ID: 492636
Sample Name: a4vEYL53cZ
Cookbook: default.jbs
Time: 21:43:41
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

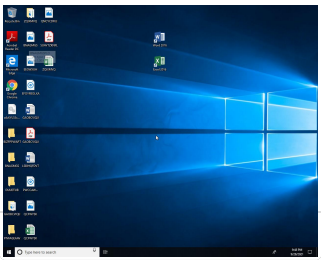
Windows Analysis Report a4vEYL53cZ

Overview

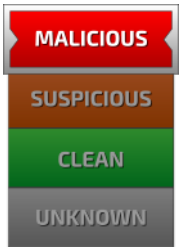
General Information

Sample Name:	a4vEYL53cZ (renamed file extension from none to dll)
Analysis ID:	492636
MD5:	d49772c85d426c..
SHA1:	4eaa4a005cd682..
SHA256:	73541b82ca26c8..
Tags:	Dridex exe
Infos:	

Most interesting Screenshot:



Detection

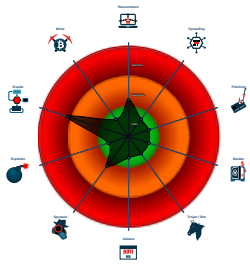


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Queues an APC in another process …
- PE file has nameless sections
- 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
- Contains functionality to call native f…
- PE file contains executable resource…
- Found a high number of Window / Us…
- Sample file is different than original …
- PE file contains an invalid checksum

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 4020 cmdline: loaddll64.exe 'C:\Users\user\Desktop\a4vEYL53cZ.dll' MD5: E0CC9D126C39A9D2FA1CAD5027EBBD18)
  - cmd.exe (PID: 4480 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\a4vEYL53cZ.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 2716 cmdline: rundll32.exe 'C:\Users\user\Desktop\a4vEYL53cZ.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 4552 cmdline: rundll32.exe C:\Users\user\Desktop\a4vEYL53cZ.dll,??0?$PatternProvider@VExpandCollapseProvider@DirectUI@@UIExpandCollapseProvider@@$00@DirectUI@@QEAA@XZ MD5: 73C519F050C20580F8A62C849D49215A)
    - explorer.exe (PID: 3292 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - rundll32.exe (PID: 852 cmdline: rundll32.exe C:\Users\user\Desktop\a4vEYL53cZ.dll,??0?$PatternProvider@VGridItemProvider@DirectUI@@UIGridItemProvider@@$01@DirectUI@@QEAA@XZ MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 4676 cmdline: rundll32.exe C:\Users\user\Desktop\a4vEYL53cZ.dll,??0?$PatternProvider@VGridProvider@DirectUI@@UIGridProvider@@$02@DirectUI@@QEAA@XZ MD5: 73C519F050C20580F8A62C849D49215A)
- explorer.exe (PID: 1004 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 6228 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 7160 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 6332 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 6252 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 6032 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

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

System Summary:

PE file has nameless sections

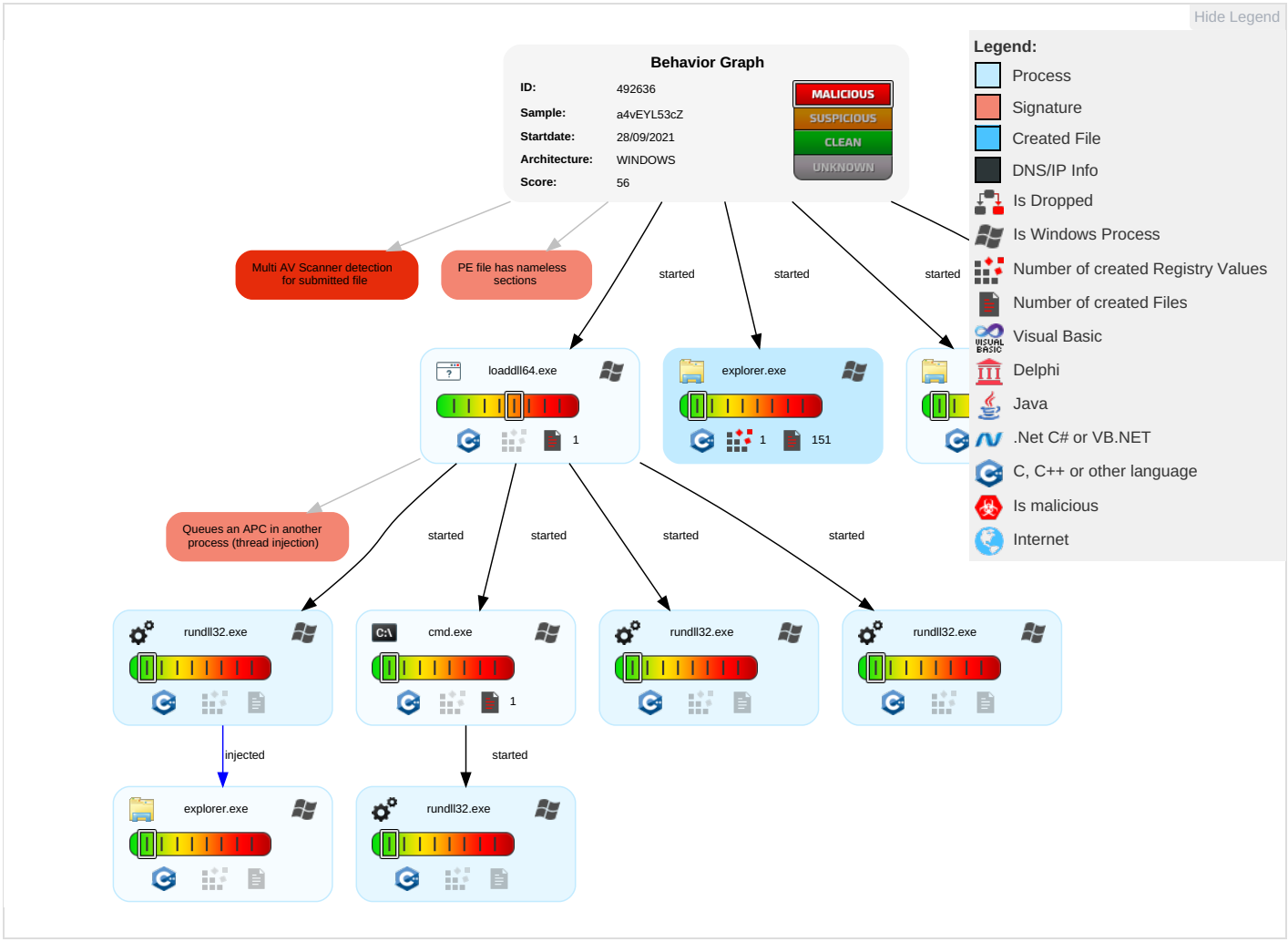
HIPS / PFW / Operating System Protection Evasion:

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	Networ Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdr Insecure Networ Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit S Redirec Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit S Track D Locatior
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Process Discovery 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rundll32 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 2	Cached Domain Credentials	Account Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial c Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	File and Directory Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecure Protoco
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 1 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue C Base St

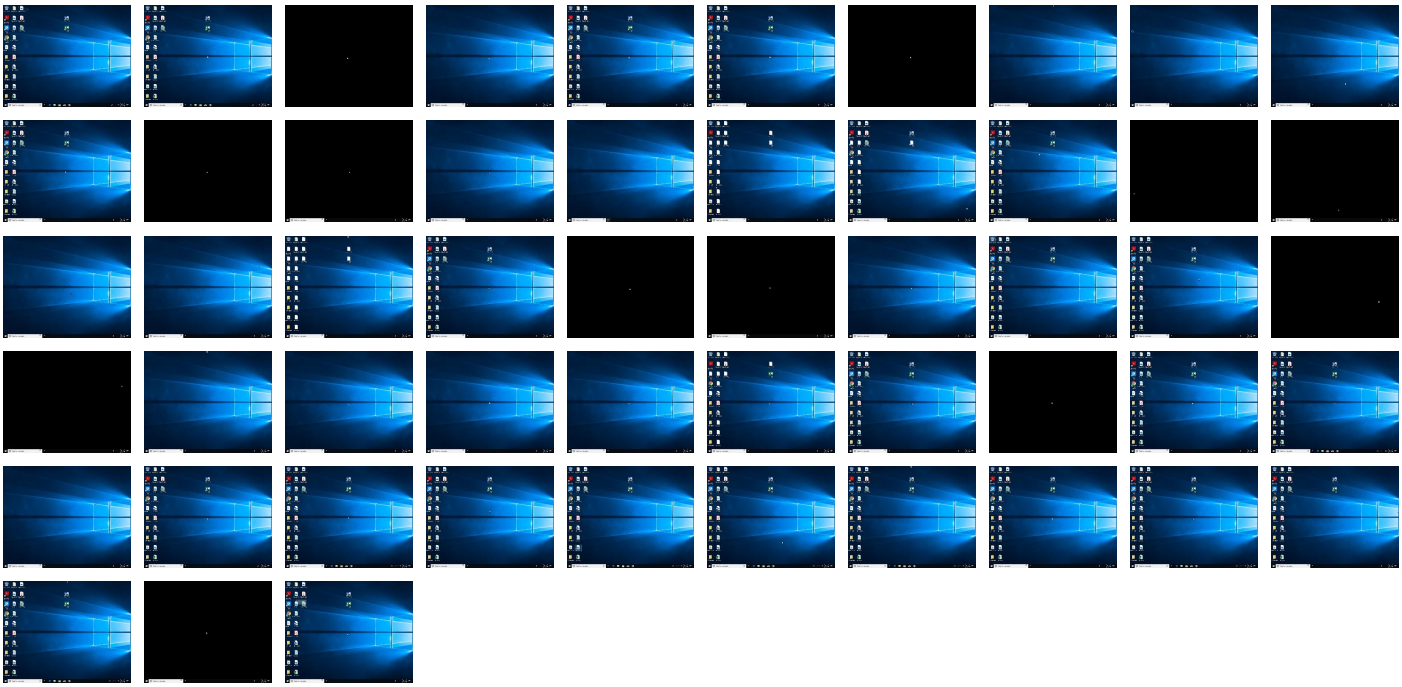
Behavior Graph



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
a4vEYL53cZ.dll	55%	Virustotal		Browse
a4vEYL53cZ.dll	51%	Metadefender		Browse
a4vEYL53cZ.dll	60%	ReversingLabs	Win64.Trojan.Injexa	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ns.adobe.co/1	0%	Avira URL Cloud	safe	
http://purl.or	0%	Avira URL Cloud	safe	

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:	492636
Start date:	28.09.2021
Start time:	21:43:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	a4vEYL53cZ (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:	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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.evad.winDLL@17/1@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 6.3% (good quality ratio 5.7%) • Quality average: 84.1% • Quality standard deviation: 31.2%
HCA Information:	• Successful, ratio: 52% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
21:45:00	API Interceptor	479x 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

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	modified
Size (bytes):	29232
Entropy (8bit):	0.005894213252755928
Encrypted:	false
SSDEEP:	3:tnElC:G
MD5:	4D9C1D76BA4558B9CE42B01E619E3053
SHA1:	1E5BB12B567E443A3A8B2CFCB28800437CCFAFCA
SHA-256:	CBC9A97F9BCF1AE406D191DAA4C393D778A60CFBF0499F066DD70CBD4744F59A
SHA-512:	08025CE1F212CF993732C92F5BBD045F2FE80DFBB200B4C2E8A9543B23C881F5A040D5791C8ABAFE450FEA53EEDCC4F0BD8BF36ABE5A6A1D256B1BA51CB1AACF
Malicious:	false
Preview:	..0 IMMM ....

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	5.608636531535347
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:	a4vEYL53cZ.dll
File size:	1368064

General

MD5:	d49772c85d426ce5fe41cf8c5529a5ff
SHA1:	4eaa4a005cd6825706634cf5fb9b95c4f546778e
SHA256:	73541b82ca26c8c60a84354c657c42bd2ece5cfad3f49437a927b4265234b9da
SHA512:	ac76de00fd7f4cfaaac884990f02ff26883500d4a7c1c37e13a173de04b7228847527bca4737aa32e9498a05f473ac1a27ce98f35dead85fcc95e9c54efc924e
SSDEEP:	12288:NdMIwS97wJs6tSKDXEabXaC+jhc1S8XXk7CZzHsZH9dq0TbEA:jMIJxSDX3bqjhcfHk7MzH6zn
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
	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	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
	0xba000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
	0x100000	0x197d	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
	0x102000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
	0x103000	0xd33	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
	0x104000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
	0x105000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
	0x107000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
	0x108000	0x451c2	0x46000	False	0.220598493304	data	5.77128234001	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: 4020 Parent PID: 5016

General

Start time:	21:44:39
Start date:	28/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\a4vEYL53cZ.dll'
Imagebase:	0x7ff6897c0000
File size:	1136128 bytes
MD5 hash:	E0CC9D126C39A9D2FA1CAD5027EBBD18
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 4480 Parent PID: 4020

General

Start time:	21:44:40
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\a4vEYL53cZ.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: 2716 Parent PID: 4480

General

Start time:	21:44:40
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\a4vEYL53cZ.dll',#1
Imagebase:	0x7ff644a30000
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: rundll32.exe PID: 4552 Parent PID: 4020

General

Start time:	21:44:40
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\a4vEYL53cZ.dll,??0?$PatternProvider@VExpandCollapseProvider@DirectUI@@UIExpandCollapseProvider@@$00@DirectUI@@QEAA@XZ
Imagebase:	0x7ff644a30000
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: 3292 Parent PID: 4552

General

Start time:	21:44:43
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: 852 Parent PID: 4020

General

Start time:	21:44:44
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\a4vEYL53cZ.dll,??0?$PatternProvider@VGridItemProvider@DirectUI@@UIGridItemProvider@@$01@DirectUI@@QEAA@XZ
Imagebase:	0x7ff644a30000
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: rundll32.exe PID: 4676 Parent PID: 4020

General

Start time:	21:44:48
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\a4vEYL53cZ.dll,??0?$PatternProvider@VGridProvider@DirectUI@@UIGridProvider@@$02@DirectUI@@QEAA@XZ
Imagebase:	0x7ff644a30000
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: 1004 Parent PID: 568

General

Start time:	21:44:54
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: explorer.exe PID: 6228 Parent PID: 568

General

Start time:	21:45:20
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: explorer.exe PID: 7160 Parent PID: 568

General

Start time:	21:45:36
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: explorer.exe PID: 6332 Parent PID: 568

General

Start time:	21:45:55
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: explorer.exe PID: 6252 Parent PID: 568

General

Start time:	21:46:14
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: explorer.exe PID: 6032 Parent PID: 568

General

Start time:	21:46:40
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

Disassembly

Code Analysis