                                                                                                                                                                       |
| TrID:                 | <div><div><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>VXD Driver (31/22) 0.00%</li><li>Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%</li></ul></div></div> |
| File name:            | 6k00SOeMjU.dll                                                                                                                                                                                                                                                                                                                          |
| File size:            | 7566544                                                                                                                                                                                                                                                                                                                                 |
| MD5:                  | 0d079a931e42f554016db36476e55ba7                                                                                                                                                                                                                                                                                                        |
| SHA1:                 | d5f1ab52221019c746f1cc59a45ce18d0b817496                                                                                                                                                                                                                                                                                                |
| SHA256:               | ead2c5aaf92fe07db45b99587f586c7a45f92c67220cd8113a5d2e7bcb320798                                                                                                                                                                                                                                                                        |
| SHA512:               | 1496f1296df89e1da8780f175631e2551300a99e6c7ea43d2750653fd6e7ed096fdeedd9f0d23b94190ecf418da09cf9c9b6caee5821ba1c457f0294063bbc9e                                                                                                                                                                                                        |
| SSDEEP:               | 196608:l3ksPqmzcl+LG314Hujb7KgkYCbGNBmHTER:lUON+2HBb8                                                                                                                                                                                                                                                                                   |
| TLSH:                 | 5776332F16980415E4EECC3A85EBBE9132F5073A9E8278BCA5DA5DC13A354F5B702163                                                                                                                                                                                                                                                                  |
| File Content Preview: | MZ.....@.....!..L!This program cannot be run in DOS mode....\$.L...8.ob.....!...."....@.....=XT.....@.....Ft...../..E..                                                                                                                                                                                                                 |

| File Icon                                                                           |                  |
|-------------------------------------------------------------------------------------|------------------|
|  |                  |
| Icon Hash:                                                                          | b99988fcd4f66e0f |

| Static PE Info              |                                                                               |
|-----------------------------|-------------------------------------------------------------------------------|
| General                     |                                                                               |
| Entrypoint:                 | 0x1054583d                                                                    |
| Entrypoint Section:         | nUPwRZiK                                                                      |
| Digitally signed:           | true                                                                          |
| Imagebase:                  | 0x10000000                                                                    |
| Subsystem:                  | windows gui                                                                   |
| Image File Characteristics: | EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, DLL |
| DLL Characteristics:        |                                                                               |

|                          |                                          |
|--------------------------|------------------------------------------|
| Time Stamp:              | 0x626FE238 [Mon May 2 13:52:56 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:             | d3a98daa37dbe78969711cc1194ce51b         |

### Authenticode Signature

|                             |                                                                                                                       |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Signature Valid:            | <b>false</b>                                                                                                          |
| Signature Issuer:           | CN=fumblng corp.                                                                                                      |
| Signature Validation Error: | <b>A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider</b> |
| Error Number:               | -2146762487                                                                                                           |
| Not Before, Not After       | <ul style="list-style-type: none"><li>12/8/2022 9:12:34 AM 12/8/2023 9:32:34 AM</li></ul>                             |
| Subject Chain               | <ul style="list-style-type: none"><li>CN=fumblng corp.</li></ul>                                                      |
| Version:                    | 3                                                                                                                     |
| Thumbprint MD5:             | BFCF38BCEDDC6D492EE1D807C07B0E02                                                                                      |
| Thumbprint SHA-1:           | 92A18235585F157E75D33B92CC8E394210AEAD16                                                                              |
| Thumbprint SHA-256:         | E3FCBA8CB056D8C4B5F3C974DD82C3CD9C96AF2621722C26119E478F35637E99                                                      |
| Serial:                     | 78919934276F458544703D1C7FC21303                                                                                      |

### Entrypoint Preview

| Instruction                            |
|----------------------------------------|
| push edx                               |
| mov edx, 3F442022h                     |
| pushfd                                 |
| xor edx, 7B9D646Dh                     |
| xor dl, dl                             |
| mov edx, dword ptr [esp+edx-44D943FCh] |
| mov dword ptr [esp+04h], 8EECC51Ah     |
| push dword ptr [esp+00h]               |
| popfd                                  |
| lea esp, dword ptr [esp+04h]           |
| call 00007F36F8B8AD93h                 |
| xchg al, al                            |
| pushfd                                 |
| lahf                                   |
| shr al, FFFFFFF8Fh                     |
| shl ah, FFFFFFF86h                     |
| pop dword ptr [edi]                    |
| bt eax, ecx                            |
| and ax, 00007B5Bh                      |
| xchg al, ah                            |
| mov eax, dword ptr [esi]               |
| cmp si, bp                             |
| lea esi, dword ptr [esi+00000004h]     |
| xor eax, ebx                           |
| jmp 00007F36F8C42417h                  |
| stosb                                  |
| retf A814h                             |
| jmp far 0F97h : 3CD32403h              |
| stosd                                  |
| enter B68Dh, 01h                       |
| add byte ptr [eax], al                 |
| add cl, al                             |
| loopne 00007F36F8BAE893h               |
| xor cl, bl                             |

| Instruction                        |
|------------------------------------|
| btr ax, dx                         |
| or ax, bp                          |
| not cl                             |
| add al, ah                         |
| bts eax, ebp                       |
| sar al, cl                         |
| add cl, 0000007Eh                  |
| shld ax, si, 00000065h             |
| bts ax, sp                         |
| not ah                             |
| xor cl, 0000006Bh                  |
| cmovno ax, dx                      |
| movsx eax, si                      |
| rol ax, 0000h                      |
| rol cl, 1                          |
| cmovno ax, bx                      |
| xor bl, cl                         |
| movzx eax, dx                      |
| lahf                               |
| lea edi, dword ptr [edi-00000002h] |
| btr ax, 0046h                      |
| sal al, FFFFFFF9Dh                 |
| mov word ptr [edi], cx             |
| mov eax, dword ptr [esi]           |
| add esi, 00000004h                 |
| jmp 00007F36F8AD6A41h              |
| push ebp                           |
| ret                                |
| rol eax, 1                         |
| sub eax, 000066B4h                 |

| Data Directories                     |                 |              |               |
|--------------------------------------|-----------------|--------------|---------------|
| Name                                 | Virtual Address | Virtual Size | Is in Section |
| IMAGE_DIRECTORY_ENTRY_EXPORT         | 0xaf2fa4        | 0x45         | nUPwRZiK      |
| IMAGE_DIRECTORY_ENTRY_IMPORT         | 0x660b3c        | 0x104        | nUPwRZiK      |
| IMAGE_DIRECTORY_ENTRY_RESOURCE       | 0xb6a000        | 0x800        | K)'tLNvc      |
| IMAGE_DIRECTORY_ENTRY_EXCEPTION      | 0x0             | 0x0          |               |
| IMAGE_DIRECTORY_ENTRY_SECURITY       | 0x735e00        | 0x16d0       | nUPwRZiK      |
| IMAGE_DIRECTORY_ENTRY_BASERELOC      | 0xb69000        | 0x5d4        | \$u!6XeN&     |
| 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            | 0x433000        | 0x78         | 0Ys"rSd       |
| 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                                               |
| *;>%1sXO | 0x1000          | 0x219c       | 0x0      | False    | 0               | empty     | 0.0     | IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ |
| 7rP!Ni:j | 0x4000          | 0x845        | 0x0      | False    | 0               | empty     | 0.0     | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ            |

| Name      | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity     | File Type          | Entropy            | Characteristics                                                               |
|-----------|-----------------|--------------|----------|----------|---------------------|--------------------|--------------------|-------------------------------------------------------------------------------|
| bKE<E278  | 0x5000          | 0x250        | 0x0      | False    | 0                   | empty              | 0.0                | IMAGE_SCN_CNT_INITIALIZED_DATA,<br>IMAGE_SCN_MEM_READ,<br>IMAGE_SCN_MEM_WRITE |
| 8*7" Joyq | 0x6000          | 0x42c264     | 0x0      | unknown  | unknown             | unknown            | unknown            | IMAGE_SCN_CNT_CODE,<br>IMAGE_SCN_MEM_EXECUTE,<br>IMAGE_SCN_MEM_READ           |
| 0Ys""rSd  | 0x433000        | 0x4a4        | 0x600    | False    | 0.06575520833333333 | OpenPGP Public Key | 0.4141326418166997 | IMAGE_SCN_CNT_INITIALIZED_DATA,<br>IMAGE_SCN_MEM_READ,<br>IMAGE_SCN_MEM_WRITE |
| nUPwRZiK  | 0x434000        | 0x734590     | 0x734600 | unknown  | unknown             | unknown            | unknown            | IMAGE_SCN_CNT_CODE,<br>IMAGE_SCN_MEM_EXECUTE,<br>IMAGE_SCN_MEM_READ           |
| \$uI6XeN& | 0xb69000        | 0x5d4        | 0x600    | False    | 0.53515625          | data               | 4.2912698570834    | IMAGE_SCN_CNT_INITIALIZED_DATA,<br>IMAGE_SCN_MEM_READ                         |
| K)'tLNvc  | 0xb6a000        | 0x800        | 0x800    | False    | 0.44287109375       | data               | 3.8514204088109953 | IMAGE_SCN_CNT_INITIALIZED_DATA,<br>IMAGE_SCN_MEM_READ                         |

| Resources     |          |       |                                                                |          |               |
|---------------|----------|-------|----------------------------------------------------------------|----------|---------------|
| Name          | RVA      | Size  | Type                                                           | Language | Country       |
| RT_ICON       | 0xb6a0fc | 0x2e8 | Device independent bitmap graphic, 32 x 64 x 4, image size 512 | Dutch    | Netherlands   |
| RT_GROUP_ICON | 0xb6a3e4 | 0x14  | data                                                           | Dutch    | Netherlands   |
| RT_VERSION    | 0xb6a3f8 | 0x408 | data                                                           | English  | United States |

| Imports      |                                                                                                        |
|--------------|--------------------------------------------------------------------------------------------------------|
| DLL          | Import                                                                                                 |
| user32.dll   | SendMessageA                                                                                           |
| kernel32.dll | LocalFree                                                                                              |
| advapi32.dll | GetSidSubAuthority                                                                                     |
| wsock32.dll  | WSAStartup                                                                                             |
| shell32.dll  | CommandLineToArgvW                                                                                     |
| ws2_32.dll   | freeaddrinfo                                                                                           |
| ole32.dll    | CoUninitialize                                                                                         |
| secur32.dll  | GetUserNameExA                                                                                         |
| psapi.dll    | GetModuleFileNameExA                                                                                   |
| kernel32.dll | GetSystemTimeAsFileTime                                                                                |
| user32.dll   | CharUpperBuffW                                                                                         |
| kernel32.dll | LocalAlloc, LocalFree, GetModuleFileNameW, ExitProcess, LoadLibraryA, GetModuleHandleA, GetProcAddress |

| Exports |         |            |
|---------|---------|------------|
| Name    | Ordinal | Address    |
| rundll  | 1       | 0x1000100c |

| Possible Origin                |                                  |                                                                                       |
|--------------------------------|----------------------------------|---------------------------------------------------------------------------------------|
| Language of compilation system | Country where language is spoken | Map                                                                                   |
| Dutch                          | Netherlands                      |  |
| English                        | United States                    |  |

# Network Behavior

## TCP Packets

| Timestamp                          | Source Port | Dest Port | Source IP     | Dest IP       |
|------------------------------------|-------------|-----------|---------------|---------------|
| Dec 9, 2022 10:52:05.048599958 CET | 49698       | 4193      | 192.168.2.3   | 89.22.236.225 |
| Dec 9, 2022 10:52:05.074860096 CET | 4193        | 49698     | 89.22.236.225 | 192.168.2.3   |
| Dec 9, 2022 10:52:05.075001955 CET | 49698       | 4193      | 192.168.2.3   | 89.22.236.225 |
| Dec 9, 2022 10:52:05.076816082 CET | 49698       | 4193      | 192.168.2.3   | 89.22.236.225 |
| Dec 9, 2022 10:52:05.102937937 CET | 4193        | 49698     | 89.22.236.225 | 192.168.2.3   |
| Dec 9, 2022 10:52:05.162826061 CET | 49699       | 4193      | 192.168.2.3   | 89.22.236.225 |
| Dec 9, 2022 10:52:05.188915968 CET | 4193        | 49699     | 89.22.236.225 | 192.168.2.3   |
| Dec 9, 2022 10:52:05.189066887 CET | 49699       | 4193      | 192.168.2.3   | 89.22.236.225 |
| Dec 9, 2022 10:52:05.190913916 CET | 49699       | 4193      | 192.168.2.3   | 89.22.236.225 |
| Dec 9, 2022 10:52:05.216546059 CET | 4193        | 49699     | 89.22.236.225 | 192.168.2.3   |
| Dec 9, 2022 10:52:09.218707085 CET | 49700       | 4193      | 192.168.2.3   | 89.22.236.225 |
| Dec 9, 2022 10:52:09.245634079 CET | 4193        | 49700     | 89.22.236.225 | 192.168.2.3   |
| Dec 9, 2022 10:52:09.245754957 CET | 49700       | 4193      | 192.168.2.3   | 89.22.236.225 |
| Dec 9, 2022 10:52:09.262767076 CET | 49700       | 4193      | 192.168.2.3   | 89.22.236.225 |
| Dec 9, 2022 10:52:09.288966894 CET | 4193        | 49700     | 89.22.236.225 | 192.168.2.3   |
| Dec 9, 2022 10:53:07.081410885 CET | 4193        | 49699     | 89.22.236.225 | 192.168.2.3   |
| Dec 9, 2022 10:53:07.081504107 CET | 49699       | 4193      | 192.168.2.3   | 89.22.236.225 |
| Dec 9, 2022 10:53:07.081511974 CET | 4193        | 49698     | 89.22.236.225 | 192.168.2.3   |
| Dec 9, 2022 10:53:07.081585884 CET | 49698       | 4193      | 192.168.2.3   | 89.22.236.225 |
| Dec 9, 2022 10:53:11.177726030 CET | 4193        | 49700     | 89.22.236.225 | 192.168.2.3   |
| Dec 9, 2022 10:53:11.177835941 CET | 49700       | 4193      | 192.168.2.3   | 89.22.236.225 |
| Dec 9, 2022 10:54:08.521687984 CET | 4193        | 49699     | 89.22.236.225 | 192.168.2.3   |
| Dec 9, 2022 10:54:08.522161961 CET | 49699       | 4193      | 192.168.2.3   | 89.22.236.225 |
| Dec 9, 2022 10:54:08.522314072 CET | 4193        | 49698     | 89.22.236.225 | 192.168.2.3   |
| Dec 9, 2022 10:54:08.522413969 CET | 49698       | 4193      | 192.168.2.3   | 89.22.236.225 |
| Dec 9, 2022 10:54:12.618275881 CET | 4193        | 49700     | 89.22.236.225 | 192.168.2.3   |
| Dec 9, 2022 10:54:12.618397951 CET | 49700       | 4193      | 192.168.2.3   | 89.22.236.225 |
| Dec 9, 2022 10:55:09.961476088 CET | 4193        | 49699     | 89.22.236.225 | 192.168.2.3   |
| Dec 9, 2022 10:55:09.961595058 CET | 49699       | 4193      | 192.168.2.3   | 89.22.236.225 |
| Dec 9, 2022 10:55:09.961711884 CET | 4193        | 49698     | 89.22.236.225 | 192.168.2.3   |
| Dec 9, 2022 10:55:09.961854935 CET | 49698       | 4193      | 192.168.2.3   | 89.22.236.225 |
| Dec 9, 2022 10:55:14.058015108 CET | 4193        | 49700     | 89.22.236.225 | 192.168.2.3   |
| Dec 9, 2022 10:55:14.058202982 CET | 49700       | 4193      | 192.168.2.3   | 89.22.236.225 |
| Dec 9, 2022 10:56:11.402008057 CET | 4193        | 49699     | 89.22.236.225 | 192.168.2.3   |
| Dec 9, 2022 10:56:11.402087927 CET | 49699       | 4193      | 192.168.2.3   | 89.22.236.225 |
| Dec 9, 2022 10:56:11.402550936 CET | 4193        | 49698     | 89.22.236.225 | 192.168.2.3   |
| Dec 9, 2022 10:56:11.402653933 CET | 49698       | 4193      | 192.168.2.3   | 89.22.236.225 |

## Statistics

### Behavior

- loadll32.exe
- conhost.exe
- cmd.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe

 Click to jump to process

## System Behavior

**Analysis Process: loaddll32.exe** PID: 5288, Parent PID: 3452

### General

|                               |                                                      |
|-------------------------------|------------------------------------------------------|
| Target ID:                    | 0                                                    |
| Start time:                   | 10:52:02                                             |
| Start date:                   | 09/12/2022                                           |
| Path:                         | C:\Windows\System32\loaddll32.exe                    |
| Wow64 process (32bit):        | true                                                 |
| Commandline:                  | loaddll32.exe "C:\Users\user\Desktop\6k00SOeMjU.dll" |
| Imagebase:                    | 0xdc0000                                             |
| File size:                    | 116736 bytes                                         |
| MD5 hash:                     | 1F562FBF37040EC6C43C8D5EF619EA39                     |
| Has elevated privileges:      | true                                                 |
| Has administrator privileges: | true                                                 |
| Programmed in:                | C, C++ or other language                             |
| Reputation:                   | moderate                                             |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

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

**Analysis Process: conhost.exe** PID: 5260, Parent PID: 5288

### General

|                               |                                                     |
|-------------------------------|-----------------------------------------------------|
| Target ID:                    | 1                                                   |
| Start time:                   | 10:52:02                                            |
| Start date:                   | 09/12/2022                                          |
| Path:                         | C:\Windows\System32\conhost.exe                     |
| Wow64 process (32bit):        | false                                               |
| Commandline:                  | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase:                    | 0x7f745070000                                       |
| File size:                    | 625664 bytes                                        |
| MD5 hash:                     | EA777DEEA782E8B4D7C7C33BBF8A4496                    |
| Has elevated privileges:      | true                                                |
| Has administrator privileges: | true                                                |
| Programmed in:                | C, C++ or other language                            |

|             |      |
|-------------|------|
| Reputation: | high |
|-------------|------|

## Analysis Process: cmd.exe PID: 5316, Parent PID: 5288

### General

|                               |                                                                   |
|-------------------------------|-------------------------------------------------------------------|
| Target ID:                    | 2                                                                 |
| Start time:                   | 10:52:02                                                          |
| Start date:                   | 09/12/2022                                                        |
| Path:                         | C:\Windows\SysWOW64\cmd.exe                                       |
| Wow64 process (32bit):        | true                                                              |
| Commandline:                  | cmd.exe /C rundll32.exe "C:\Users\user\Desktop\6k00SOeMjU.dll",#1 |
| Imagebase:                    | 0xb0000                                                           |
| 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 **Show Windows Behavior** to show it.

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

## Analysis Process: rundll32.exe PID: 5448, Parent PID: 5288

### General

|                               |                                                                                                                                                                                                                                                                                                                     |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Target ID:                    | 3                                                                                                                                                                                                                                                                                                                   |
| Start time:                   | 10:52:02                                                                                                                                                                                                                                                                                                            |
| Start date:                   | 09/12/2022                                                                                                                                                                                                                                                                                                          |
| Path:                         | C:\Windows\SysWOW64\rundll32.exe                                                                                                                                                                                                                                                                                    |
| Wow64 process (32bit):        | true                                                                                                                                                                                                                                                                                                                |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\6k00SOeMjU.dll,rundll                                                                                                                                                                                                                                                            |
| Imagebase:                    | 0x1060000                                                                                                                                                                                                                                                                                                           |
| File size:                    | 61952 bytes                                                                                                                                                                                                                                                                                                         |
| MD5 hash:                     | D7CA562B0DB4F4DD0F03A89A1FDAD63D                                                                                                                                                                                                                                                                                    |
| Has elevated privileges:      | true                                                                                                                                                                                                                                                                                                                |
| Has administrator privileges: | true                                                                                                                                                                                                                                                                                                                |
| Programmed in:                | C, C++ or other language                                                                                                                                                                                                                                                                                            |
| Yara matches:                 | <ul style="list-style-type: none"> <li>Rule: EXT_MAL_SystemBC_Mar22_1, Description: Detects unpacked SystemBC module as used by Emotet in March 2022, Source: 00000003.00000002.764685317.0000000010005000.00000004.00000001.01000000.00000003.sdmp, Author: Thomas Barabosch, Deutsche Telekom Security</li> </ul> |
| Reputation:                   | high                                                                                                                                                                                                                                                                                                                |

## Analysis Process: rundll32.exe PID: 5476, Parent PID: 5316

### General

|                          |                                                        |
|--------------------------|--------------------------------------------------------|
| Target ID:               | 4                                                      |
| Start time:              | 10:52:02                                               |
| Start date:              | 09/12/2022                                             |
| Path:                    | C:\Windows\SysWOW64\rundll32.exe                       |
| Wow64 process (32bit):   | true                                                   |
| Commandline:             | rundll32.exe "C:\Users\user\Desktop\6k00SOeMjU.dll",#1 |
| Imagebase:               | 0x1060000                                              |
| File size:               | 61952 bytes                                            |
| MD5 hash:                | D7CA562B0DB4F4DD0F03A89A1FDAD63D                       |
| Has elevated privileges: | true                                                   |

|                               |                                                                                                                                                                                                                                                                                                                     |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Has administrator privileges: | true                                                                                                                                                                                                                                                                                                                |
| Programmed in:                | C, C++ or other language                                                                                                                                                                                                                                                                                            |
| Yara matches:                 | <ul style="list-style-type: none"> <li>Rule: EXT_MAL_SystemBC_Mar22_1, Description: Detects unpacked SystemBC module as used by Emotet in March 2022, Source: 00000004.00000002.764666285.0000000010005000.00000004.00000001.01000000.00000003.sdmp, Author: Thomas Barabosch, Deutsche Telekom Security</li> </ul> |
| Reputation:                   | high                                                                                                                                                                                                                                                                                                                |

## Analysis Process: rundll32.exe PID: 3920, Parent PID: 5288

### General

|                               |                                                                                                                                                                                                                                                                                                                     |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Target ID:                    | 5                                                                                                                                                                                                                                                                                                                   |
| Start time:                   | 10:52:07                                                                                                                                                                                                                                                                                                            |
| Start date:                   | 09/12/2022                                                                                                                                                                                                                                                                                                          |
| Path:                         | C:\Windows\SysWOW64\rundll32.exe                                                                                                                                                                                                                                                                                    |
| Wow64 process (32bit):        | true                                                                                                                                                                                                                                                                                                                |
| Commandline:                  | rundll32.exe "C:\Users\user\Desktop\6k00SOeMjU.dll",rundll                                                                                                                                                                                                                                                          |
| Imagebase:                    | 0x1060000                                                                                                                                                                                                                                                                                                           |
| File size:                    | 61952 bytes                                                                                                                                                                                                                                                                                                         |
| MD5 hash:                     | D7CA562B0DB4F4DD0F03A89A1FDAD63D                                                                                                                                                                                                                                                                                    |
| Has elevated privileges:      | true                                                                                                                                                                                                                                                                                                                |
| Has administrator privileges: | true                                                                                                                                                                                                                                                                                                                |
| Programmed in:                | C, C++ or other language                                                                                                                                                                                                                                                                                            |
| Yara matches:                 | <ul style="list-style-type: none"> <li>Rule: EXT_MAL_SystemBC_Mar22_1, Description: Detects unpacked SystemBC module as used by Emotet in March 2022, Source: 00000005.00000002.764703413.0000000010005000.00000004.00000001.01000000.00000003.sdmp, Author: Thomas Barabosch, Deutsche Telekom Security</li> </ul> |
| Reputation:                   | high                                                                                                                                                                                                                                                                                                                |

### Disassembly

 No disassembly