ID: 492188
Sample Name: 0G0AO3HYEI
Cookbook: default.jbs
Time: 13:03:29
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

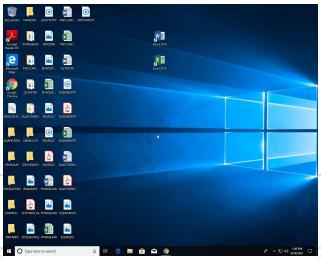
Windows Analysis Report 0G0AO3HYEI

Overview

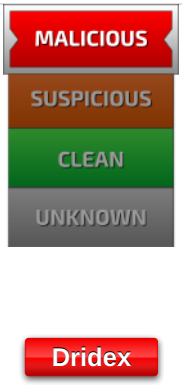
General Information

Sample Name:	0G0AO3HYEI (renamed file extension from none to dll)
Analysis ID:	492188
MD5:	c50f692a715db80.
SHA1:	229b257301ed99..
SHA256:	ff3aa75e4d46375..
Tags:	Dridex exe
Infos:	

Most interesting Screenshot:



Detection

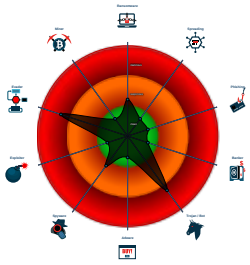


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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**
- loaddll64.exe (PID: 6488 cmdline: loaddll64.exe 'C:\Users\user\Desktop\0G0AO3HYEI.dll' MD5: A84133CCB118CF35D49A423CD836D0EF)
  - cmd.exe (PID: 6512 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\0G0AO3HYEI.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6532 cmdline: rundll32.exe 'C:\Users\user\Desktop\0G0AO3HYEI.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - explorer.exe (PID: 3292 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - rundll32.exe (PID: 6520 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,CheckDriverSoftwareDependenciesSatisfied MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6864 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DeviceInternetSettingUiW MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6924 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiInstallDevice MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6940 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiInstallDriverA MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 7116 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiInstallDriverW MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 4604 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiRollbackDriver MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5392 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiShowUpdateDevice MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6508 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiShowUpdateDriver MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6656 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiUninstallDevice MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5636 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiUninstallDriverA MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 4516 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiUninstallDriverW MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 3324 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,GetInternetPolicies MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 3604 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,InstallNewDevice MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 4912 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,InstallSelectedDriver MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 3864 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,InstallWindowsUpdateDriver MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 1392 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,InstallWindowsUpdateDriverEx MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6568 cmdline: rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,InstallWindowsUpdateDrivers MD5: 73C519F050C20580F8A62C849D49215A)
- explorer.exe (PID: 7024 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 4932 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 4628 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.531717710.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000025.00000002.532357019.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000015.00000002.531718093.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000009.00000002.531527593.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000014.00000002.531894805.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
Click to see the 14 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

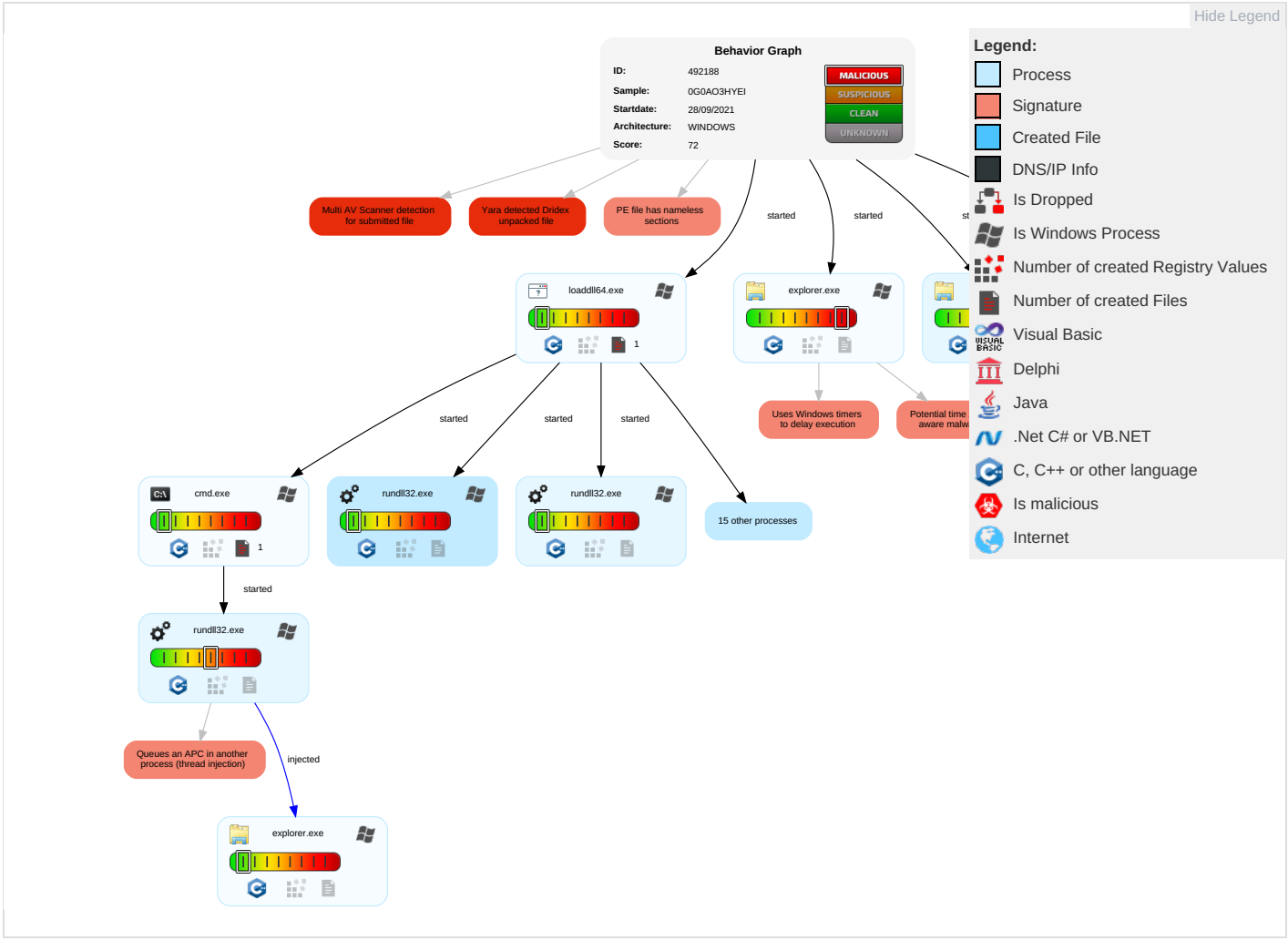
HIPS / PFW / Operating System Protection Evasion:

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 Contro
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 1	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	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganogra
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Virtualization/Sandbox Evasion 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonati
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 Communica
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 Proto
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 Protoc
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 Transfe Protocols

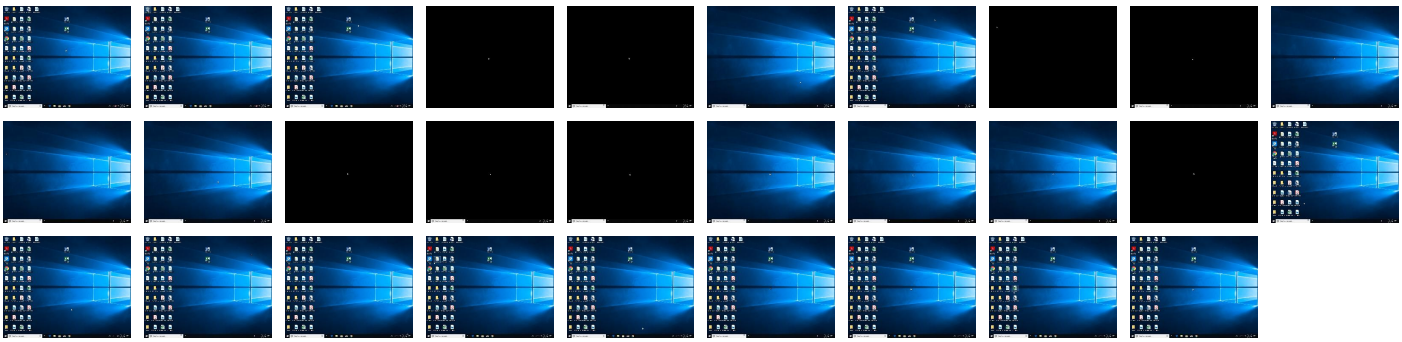
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
0G0AO3HYEI.dll	59%	Virustotal		Browse
0G0AO3HYEI.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:	13:03:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0G0AO3HYEI (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.troj.evad.winDLL@45/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 17.7% (good quality ratio 15.7%) • Quality average: 82.8% • Quality standard deviation: 33.1%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:04:51	API Interceptor	118x 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:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	0G0AO3HYEI.dll
File size:	1110016
MD5:	c50f692a715db805e68e9655ff6a9ab2
SHA1:	229b257301ed99d518364afd22c4276daa5b3d20
SHA256:	ff3aa75e4d4637599d3e97fb8b42ce8a1254425f856671ae56377df2676b1033
SHA512:	ad74f556ccef1f8fd4a3c18a18c27adcafd2f552025bf7f83864261c6944db5423c719ea161c341e593800499c6e01aba846031e79caf1e771b2b16e7d6e33d1
SSDEEP:	12288:4dMIwS97wJs6tSKDXEabXaC+jhc1S8XXk7CZzHsZH9dq0T:SMIJxSDX3bqjhcfHk7MzH6z
File Content Preview:	MZ.....@.....[.r.:.!.:.!.:.!..[!n;.!.:.!d:.!..8!..:.!.Br!j:.!...!N:.!.hL!>:.!(d. |;.!x.^!.:.!-d. .;.!.g. .;.!P^. .:.!.BN!.:.!.._!.:.!.._!.:.!..Y!v;.!!._!M;.!Rich.:.!.....PE.

File Icon

Icon Hash:	54b26869f8c8cc00

Static PE Info

General

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
	0xba000	0x6cd0	0x7000	False	0.00177873883929	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
	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: loaddll64.exe PID: 6488 Parent PID: 4744

General

Start time:	13:04:28
Start date:	28/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\0G0AO3HYEI.dll'
Imagebase:	0x7ff65ceb0000
File size:	140288 bytes
MD5 hash:	A84133CCB118CF35D49A423CD836D0EF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000001.00000002.531295536.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6512 Parent PID: 6488

General

Start time:	13:04:29
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:	0x7ff7bf140000
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: 6520 Parent PID: 6488

General

Start time:	13:04:30
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,CheckDriverSoftwareDependencieSatisfied
Imagebase:	0x7ff687d70000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000003.00000002.531206986.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6532 Parent PID: 6512

General

Start time:	13:04:30
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\0G0AO3HYEI.dll',#1
Imagebase:	0x7ff687d70000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000004.00000002.531244676.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3292 Parent PID: 6532

General

Start time:	13:04:31
Start date:	28/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff662bf0000
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: 6864 Parent PID: 6488

General

Start time:	13:04:33
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:	0x7ff687d70000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000008.00000002.531418646.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6924 Parent PID: 6488

General

Start time:	13:04:37
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiInstallDevice
Imagebase:	0x7ff687d70000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000009.00000002.531527593.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6940 Parent PID: 6488

General

Start time:	13:04:40
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:	0x7ff687d70000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000000A.00000002.531585014.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 7024 Parent PID: 568

General

Start time:	13:04:42
Start date:	28/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	explorer.exe
Imagebase:	0x7ff662bf0000
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: 7116 Parent PID: 6488

General

Start time:	13:04:44
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:	0x7ff687d70000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000000E.00000002.531716160.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 4604 Parent PID: 6488

General

Start time:	13:04:48
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiRollbackDriver
Imagebase:	0x7ff687d70000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000011.00000002.531717710.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 5392 Parent PID: 6488

General

Start time:	13:04:51
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:	0x7ff687d70000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000014.00000002.531894805.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6508 Parent PID: 6488

General

Start time:	13:04:55
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:	0x7ff687d70000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000015.00000002.531718093.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6656 Parent PID: 6488

General

Start time:	13:04:58
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:	0x7ff687d70000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000018.00000002.531937010.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 5636 Parent PID: 6488

General

Start time:	13:05:02
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:	0x7ff687d70000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001A.00000002.531718874.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: explorer.exe PID: 4932 Parent PID: 568

General

Start time:	13:05:05
Start date:	28/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	explorer.exe
Imagebase:	0x7ff662bf0000
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: 4516 Parent PID: 6488

General

Start time:	13:05:06
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,DiUninstallDriverW
Imagebase:	0x7ff687d70000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001C.00000002.532059437.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 3324 Parent PID: 6488

General

Start time:	13:05:10
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,GetInternetPolicies
Imagebase:	0x7ff687d70000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001E.00000002.532228237.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 3604 Parent PID: 6488

General

Start time:	13:05:14
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:	0x7ff687d70000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001F.00000002.532276672.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 4912 Parent PID: 6488

General

Start time:	13:05:17
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,InstallSelectedDriver
Imagebase:	0x7ff687d70000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000021.00000002.532290767.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 3864 Parent PID: 6488

General

Start time:	13:05:21
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\0G0AO3HYEI.dll,InstallWindowsUpdateDriver
Imagebase:	0x7ff687d70000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000022.00000002.533238918.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 1392 Parent PID: 6488

General

Start time:	13:05:25
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:	0x7ff687d70000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000025.00000002.532357019.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: explorer.exe PID: 4628 Parent PID: 568

General

Start time:	13:05:26
Start date:	28/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	explorer.exe
Imagebase:	0x7ff772bb0000
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: 6568 Parent PID: 6488

General

Start time:	13:05:29
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:	0x7ff687d70000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000028.00000002.532418928.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Disassembly

Code Analysis