

JoeSandbox Cloud BASIC



ID: 492188

Sample Name: OG0AO3HYEI.dll

Cookbook: default.jbs

Time: 13:17:48

Date: 28/09/2021

Version: 33.0.0 White Diamond

Table of Contents

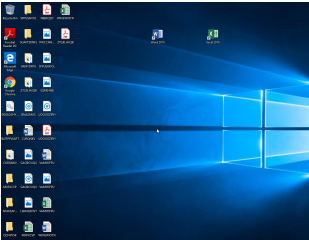
Table of Contents	2
Windows Analysis Report 0G0AO3HYEI.dll	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Overview	5
Memory Dumps	5
Sigma Overview	5
Jbx Signature Overview	5
AV Detection:	5
E-Banking Fraud:	5
System Summary:	5
Malware Analysis System Evasion:	5
HIPS / PFW / Operating System Protection Evasion:	5
Mitre Att&ck Matrix	5
Behavior Graph	6
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	8
Domains and IPs	9
Contacted Domains	9
URLs from Memory and Binaries	9
Contacted IPs	9
General Information	9
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASN	10
JA3 Fingerprints	10
Dropped Files	10
Created / dropped Files	10
Static File Info	10
General	10
File Icon	10
Static PE Info	11
General	11
Entrypoint Preview	11
Data Directories	11
Sections	11
Resources	12
Imports	12
Exports	12
Version Infos	12
Possible Origin	12
Network Behavior	12
Network Port Distribution	12
UDP Packets	12
Code Manipulations	12
Statistics	12
Behavior	12
System Behavior	13
Analysis Process: loadll64.exe PID: 396 Parent PID: 6692	13
General	13
File Activities	13
Analysis Process: cmd.exe PID: 5468 Parent PID: 396	13
General	13
File Activities	13
Analysis Process: rundll32.exe PID: 5612 Parent PID: 396	13
General	13
File Activities	14
File Read	14
Analysis Process: rundll32.exe PID: 4716 Parent PID: 5468	14
General	14
File Activities	14

File Read	14
Analysis Process: explorer.exe PID: 3440 Parent PID: 5612	14
General	14
Analysis Process: rundll32.exe PID: 7056 Parent PID: 396	14
General	14
File Activities	15
File Read	15
Analysis Process: rundll32.exe PID: 5184 Parent PID: 396	15
General	15
File Activities	15
File Read	15
Analysis Process: rundll32.exe PID: 1360 Parent PID: 396	15
General	15
File Activities	15
File Read	15
Analysis Process: explorer.exe PID: 7080 Parent PID: 568	16
General	16
File Activities	16
Registry Activities	16
Analysis Process: rundll32.exe PID: 1520 Parent PID: 396	16
General	16
Analysis Process: rundll32.exe PID: 3912 Parent PID: 396	16
General	16
Analysis Process: rundll32.exe PID: 5624 Parent PID: 396	17
General	17
Analysis Process: rundll32.exe PID: 6764 Parent PID: 396	17
General	17
Analysis Process: rundll32.exe PID: 2892 Parent PID: 396	17
General	17
Analysis Process: rundll32.exe PID: 3444 Parent PID: 396	17
General	17
Analysis Process: explorer.exe PID: 3208 Parent PID: 568	18
General	18
Analysis Process: rundll32.exe PID: 784 Parent PID: 396	18
General	18
Analysis Process: rundll32.exe PID: 3692 Parent PID: 396	18
General	18
Analysis Process: rundll32.exe PID: 348 Parent PID: 396	19
General	19
Analysis Process: rundll32.exe PID: 6296 Parent PID: 396	19
General	19
Analysis Process: rundll32.exe PID: 3440 Parent PID: 396	19
General	19
Analysis Process: rundll32.exe PID: 2384 Parent PID: 396	19
General	20
Analysis Process: rundll32.exe PID: 2152 Parent PID: 396	20
General	20
Analysis Process: explorer.exe PID: 5252 Parent PID: 568	20
General	20
Analysis Process: rundll32.exe PID: 1148 Parent PID: 396	20
General	20
Analysis Process: rundll32.exe PID: 4224 Parent PID: 396	21
General	21
Analysis Process: rundll32.exe PID: 1432 Parent PID: 396	21
General	21
Disassembly	21
Code Analysis	21

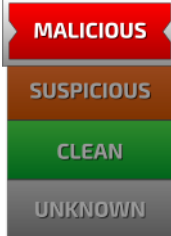
Windows Analysis Report 0G0AO3HYEI.dll

Overview

General Information

Sample Name:	0G0AO3HYEi.dll
Analysis ID:	492188
MD5:	c50f692a715db80..
SHA1:	229b257301ed99..
SHA256:	ff3aa75e4d46375..
Tags:	Dridex exe
Infos:	   
Most interesting Screenshot:	
	

Detection



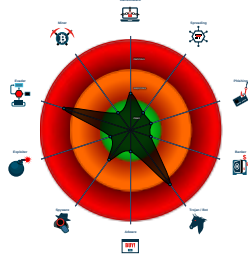
Dridex

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Dridex unpacked file
- Multi AV Scanner detection for subm...
- Queues an APC in another process ...
- PE file has nameless sections
- Potential time zone aware malware
- Uses Windows timers to delay exec...
- May sleep (evasive loops) to hinder ...
- Uses code obfuscation techniques (...)
- PE file contains sections with non-s...
- Queries the installation date of Wind...
- Detected potential crypto function
- Sample execution stops while proce...

Classification



Process Tree

- ```

System is w10x64
•  loadll64.exe (PID: 396 cmdline: loadll64.exe "C:\Users\user\Desktop\0G0AO3HYEI.dll" MD5: A84133CCB118CF35D49A423CD836D0EF)
 •  cmd.exe (PID: 5468 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\0G0AO3HYEI.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
 •  rundll32.exe (PID: 4716 cmdline: rundll32.exe "C:\Users\user\Desktop\0G0AO3HYEI.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
 •  rundll32.exe (PID: 5612 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,CheckDriverSoftwareDependenciesSatisfied MD5: 73C519F050C20580F8A62C849D49215A)
 •  explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
 •  rundll32.exe (PID: 7056 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DeviceInternetSettingUiW MD5: 73C519F050C20580F8A62C849D49215A)
 •  rundll32.exe (PID: 5184 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DilnstallDevice MD5: 73C519F050C20580F8A62C849D49215A)
 •  rundll32.exe (PID: 1360 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DilnstallDriverA MD5: 73C519F050C20580F8A62C849D49215A)
 •  rundll32.exe (PID: 1520 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DilnstallDriverW MD5: 73C519F050C20580F8A62C849D49215A)
 •  rundll32.exe (PID: 3912 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiRollbackDriver MD5: 73C519F050C20580F8A62C849D49215A)
 •  rundll32.exe (PID: 5624 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiShowUpdateDevice MD5: 73C519F050C20580F8A62C849D49215A)
 •  rundll32.exe (PID: 6764 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiShowUpdateDriver MD5: 73C519F050C20580F8A62C849D49215A)
 •  rundll32.exe (PID: 2892 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiUninstallDevice MD5: 73C519F050C20580F8A62C849D49215A)
 •  rundll32.exe (PID: 3444 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiUninstallDriverA MD5: 73C519F050C20580F8A62C849D49215A)
 •  rundll32.exe (PID: 784 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiUninstallDriverW MD5: 73C519F050C20580F8A62C849D49215A)
 •  rundll32.exe (PID: 3692 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,GetInternetPolicies MD5: 73C519F050C20580F8A62C849D49215A)
 •  rundll32.exe (PID: 348 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,InstallNewDevice MD5: 73C519F050C20580F8A62C849D49215A)
 •  rundll32.exe (PID: 6296 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,InstallSelectedDriver MD5: 73C519F050C20580F8A62C849D49215A)
 •  rundll32.exe (PID: 3440 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,InstallWindowsUpdateDriver MD5: 73C519F050C20580F8A62C849D49215A)
 •  rundll32.exe (PID: 2384 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,InstallWindowsUpdateDriverEx MD5: 73C519F050C20580F8A62C849D49215A)
 •  rundll32.exe (PID: 2152 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,InstallWindowsUpdateDrivers MD5: 73C519F050C20580F8A62C849D49215A)
 •  rundll32.exe (PID: 1148 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,QueryWindowsUpdateDriverStatus MD5: 73C519F050C20580F8A62C849D49215A)
 •  rundll32.exe (PID: 4224 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,SetInternetPolicies MD5: 73C519F050C20580F8A62C849D49215A)
 •  rundll32.exe (PID: 1432 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,UpdateDriverForPlugAndPlayDevicesA MD5: 73C519F050C20580F8A62C849D49215A)
 •  explorer.exe (PID: 7080 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
 •  explorer.exe (PID: 3208 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
 •  explorer.exe (PID: 5252 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
• cleanup

```

## Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

| Source                                                              | Rule                 | Description                        | Author       | Strings |
|---------------------------------------------------------------------|----------------------|------------------------------------|--------------|---------|
| 00000024.00000002.750032138.0000000140001000.00000020.00020000.sdmp | JoeSecurity_Dridex_2 | Yara detected Dridex unpacked file | Joe Security |         |
| 0000001B.00000002.749674160.0000000140001000.00000020.00020000.sdmp | JoeSecurity_Dridex_2 | Yara detected Dridex unpacked file | Joe Security |         |
| 00000008.00000002.748754528.0000000140001000.00000020.00020000.sdmp | JoeSecurity_Dridex_2 | Yara detected Dridex unpacked file | Joe Security |         |
| 0000000B.00000002.749145318.0000000140001000.00000020.00020000.sdmp | JoeSecurity_Dridex_2 | Yara detected Dridex unpacked file | Joe Security |         |
| 00000029.00000002.750110395.0000000140001000.00000020.00020000.sdmp | JoeSecurity_Dridex_2 | Yara detected Dridex unpacked file | Joe Security |         |
| Click to see the 6 entries                                          |                      |                                    |              |         |

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

 Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

E-Banking Fraud:



Yara detected Dridex unpacked file

System Summary:



PE file has nameless sections

Malware Analysis System Evasion:



Potential time zone aware malware

Uses Windows timers to delay execution

HIPS / PFW / Operating System Protection Evasion:



Queues an APC in another process (thread injection)

Mitre Att&ck Matrix

| Initial Access                      | Execution                          | Persistence                          | Privilege Escalation                 | Defense Evasion                    | Credential Access           | Discovery                          | Lateral Movement                   | Collection                     | Exfiltration                                             | Command and Control        |
|-------------------------------------|------------------------------------|--------------------------------------|--------------------------------------|------------------------------------|-----------------------------|------------------------------------|------------------------------------|--------------------------------|----------------------------------------------------------|----------------------------|
| Valid Accounts                      | Windows Management Instrumentation | Path Interception                    | Process Injection 1 1 2              | Masquerading 1                     | OS Credential Dumping       | System Time Discovery 1            | Remote Services                    | Archive Collected Data 1       | Exfiltration Over Other Network Medium                   | Encrypted Channel 1        |
| Default Accounts                    | Scheduled Task/Job                 | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Virtualization/Sandbox Evasion 1 2 | LSASS Memory                | Query Registry 1                   | Remote Desktop Protocol            | Data from Removable Media      | Exfiltration Over Bluetooth                              | Junk Data                  |
| Domain Accounts                     | At (Linux)                         | Logon Script (Windows)               | Logon Script (Windows)               | Process Injection 1 1 2            | Security Account Manager    | Security Software Discovery 1 1    | SMB/Windows Admin Shares           | Data from Network Shared Drive | Automated Exfiltration                                   | Steganography              |
| Local Accounts                      | At (Windows)                       | Logon Script (Mac)                   | Logon Script (Mac)                   | Obfuscated Files or Information 2  | NTDS                        | Virtualization/Sandbox Evasion 1 2 | Distributed Component Object Model | Input Capture                  | Scheduled Transfer                                       | Protocol Impersonation     |
| Cloud Accounts                      | Cron                               | Network Logon Script                 | Network Logon Script                 | Rundll32 1                         | LSA Secrets                 | Process Discovery 2                | SSH                                | Keylogging                     | Data Transfer Size Limits                                | Fallback Channels          |
| Replication Through Removable Media | Launchd                            | Rc.common                            | Rc.common                            | Software Packing 2                 | Cached Domain Credentials   | Application Window Discovery 1     | VNC                                | GUI Input Capture              | Exfiltration Over C2 Channel                             | Multiband Communication    |
| External Remote Services            | Scheduled Task                     | Startup Items                        | Startup Items                        | Compile After Delivery             | DCSync                      | Account Discovery 1                | Windows Remote Management          | Web Portal Capture             | Exfiltration Over Alternative Protocol                   | Commonly Used Port         |
| Drive-by Compromise                 | Command and Scripting Interpreter  | Scheduled Task/Job                   | Scheduled Task/Job                   | Indicator Removal from Tools       | Proc Filesystem             | System Owner/User Discovery 1      | Shared Webroot                     | Credential API Hooking         | Exfiltration Over Symmetric Encrypted Non-C2 Protocol    | Application Layer Protocol |
| Exploit Public-Facing Application   | PowerShell                         | At (Linux)                           | At (Linux)                           | Masquerading                       | /etc/passwd and /etc/shadow | File and Directory Discovery 2     | Software Deployment Tools          | Data Staged                    | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol   | Web Protocol               |
| Supply Chain Compromise             | AppleScript                        | At (Windows)                         | At (Windows)                         | Invalid Code Signature             | Network Sniffing            | System Information Discovery 1 3   | Taint Shared Content               | Local Data Staging             | Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol | File Transfer Protocols    |

## Behavior Graph

## Thumbnails



## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source         | Detection | Scanner       | Label               | Link                   |
|----------------|-----------|---------------|---------------------|------------------------|
| OG0AO3HYEI.dll | 59%       | Virustotal    |                     | <a href="#">Browse</a> |
| OG0AO3HYEI.dll | 62%       | ReversingLabs | Win64.Trojan.Injexa |                        |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

No Antivirus matches

## Domains and IPs

### Contacted Domains

No contacted domains info

### URLs from Memory and Binaries

### Contacted IPs

No contacted IP infos

## General Information

|                                                    |                                                                                                                                                                                                                                     |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Joe Sandbox Version:                               | 33.0.0 White Diamond                                                                                                                                                                                                                |
| Analysis ID:                                       | 492188                                                                                                                                                                                                                              |
| Start date:                                        | 28.09.2021                                                                                                                                                                                                                          |
| Start time:                                        | 13:17:48                                                                                                                                                                                                                            |
| Joe Sandbox Product:                               | CloudBasic                                                                                                                                                                                                                          |
| Overall analysis duration:                         | 0h 14m 37s                                                                                                                                                                                                                          |
| Hypervisor based Inspection enabled:               | false                                                                                                                                                                                                                               |
| Report type:                                       | light                                                                                                                                                                                                                               |
| Sample file name:                                  | 0G0AO3HYEI.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: | 41                                                                                                                                                                                                                                  |
| 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@48/0@0/0                                                                                                                                                                                                     |
| EGA Information:                                   | Failed                                                                                                                                                                                                                              |
| HDC Information:                                   | <ul style="list-style-type: none"><li>• Successful, ratio: 19.6% (good quality ratio 17.4%)</li><li>• Quality average: 82.8%</li><li>• Quality standard deviation: 33.2%</li></ul>                                                  |
| HCA Information:                                   | Failed                                                                                                                                                                                                                              |
| Cookbook Comments:                                 | <ul style="list-style-type: none"><li>• Adjust boot time</li><li>• Enable AMSI</li><li>• Sleeps bigger than 120000ms are automatically reduced to 1000ms</li><li>• Found application associated with file extension: .dll</li></ul> |
| Warnings:                                          | Show All                                                                                                                                                                                                                            |

## Simulations

### Behavior and APIs

| Time     | Type            | Description                                       |
|----------|-----------------|---------------------------------------------------|
| 13:19:08 | API Interceptor | 15x Sleep call for process: explorer.exe modified |

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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) x86-64, for MS Windows                                                                                                                                                                                                                                                                                 |
| Entropy (8bit):       | 5.0210157653928675                                                                                                                                                                                                                                                                                                                  |
| TrID:                 | <ul style="list-style-type: none"><li>Win64 Dynamic Link Library (generic) (102004/3) 86.43%</li><li>Win64 Executable (generic) (12005/4) 10.17%</li><li>Generic Win/DOS Executable (2004/3) 1.70%</li><li>DOS Executable Generic (2002/1) 1.70%</li><li>Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%</li></ul> |
| File name:            | OG0AO3HYEI.dll                                                                                                                                                                                                                                                                                                                      |
| File size:            | 1110016                                                                                                                                                                                                                                                                                                                             |
| MD5:                  | c50f692a715db805e68e9655ff6a9ab2                                                                                                                                                                                                                                                                                                    |
| SHA1:                 | 229b257301ed99d518364afd22c4276daa5b3d20                                                                                                                                                                                                                                                                                            |
| SHA256:               | ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033                                                                                                                                                                                                                                                                    |
| SHA512:               | ad74f556cce1f8fd4a3c18a18c27adcafd2f552025bf7f83864261c6944db5423c719ea161c341e593800499c6e01aba846031e79caf1e771b2b16e7d6e33d1                                                                                                                                                                                                     |
| SSDEEP:               | 12288:4dMlwS97wJs6tSKDXEabXaC+jhc1S8XXk7CZzHsZH9dq0T:SMlJxSDX3bqjhcHk7MzH6z                                                                                                                                                                                                                                                         |
| File Content Preview: | MZ.....@.....[r.....[<br>!n;.....!d;.....!8!.....!Br!j;.....!N:.....!hLL>.....!(d. ....!x.^!.....!-d. ....!g. ....<br>!P^ .....!BN!.....!;.....!;.....!Ylv;.....!M;.....!Rich;.....<br>.....PE.                                                                                                                                     |

File Icon

|                                                                                     |                  |
|-------------------------------------------------------------------------------------|------------------|
|  |                  |
| Icon Hash:                                                                          | 54b26869f8c8cc00 |

## Static PE Info

|                             |                                                                 |
|-----------------------------|-----------------------------------------------------------------|
| <b>General</b>              |                                                                 |
| Entrypoint:                 | 0x140078760                                                     |
| Entrypoint Section:         | .text                                                           |
| Digitally signed:           | false                                                           |
| Imagebase:                  | 0x140000000                                                     |
| Subsystem:                  | windows gui                                                     |
| Image File Characteristics: | EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE                      |
| DLL Characteristics:        | TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA |
| Time Stamp:                 | 0x60ADEC84 [Wed May 26 06:36:52 2021 UTC]                       |
| TLS Callbacks:              |                                                                 |
| CLR (.Net) Version:         |                                                                 |
| OS Version Major:           | 5                                                               |
| OS Version Minor:           | 1                                                               |
| File Version Major:         | 5                                                               |
| File Version Minor:         | 1                                                               |
| Subsystem Version Major:    | 5                                                               |
| Subsystem Version Minor:    | 1                                                               |
| Import Hash:                | c6b4c2eec8a93016c63563421e15f011                                |

## Entrypoint Preview

## Data Directories

## Sections

| Name   | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity  | File Type | Entropy        | Characteristics                                                               |
|--------|-----------------|--------------|----------|----------|------------------|-----------|----------------|-------------------------------------------------------------------------------|
| .text  | 0x1000          | 0x7bb10      | 0x7c000  | False    | 0.803878291961   | data      | 7.84727441246  | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ                 |
| .rdata | 0x7d000         | 0xc210       | 0xd000   | False    | 0.772648737981   | data      | 7.6188975428   | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                            |
| .data  | 0x8a000         | 0xd218       | 0xe000   | False    | 0.125104631696   | data      | 1.89187623617  | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ       |
| .pdata | 0x98000         | 0x138        | 0x1000   | False    | 0.060791015625   | data      | 0.590508203574 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                            |
| .rsrc  | 0x99000         | 0x2f98       | 0x3000   | False    | 0.302408854167   | data      | 3.73793039709  | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                            |
| .reloc | 0x9c000         | 0x244        | 0x1000   | False    | 0.076171875      | data      | 1.23641369386  | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |
|        | 0x9d000         | 0x6cd0       | 0x7000   | False    | 0.00177873883929 | data      | 0.0            | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                            |
|        | 0xa4000         | 0x1f2a       | 0x2000   | False    | 0.0037841796875  | data      | 0.0            | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                            |
|        | 0xa6000         | 0x13e        | 0x1000   | False    | 0.00634765625    | data      | 0.0            | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                            |
|        | 0xa7000         | 0x6cd0       | 0x7000   | False    | 0.00177873883929 | data      | 0.0            | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                            |
|        | 0xae000         | 0x7fd        | 0x1000   | False    | 0.00634765625    | data      | 0.0            | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                            |
|        | 0xaf000         | 0x13e        | 0x1000   | False    | 0.00634765625    | data      | 0.0            | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                            |
|        | 0xb0000         | 0x1f7        | 0x1000   | False    | 0.00634765625    | data      | 0.0            | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                            |
|        | 0xb1000         | 0x23b        | 0x1000   | False    | 0.00634765625    | data      | 0.0            | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                            |
|        | 0xb2000         | 0x1278       | 0x2000   | False    | 0.0037841796875  | data      | 0.0            | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                            |
|        | 0xb4000         | 0x13e        | 0x1000   | False    | 0.00634765625    | data      | 0.0            | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                            |
|        | 0xb5000         | 0x9cd        | 0x1000   | False    | 0.00634765625    | data      | 0.0            | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                            |
|        | 0xb6000         | 0x1124       | 0x2000   | False    | 0.0037841796875  | data      | 0.0            | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                            |
|        | 0xb8000         | 0x23b        | 0x1000   | False    | 0.00634765625    | data      | 0.0            | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                            |
|        | 0xb9000         | 0x896        | 0x1000   | False    | 0.00634765625    | data      | 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                                    |
|------|-----------------|--------------|----------|----------|------------------|-----------|--------------|----------------------------------------------------|
|      | 0xba000         | 0x6cd0       | 0x7000   | False    | 0.00177873883929 | data      | 0.0          | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
|      | 0xc1000         | 0x13e        | 0x1000   | False    | 0.00634765625    | data      | 0.0          | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
|      | 0xc2000         | 0x1af        | 0x1000   | False    | 0.00634765625    | data      | 0.0          | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
|      | 0xc3000         | 0x45174      | 0x46000  | False    | 0.0010498046875  | data      | 0.0          | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
|      | 0x109000        | 0x197d       | 0x2000   | False    | 0.0037841796875  | data      | 0.0          | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
|      | 0x10b000        | 0x197d       | 0x2000   | False    | 0.0037841796875  | data      | 0.0          | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
|      | 0x10d000        | 0x1ee        | 0x1000   | False    | 0.00634765625    | data      | 0.0          | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
|      | 0x10e000        | 0x36d        | 0x1000   | False    | 0.1259765625     | data      | 1.6701021982 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

Resources

Imports

Exports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

 Click to jump to process

## System Behavior

Analysis Process: loadll64.exe PID: 396 Parent PID: 6692

### General

|                               |                                                     |
|-------------------------------|-----------------------------------------------------|
| Start time:                   | 13:18:48                                            |
| Start date:                   | 28/09/2021                                          |
| Path:                         | C:\Windows\System32\loadll64.exe                    |
| Wow64 process (32bit):        | false                                               |
| Commandline:                  | loadll64.exe 'C:\Users\user\Desktop\0G0AO3HYEI.dll' |
| Imagebase:                    | 0x7ff770a50000                                      |
| File size:                    | 140288 bytes                                        |
| MD5 hash:                     | A84133CCB118CF35D49A423CD836D0EF                    |
| Has elevated privileges:      | true                                                |
| Has administrator privileges: | true                                                |
| Programmed in:                | C, C++ or other language                            |
| Reputation:                   | high                                                |

### File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5468 Parent PID: 396

### General

|                               |                                                                   |
|-------------------------------|-------------------------------------------------------------------|
| Start time:                   | 13:18:49                                                          |
| Start date:                   | 28/09/2021                                                        |
| Path:                         | C:\Windows\System32\cmd.exe                                       |
| Wow64 process (32bit):        | false                                                             |
| Commandline:                  | cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\0G0AO3HYEI.dll',#1 |
| Imagebase:                    | 0x7ff7180e0000                                                    |
| File size:                    | 273920 bytes                                                      |
| MD5 hash:                     | 4E2ACF4F8A396486AB4268C94A6A245F                                  |
| Has elevated privileges:      | true                                                              |
| Has administrator privileges: | true                                                              |
| Programmed in:                | C, C++ or other language                                          |
| Reputation:                   | high                                                              |

### File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 5612 Parent PID: 396

### General

|                               |                                                                                            |
|-------------------------------|--------------------------------------------------------------------------------------------|
| Start time:                   | 13:18:49                                                                                   |
| Start date:                   | 28/09/2021                                                                                 |
| Path:                         | C:\Windows\System32\rundll32.exe                                                           |
| Wow64 process (32bit):        | false                                                                                      |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,CheckDriverSoftwareDependenciesSatisfied |
| Imagebase:                    | 0x7ff773d70000                                                                             |
| File size:                    | 69632 bytes                                                                                |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                                           |
| 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: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000003.00000002.748525341.0000000140001000.00000020.00020000.sdmp, Author: Joe Security</li> </ul> |
| Reputation:   | high                                                                                                                                                                                                                             |

#### File Activities

Show Windows behavior

#### File Read

### Analysis Process: rundll32.exe PID: 4716 Parent PID: 5468

#### General

|                               |                                                        |
|-------------------------------|--------------------------------------------------------|
| Start time:                   | 13:18:49                                               |
| Start date:                   | 28/09/2021                                             |
| Path:                         | C:\Windows\System32\rundll32.exe                       |
| Wow64 process (32bit):        | false                                                  |
| Commandline:                  | rundll32.exe 'C:\Users\user\Desktop\0G0AO3HYEI.dll',#1 |
| Imagebase:                    | 0x7ff773d70000                                         |
| File size:                    | 69632 bytes                                            |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                       |
| Has elevated privileges:      | true                                                   |
| Has administrator privileges: | true                                                   |
| Programmed in:                | C, C++ or other language                               |
| Reputation:                   | high                                                   |

#### File Activities

Show Windows behavior

#### File Read

### Analysis Process: explorer.exe PID: 3440 Parent PID: 5612

#### General

|                               |                                  |
|-------------------------------|----------------------------------|
| Start time:                   | 13:18:50                         |
| Start date:                   | 28/09/2021                       |
| Path:                         | C:\Windows\explorer.exe          |
| Wow64 process (32bit):        | false                            |
| Commandline:                  | C:\Windows\Explorer.EXE          |
| Imagebase:                    | 0x7ff6f22f0000                   |
| File size:                    | 3933184 bytes                    |
| MD5 hash:                     | AD5296B280E8F522A8A897C96BAB0E1D |
| Has elevated privileges:      | true                             |
| Has administrator privileges: | true                             |
| Programmed in:                | C, C++ or other language         |
| Reputation:                   | high                             |

### Analysis Process: rundll32.exe PID: 7056 Parent PID: 396

#### General

|                        |                                                                             |
|------------------------|-----------------------------------------------------------------------------|
| Start time:            | 13:18:52                                                                    |
| Start date:            | 28/09/2021                                                                  |
| Path:                  | C:\Windows\System32\rundll32.exe                                            |
| Wow64 process (32bit): | false                                                                       |
| Commandline:           | rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll, DeviceInternetSettingUIW |
| Imagebase:             | 0x7ff773d70000                                                              |

|                               |                                                                                                                                                                                                                                  |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File size:                    | 69632 bytes                                                                                                                                                                                                                      |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                                                                                                                                                                                 |
| 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: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000007.00000002.748435609.0000000140001000.00000020.00020000.sdmp, Author: Joe Security</li> </ul> |
| Reputation:                   | high                                                                                                                                                                                                                             |

#### File Activities

Show Windows behavior

#### File Read

### Analysis Process: rundll32.exe PID: 5184 Parent PID: 396

#### General

|                               |                                                                                                                                                                                                                                  |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start time:                   | 13:18:56                                                                                                                                                                                                                         |
| Start date:                   | 28/09/2021                                                                                                                                                                                                                       |
| Path:                         | C:\Windows\System32\rundll32.exe                                                                                                                                                                                                 |
| Wow64 process (32bit):        | false                                                                                                                                                                                                                            |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiInstallDevice                                                                                                                                                                |
| Imagebase:                    | 0x7ff773d70000                                                                                                                                                                                                                   |
| File size:                    | 69632 bytes                                                                                                                                                                                                                      |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                                                                                                                                                                                 |
| 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: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000008.00000002.748754528.0000000140001000.00000020.00020000.sdmp, Author: Joe Security</li> </ul> |
| Reputation:                   | high                                                                                                                                                                                                                             |

#### File Activities

Show Windows behavior

#### File Read

### Analysis Process: rundll32.exe PID: 1360 Parent PID: 396

#### General

|                               |                                                                    |
|-------------------------------|--------------------------------------------------------------------|
| Start time:                   | 13:18:59                                                           |
| Start date:                   | 28/09/2021                                                         |
| Path:                         | C:\Windows\System32\rundll32.exe                                   |
| Wow64 process (32bit):        | false                                                              |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiInstallDriverA |
| Imagebase:                    | 0x7ff773d70000                                                     |
| File size:                    | 69632 bytes                                                        |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                   |
| Has elevated privileges:      | true                                                               |
| Has administrator privileges: | true                                                               |
| Programmed in:                | C, C++ or other language                                           |

#### File Activities

Show Windows behavior

#### File Read

**Analysis Process: explorer.exe PID: 7080 Parent PID: 568****General**

|                               |                                  |
|-------------------------------|----------------------------------|
| Start time:                   | 13:19:01                         |
| Start date:                   | 28/09/2021                       |
| Path:                         | C:\Windows\explorer.exe          |
| Wow64 process (32bit):        | false                            |
| Commandline:                  | explorer.exe                     |
| Imagebase:                    | 0x7ff6f22f0000                   |
| File size:                    | 3933184 bytes                    |
| MD5 hash:                     | AD5296B280E8F522A8A897C96BAB0E1D |
| Has elevated privileges:      | true                             |
| Has administrator privileges: | true                             |
| Programmed in:                | C, C++ or other language         |

**File Activities**

Show Windows behavior

**Registry Activities**

Show Windows behavior

**Analysis Process: rundll32.exe PID: 1520 Parent PID: 396****General**

|                               |                                                                                                                                                                                                                                |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start time:                   | 13:19:03                                                                                                                                                                                                                       |
| Start date:                   | 28/09/2021                                                                                                                                                                                                                     |
| Path:                         | C:\Windows\System32\rundll32.exe                                                                                                                                                                                               |
| Wow64 process (32bit):        | false                                                                                                                                                                                                                          |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiInstallDriverW                                                                                                                                                             |
| Imagebase:                    | 0x7ff773d70000                                                                                                                                                                                                                 |
| File size:                    | 69632 bytes                                                                                                                                                                                                                    |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                                                                                                                                                                               |
| 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: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000000B.00000002.749145318.0000000140001000.00000020.00020000.sdmp, Author: Joe Security</li></ul> |

**Analysis Process: rundll32.exe PID: 3912 Parent PID: 396****General**

|                               |                                                                                                                                                                                                                                |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start time:                   | 13:19:06                                                                                                                                                                                                                       |
| Start date:                   | 28/09/2021                                                                                                                                                                                                                     |
| Path:                         | C:\Windows\System32\rundll32.exe                                                                                                                                                                                               |
| Wow64 process (32bit):        | false                                                                                                                                                                                                                          |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiRollbackDriver                                                                                                                                                             |
| Imagebase:                    | 0x7ff773d70000                                                                                                                                                                                                                 |
| File size:                    | 69632 bytes                                                                                                                                                                                                                    |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                                                                                                                                                                               |
| 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: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000000C.00000002.749353008.0000000140001000.00000020.00020000.sdmp, Author: Joe Security</li></ul> |

**Analysis Process: rundll32.exe PID: 5624 Parent PID: 396****General**

|                               |                                                                                                                                                                                                                                |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start time:                   | 13:19:10                                                                                                                                                                                                                       |
| Start date:                   | 28/09/2021                                                                                                                                                                                                                     |
| Path:                         | C:\Windows\System32\rundll32.exe                                                                                                                                                                                               |
| Wow64 process (32bit):        | false                                                                                                                                                                                                                          |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiShowUpdateDevice                                                                                                                                                           |
| Imagebase:                    | 0x7ff773d70000                                                                                                                                                                                                                 |
| File size:                    | 69632 bytes                                                                                                                                                                                                                    |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                                                                                                                                                                               |
| 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: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000000E.00000002.748916641.0000000140001000.00000020.00020000.sdmp, Author: Joe Security</li></ul> |

**Analysis Process: rundll32.exe PID: 6764 Parent PID: 396****General**

|                               |                                                                      |
|-------------------------------|----------------------------------------------------------------------|
| Start time:                   | 13:19:13                                                             |
| Start date:                   | 28/09/2021                                                           |
| Path:                         | C:\Windows\System32\rundll32.exe                                     |
| Wow64 process (32bit):        | false                                                                |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiShowUpdateDriver |
| Imagebase:                    | 0x7ff773d70000                                                       |
| File size:                    | 69632 bytes                                                          |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                     |
| Has elevated privileges:      | true                                                                 |
| Has administrator privileges: | true                                                                 |
| Programmed in:                | C, C++ or other language                                             |

**Analysis Process: rundll32.exe PID: 2892 Parent PID: 396****General**

|                               |                                                                     |
|-------------------------------|---------------------------------------------------------------------|
| Start time:                   | 13:19:17                                                            |
| Start date:                   | 28/09/2021                                                          |
| Path:                         | C:\Windows\System32\rundll32.exe                                    |
| Wow64 process (32bit):        | false                                                               |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiUninstallDevice |
| Imagebase:                    | 0x7ff773d70000                                                      |
| File size:                    | 69632 bytes                                                         |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                    |
| Has elevated privileges:      | true                                                                |
| Has administrator privileges: | true                                                                |
| Programmed in:                | C, C++ or other language                                            |

**Analysis Process: rundll32.exe PID: 3444 Parent PID: 396****General**

|             |                                  |
|-------------|----------------------------------|
| Start time: | 13:19:21                         |
| Start date: | 28/09/2021                       |
| Path:       | C:\Windows\System32\rundll32.exe |

|                               |                                                                      |
|-------------------------------|----------------------------------------------------------------------|
| Wow64 process (32bit):        | false                                                                |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiUninstallDriverA |
| Imagebase:                    | 0x7ff773d70000                                                       |
| File size:                    | 69632 bytes                                                          |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                     |
| Has elevated privileges:      | true                                                                 |
| Has administrator privileges: | true                                                                 |
| Programmed in:                | C, C++ or other language                                             |

#### Analysis Process: explorer.exe PID: 3208 Parent PID: 568

##### General

|                               |                                  |
|-------------------------------|----------------------------------|
| Start time:                   | 13:19:24                         |
| Start date:                   | 28/09/2021                       |
| Path:                         | C:\Windows\explorer.exe          |
| Wow64 process (32bit):        | false                            |
| Commandline:                  | explorer.exe                     |
| Imagebase:                    | 0x7ff6f22f0000                   |
| File size:                    | 3933184 bytes                    |
| MD5 hash:                     | AD5296B280E8F522A8A897C96BAB0E1D |
| Has elevated privileges:      | true                             |
| Has administrator privileges: | true                             |
| Programmed in:                | C, C++ or other language         |

#### Analysis Process: rundll32.exe PID: 784 Parent PID: 396

##### General

|                               |                                                                      |
|-------------------------------|----------------------------------------------------------------------|
| Start time:                   | 13:19:26                                                             |
| Start date:                   | 28/09/2021                                                           |
| Path:                         | C:\Windows\System32\rundll32.exe                                     |
| Wow64 process (32bit):        | false                                                                |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiUninstallDriverW |
| Imagebase:                    | 0x7ff773d70000                                                       |
| File size:                    | 69632 bytes                                                          |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                     |
| Has elevated privileges:      | true                                                                 |
| Has administrator privileges: | true                                                                 |
| Programmed in:                | C, C++ or other language                                             |

#### Analysis Process: rundll32.exe PID: 3692 Parent PID: 396

##### General

|                               |                                                                                                                                                                                                                                  |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start time:                   | 13:19:30                                                                                                                                                                                                                         |
| Start date:                   | 28/09/2021                                                                                                                                                                                                                       |
| Path:                         | C:\Windows\System32\rundll32.exe                                                                                                                                                                                                 |
| Wow64 process (32bit):        | false                                                                                                                                                                                                                            |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,GetInternetPolicies                                                                                                                                                            |
| Imagebase:                    | 0x7ff773d70000                                                                                                                                                                                                                   |
| File size:                    | 69632 bytes                                                                                                                                                                                                                      |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                                                                                                                                                                                 |
| 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: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001B.00000002.749674160.0000000140001000.00000020.00020000.sdmp, Author: Joe Security</li> </ul> |

**Analysis Process: rundll32.exe PID: 348 Parent PID: 396****General**

|                               |                                                                                                                                                                                                                                |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start time:                   | 13:19:34                                                                                                                                                                                                                       |
| Start date:                   | 28/09/2021                                                                                                                                                                                                                     |
| Path:                         | C:\Windows\System32\rundll32.exe                                                                                                                                                                                               |
| Wow64 process (32bit):        | false                                                                                                                                                                                                                          |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,InstallNewDevice                                                                                                                                                             |
| Imagebase:                    | 0x7ff773d70000                                                                                                                                                                                                                 |
| File size:                    | 69632 bytes                                                                                                                                                                                                                    |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                                                                                                                                                                               |
| 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: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001D.00000002.749906681.0000000140001000.00000020.00020000.sdmp, Author: Joe Security</li></ul> |

**Analysis Process: rundll32.exe PID: 6296 Parent PID: 396****General**

|                               |                                                                         |
|-------------------------------|-------------------------------------------------------------------------|
| Start time:                   | 13:19:37                                                                |
| Start date:                   | 28/09/2021                                                              |
| Path:                         | C:\Windows\System32\rundll32.exe                                        |
| Wow64 process (32bit):        | false                                                                   |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,InstallSelectedDriver |
| Imagebase:                    | 0x7ff773d70000                                                          |
| File size:                    | 69632 bytes                                                             |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                        |
| Has elevated privileges:      | true                                                                    |
| Has administrator privileges: | true                                                                    |
| Programmed in:                | C, C++ or other language                                                |

**Analysis Process: rundll32.exe PID: 3440 Parent PID: 396****General**

|                               |                                                                              |
|-------------------------------|------------------------------------------------------------------------------|
| Start time:                   | 13:19:41                                                                     |
| Start date:                   | 28/09/2021                                                                   |
| Path:                         | C:\Windows\System32\rundll32.exe                                             |
| Wow64 process (32bit):        | false                                                                        |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,InstallWindowsUpdateDriver |
| Imagebase:                    | 0x7ff773d70000                                                               |
| File size:                    | 69632 bytes                                                                  |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                             |
| Has elevated privileges:      | true                                                                         |
| Has administrator privileges: | true                                                                         |
| Programmed in:                | C, C++ or other language                                                     |

**Analysis Process: rundll32.exe PID: 2384 Parent PID: 396**

|                               |                                                                                |
|-------------------------------|--------------------------------------------------------------------------------|
| <b>General</b>                |                                                                                |
| Start time:                   | 13:19:45                                                                       |
| Start date:                   | 28/09/2021                                                                     |
| Path:                         | C:\Windows\System32\rundll32.exe                                               |
| Wow64 process (32bit):        | false                                                                          |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,InstallWindowsUpdateDriverEx |
| Imagebase:                    | 0x7ff773d70000                                                                 |
| File size:                    | 69632 bytes                                                                    |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                               |
| Has elevated privileges:      | true                                                                           |
| Has administrator privileges: | true                                                                           |
| Programmed in:                | C, C++ or other language                                                       |

### Analysis Process: rundll32.exe PID: 2152 Parent PID: 396

|                               |                                                                                                                                                                                                                                  |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>General</b>                |                                                                                                                                                                                                                                  |
| Start time:                   | 13:19:48                                                                                                                                                                                                                         |
| Start date:                   | 28/09/2021                                                                                                                                                                                                                       |
| Path:                         | C:\Windows\System32\rundll32.exe                                                                                                                                                                                                 |
| Wow64 process (32bit):        | false                                                                                                                                                                                                                            |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,InstallWindowsUpdateDrivers                                                                                                                                                    |
| Imagebase:                    | 0x7ff773d70000                                                                                                                                                                                                                   |
| File size:                    | 69632 bytes                                                                                                                                                                                                                      |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                                                                                                                                                                                 |
| 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: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000024.00000002.750032138.0000000140001000.00000020.00020000.sdmp, Author: Joe Security</li> </ul> |

### Analysis Process: explorer.exe PID: 5252 Parent PID: 568

|                               |                                  |
|-------------------------------|----------------------------------|
| <b>General</b>                |                                  |
| Start time:                   | 13:19:51                         |
| Start date:                   | 28/09/2021                       |
| Path:                         | C:\Windows\explorer.exe          |
| Wow64 process (32bit):        | false                            |
| Commandline:                  | explorer.exe                     |
| Imagebase:                    | 0x7ff6f22f0000                   |
| File size:                    | 3933184 bytes                    |
| MD5 hash:                     | AD5296B280E8F522A8A897C96BAB0E1D |
| Has elevated privileges:      | true                             |
| Has administrator privileges: | true                             |
| Programmed in:                | C, C++ or other language         |

### Analysis Process: rundll32.exe PID: 1148 Parent PID: 396

|                        |                                                                                  |
|------------------------|----------------------------------------------------------------------------------|
| <b>General</b>         |                                                                                  |
| Start time:            | 13:19:52                                                                         |
| Start date:            | 28/09/2021                                                                       |
| Path:                  | C:\Windows\System32\rundll32.exe                                                 |
| Wow64 process (32bit): | false                                                                            |
| Commandline:           | rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,QueryWindowsUpdateDriverStatus |
| Imagebase:             | 0x7ff773d70000                                                                   |

|                               |                                  |
|-------------------------------|----------------------------------|
| File size:                    | 69632 bytes                      |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A |
| Has elevated privileges:      | true                             |
| Has administrator privileges: | true                             |
| Programmed in:                | C, C++ or other language         |

### Analysis Process: rundll32.exe PID: 4224 Parent PID: 396

#### General

|                               |                                                                                                                                                                                                                                  |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start time:                   | 13:19:56                                                                                                                                                                                                                         |
| Start date:                   | 28/09/2021                                                                                                                                                                                                                       |
| Path:                         | C:\Windows\System32\rundll32.exe                                                                                                                                                                                                 |
| Wow64 process (32bit):        | false                                                                                                                                                                                                                            |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll, SetInternetPolicies                                                                                                                                                           |
| Imagebase:                    | 0x7ff773d70000                                                                                                                                                                                                                   |
| File size:                    | 69632 bytes                                                                                                                                                                                                                      |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                                                                                                                                                                                 |
| 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: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000028.00000002.750108429.0000000140001000.00000020.00020000.sdmp, Author: Joe Security</li> </ul> |

### Analysis Process: rundll32.exe PID: 1432 Parent PID: 396

#### General

|                               |                                                                                                                                                                                                                                  |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start time:                   | 13:19:59                                                                                                                                                                                                                         |
| Start date:                   | 28/09/2021                                                                                                                                                                                                                       |
| Path:                         | C:\Windows\System32\rundll32.exe                                                                                                                                                                                                 |
| Wow64 process (32bit):        | false                                                                                                                                                                                                                            |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll, UpdateDriverForPlugAndPlayDevicesA                                                                                                                                            |
| Imagebase:                    | 0x7ff773d70000                                                                                                                                                                                                                   |
| File size:                    | 69632 bytes                                                                                                                                                                                                                      |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                                                                                                                                                                                 |
| 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: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000029.00000002.750110395.0000000140001000.00000020.00020000.sdmp, Author: Joe Security</li> </ul> |

## Disassembly

## Code Analysis