

JoeSandbox Cloud BASIC



ID: 532354

Sample Name: Giowcosi64.dll

Cookbook: default.jbs

Time: 04:27:03

Date: 02/12/2021

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report Giowcosi64.dll	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: IcedID	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	5
Jbx Signature Overview	5
AV Detection:	6
Networking:	6
E-Banking Fraud:	6
Stealing of Sensitive Information:	6
Remote Access Functionality:	6
Mitre Att&ck Matrix	6
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
Contacted URLs	9
Contacted IPs	9
General Information	9
Simulations	9
Behavior and APIs	10
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	11
Static PE Info	11
General	11
Entrypoint Preview	11
Data Directories	11
Sections	11
Imports	11
Exports	11
Network Behavior	11
Code Manipulations	11
Statistics	11
Behavior	12
System Behavior	12
Analysis Process: loadll64.exe PID: 5112 Parent PID: 5876	12
General	12
File Activities	12
Analysis Process: cmd.exe PID: 3116 Parent PID: 5112	12
General	12
File Activities	12
Analysis Process: rundll32.exe PID: 1836 Parent PID: 5112	13
General	13
Analysis Process: rundll32.exe PID: 4728 Parent PID: 3116	13
General	13
Analysis Process: rundll32.exe PID: 6528 Parent PID: 5112	13
General	13
Analysis Process: rundll32.exe PID: 6600 Parent PID: 5112	14
General	14
Analysis Process: rundll32.exe PID: 616 Parent PID: 5112	14

General	14
Analysis Process: rundll32.exe PID: 744 Parent PID: 5112	15
General	15
Analysis Process: rundll32.exe PID: 6840 Parent PID: 5112	15
General	15
Disassembly	16
Code Analysis	16

Windows Analysis Report Giowcosi64.dll

Overview

General Information

Sample Name:

Giowcosi64.dll

Analysis ID:

532354

MD5:

8afee9d09b791bf..

SHA1:

fe27de2819b394e.

SHA256:

c340ae2dde2bd8..

Tags:

Bokbot

DLL

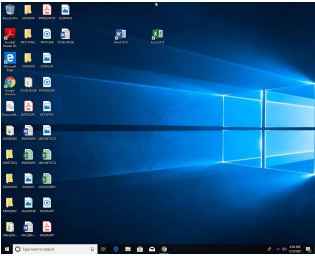
exe

IcedID

Infos:



Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

IcedID

Score:

68

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Found malware configuration

Multi AV Scanner detection for subm...

Yara detected IcedID

C2 URLs / IPs found in malware con...

Yara signature match

Contains functionality to dynamically...

May sleep (evasive loops) to hinder ...

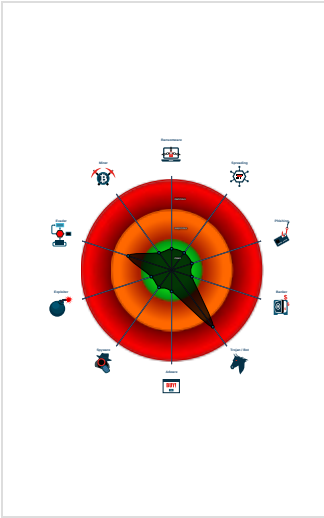
Contains functionality which may be...

Program does not show much activi...

Uses code obfuscation techniques (...)

Creates a process in suspended mo...

Classification



Process Tree

System is w10x64

 loadaddll64.exe (PID: 5112 cmdline: loadaddll64.exe "C:\Users\user\Desktop\Glowcosi64.dll" MD5: E0CC9D126C39A9D2FA1CAD5027EBBD18)

 cmd.exe (PID: 3116 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\Glowcosi64.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)

 rundll32.exe (PID: 4728 cmdline: rundll32.exe "C:\Users\user\Desktop\Glowcosi64.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)

 rundll32.exe (PID: 1836 cmdline: rundll32.exe C:\Users\user\Desktop\Glowcosi64.dll,DllMain MD5: 73C519F050C20580F8A62C849D49215A)

 rundll32.exe (PID: 6528 cmdline: rundll32.exe C:\Users\user\Desktop\Glowcosi64.dll,GeogtrHfbokouxgzMvmrq MD5: 73C519F050C20580F8A62C849D49215A)

 rundll32.exe (PID: 6600 cmdline: rundll32.exe C:\Users\user\Desktop\Glowcosi64.dll,MabefshhHuruafdtQzntqpmiqf MD5: 73C519F050C20580F8A62C849D49215A)

 rundll32.exe (PID: 616 cmdline: rundll32.exe "C:\Users\user\Desktop\Glowcosi64.dll",DllMain MD5: 73C519F050C20580F8A62C849D49215A)

 rundll32.exe (PID: 744 cmdline: rundll32.exe "C:\Users\user\Desktop\Glowcosi64.dll",GeogtrHfbokouxgzMvmrq MD5: 73C519F050C20580F8A62C849D49215A)

 rundll32.exe (PID: 6840 cmdline: rundll32.exe "C:\Users\user\Desktop\Glowcosi64.dll",MabefshhHuruafdtQzntqpmiqf MD5: 73C519F050C20580F8A62C849D49215A)

cleanup

Malware Configuration

Threatname: IcedID

{

"url_path": "/news/",

"c2 url": [

"baeswea.com",

"bersaww.com"

,

"Campaign ID": 1892568649

}

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Copyright Joe Security LLC 2021

Page 4 of 16

Source	Rule	Description	Author	Strings
00000005.00000002.753734569.000002BB4AA8 0000.00000040.00000001.sdmp	MAL_IcedId_Core_LDR_20 2104	2021 loader for Bokbot / Icedid core (license.dat)	Thomas Barabosch, Telekom Security	0x21b2:\$internal_name: sadl_64.dll 0x2422:\$string0: GetCommandLineA 0x23a6:\$string1: LoadLibraryA 0x20eb:\$string2: ProgramData 0x2354:\$string3: SHLWAPI.dll 0x2320:\$string4: SHGetFolderPathA 0x2332:\$string7: SHELL32.dll 0x244a:\$string8: CreateThread
00000005.00000002.753734569.000002BB4AA8 0000.00000040.00000001.sdmp	JoeSecurity_IcedID_6	Yara detected IcedID	Joe Security	
00000001.00000002.1023202734.000001A9C7A E0000.00000040.00000001.sdmp	MAL_IcedId_Core_LDR_20 2104	2021 loader for Bokbot / Icedid core (license.dat)	Thomas Barabosch, Telekom Security	0x21b2:\$internal_name: sadl_64.dll 0x2422:\$string0: GetCommandLineA 0x23a6:\$string1: LoadLibraryA 0x20eb:\$string2: ProgramData 0x2354:\$string3: SHLWAPI.dll 0x2320:\$string4: SHGetFolderPathA 0x2332:\$string7: SHELL32.dll 0x244a:\$string8: CreateThread
00000001.00000002.1023202734.000001A9C7A E0000.00000040.00000001.sdmp	JoeSecurity_IcedID_6	Yara detected IcedID	Joe Security	
0000000C.00000002.824770074.000001473BB1 0000.00000040.00000001.sdmp	MAL_IcedId_Core_LDR_20 2104	2021 loader for Bokbot / Icedid core (license.dat)	Thomas Barabosch, Telekom Security	0x21b2:\$internal_name: sadl_64.dll 0x2422:\$string0: GetCommandLineA 0x23a6:\$string1: LoadLibraryA 0x20eb:\$string2: ProgramData 0x2354:\$string3: SHLWAPI.dll 0x2320:\$string4: SHGetFolderPathA 0x2332:\$string7: SHELL32.dll 0x244a:\$string8: CreateThread
Click to see the 27 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.rundll32.exe.1473bb10000.1.unpack	MAL_IcedId_Core_LDR_20 2104	2021 loader for Bokbot / Icedid core (license.dat)	Thomas Barabosch, Telekom Security	0xdb2:\$internal_name: sadl_64.dll 0x1022:\$string0: GetCommandLineA 0xfa6:\$string1: LoadLibraryA 0xceb:\$string2: ProgramData 0xf54:\$string3: SHLWAPI.dll 0xf20:\$string4: SHGetFolderPathA 0xf32:\$string7: SHELL32.dll 0x104a:\$string8: CreateThread
12.2.rundll32.exe.1473bb10000.1.unpack	JoeSecurity_IcedID_6	Yara detected IcedID	Joe Security	
9.2.rundll32.exe.2332f2d0000.1.unpack	MAL_IcedId_Core_LDR_20 2104	2021 loader for Bokbot / Icedid core (license.dat)	Thomas Barabosch, Telekom Security	0xdb2:\$internal_name: sadl_64.dll 0x1022:\$string0: GetCommandLineA 0xfa6:\$string1: LoadLibraryA 0xceb:\$string2: ProgramData 0xf54:\$string3: SHLWAPI.dll 0xf20:\$string4: SHGetFolderPathA 0xf32:\$string7: SHELL32.dll 0x104a:\$string8: CreateThread
9.2.rundll32.exe.2332f2d0000.1.unpack	JoeSecurity_IcedID_6	Yara detected IcedID	Joe Security	
13.2.rundll32.exe.136b1440000.1.unpack	MAL_IcedId_Core_LDR_20 2104	2021 loader for Bokbot / Icedid core (license.dat)	Thomas Barabosch, Telekom Security	0xdb2:\$internal_name: sadl_64.dll 0x1022:\$string0: GetCommandLineA 0xfa6:\$string1: LoadLibraryA 0xceb:\$string2: ProgramData 0xf54:\$string3: SHLWAPI.dll 0xf20:\$string4: SHGetFolderPathA 0xf32:\$string7: SHELL32.dll 0x104a:\$string8: CreateThread
Click to see the 43 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview



Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected IcedID

Networking:



C2 URLs / IPs found in malware configuration

E-Banking Fraud:



Yara detected IcedID

Stealing of Sensitive Information:



Yara detected IcedID

Remote Access Functionality:

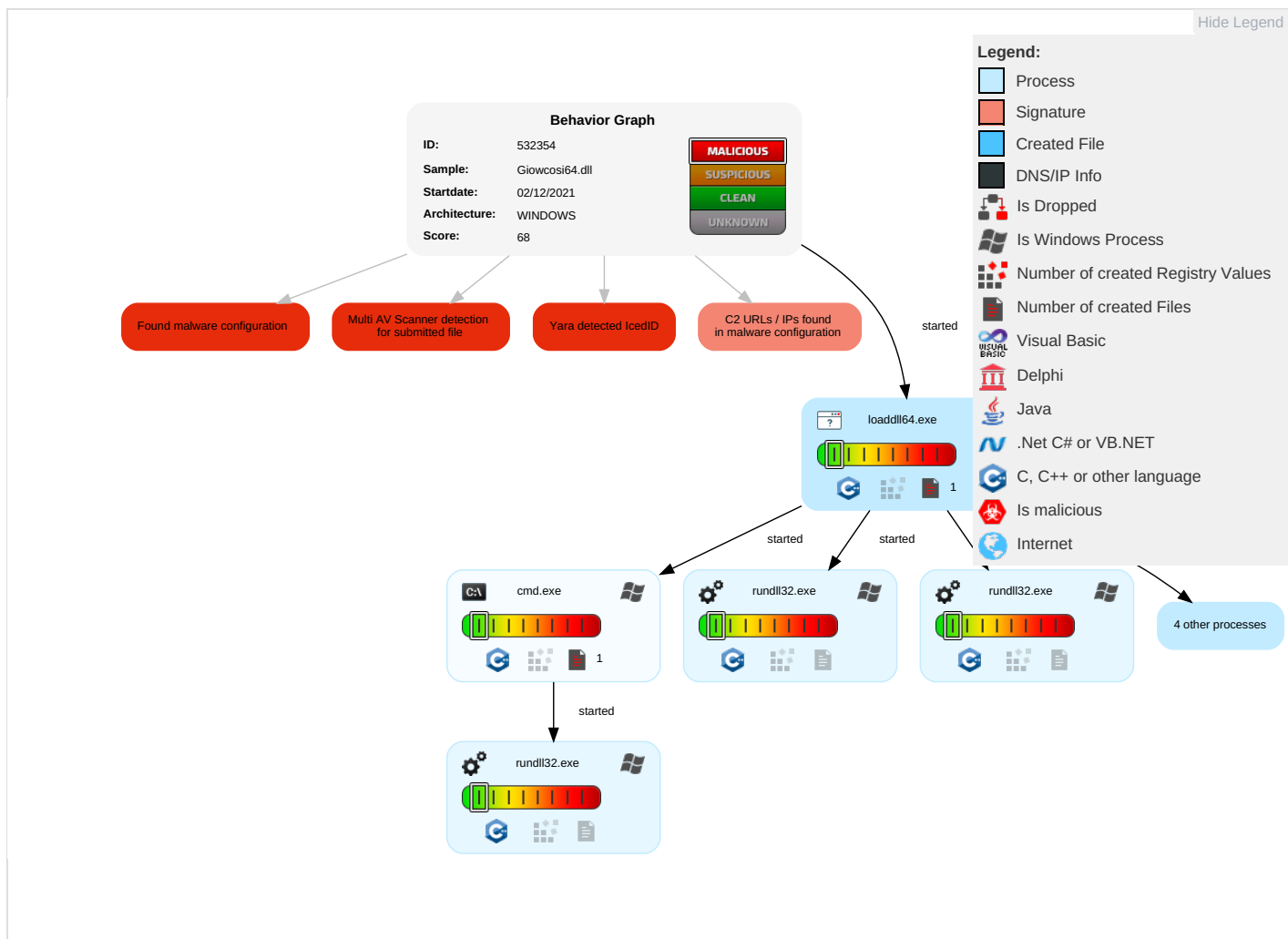


Yara detected IcedID

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Reputation
Valid Accounts	Native API 1	Path Interception	Process Injection 1 1	Rundll32 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Reputation Tracking With Aut
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Reputation Tracking With Aut
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtaining Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

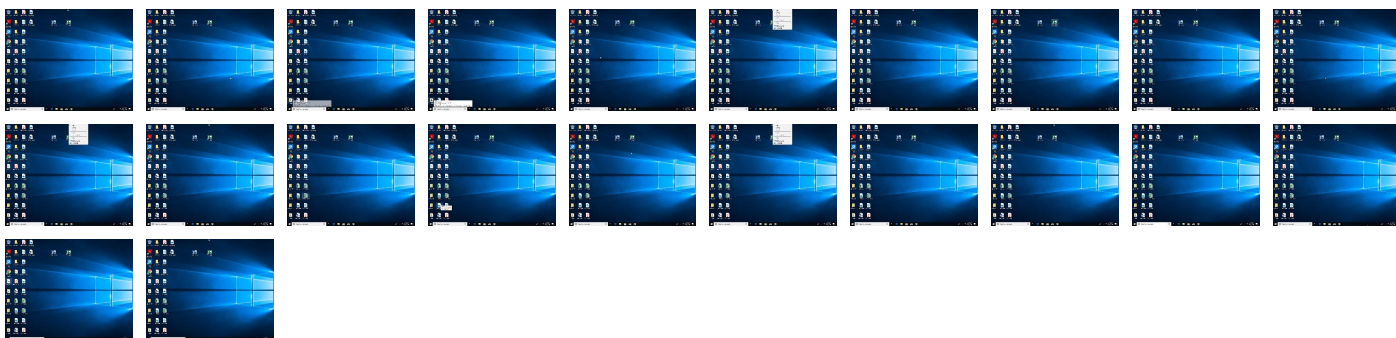
Behavior Graph



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
Giowcosi64.dll	20%	Virustotal		Browse
Giowcosi64.dll	14%	ReversingLabs	Win64.Trojan.Lazy	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
bersaww.com	0%	Avira URL Cloud	safe	
baeswea.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
bersaww.com	true	• Avira URL Cloud: safe	unknown
baeswea.com	true	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532354
Start date:	02.12.2021
Start time:	04:27:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Giowcosi64.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:	24
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:	mal68.troj.winDLL@17/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 30.4% (good quality ratio 20.6%) • Quality average: 41.9% • Quality standard deviation: 41.8%
HCA Information:	• Successful, ratio: 67% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

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):	6.413355690561383
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:	Giowcosi64.dll
File size:	116224
MD5:	8afee9d09b791bffd2372931cc9060ba
SHA1:	fe27de2819b394e2b0824dd28531a4ab914aa855
SHA256:	c340ae2dde2bd8fbae46b15abef0c7e706fe8953c837329bde409959836d6510
SHA512:	7e13ae3e0a1c783ad19e34be8a921473b239eb21d6630fa21a325aa245b5930f907182688ed819aef4cc85a0e1b4f407b5a76a40c907f8fb4eb0280e363d400e
SSDEEP:	1536:CzxBuW7NfJpGgiNrmcefpEuJDVrMOx4NQGroPYqWhO8sWKKhplKtBbM8izw8pCt2:eBnxfJgP4FfMCDVrYycoPj3QMUvvt
File Content Preview:	MZ.....@.....!..!Th is program cannot be run in DOS mode....\$......8..AY.. AY..AY...1..@Y..2:..BY..AY..KY...0..EY...0..@Y...0..@Y.. .RichAY.....PE..d.....U....."

File Icon



Icon Hash:

74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x18000eed0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x559AE088 [Mon Jul 6 20:09:44 2015 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:	f1a15344df95e4a35a13d3ab15c783e1

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1b9c2	0x1ba00	False	0.498488758484	data	6.47559683926	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1d000	0x2c4	0x400	False	0.412109375	data	3.30084623637	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1e000	0x50	0x200	False	0.04296875	Non-ISO extended-ASCII text, with no line terminators	0.188056906087	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x1f000	0xb4	0x200	False	0.267578125	data	1.85750400314	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 5112 Parent PID: 5876

General

Start time:	04:27:55
Start date:	02/12/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\Glowcosi64.dll"
Imagebase:	0x7ff6e9d40000
File size:	1136128 bytes
MD5 hash:	E0CC9D126C39A9D2FA1CAD5027EBBD18
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	- Rule: MAL_IcedId_Core_LDR_202104, Description: 2021 loader for Bokbot / Icedid core (license.dat), Source: 00000001.00000002.1023202734.000001A9C7AE0000.00000040.00000001.sdmp, Author: Thomas Barabosch, Telekom Security - Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 00000001.00000002.1023202734.000001A9C7AE0000.00000040.00000001.sdmp, Author: Joe Security - Rule: MAL_IcedId_Core_LDR_202104, Description: 2021 loader for Bokbot / Icedid core (license.dat), Source: 00000001.00000002.1023090624.000001A9C7890000.00000040.00000001.sdmp, Author: Thomas Barabosch, Telekom Security - Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 00000001.00000002.1023090624.000001A9C7890000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 3116 Parent PID: 5112

General

Start time:	04:27:56
Start date:	02/12/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\Glowcosi64.dll",#1
Imagebase:	0x7ff622070000
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: 1836 Parent PID: 5112**General**

Start time:	04:27:56
Start date:	02/12/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\Glowcosi64.dll,DllMain
Imagebase:	0x7ff7680d0000
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: MAL_IcedId_Core_LDR_202104, Description: 2021 loader for Bokbot / Icedid core (license.dat), Source: 00000004.00000002.744528892.0000023BAE180000.00000040.00000001.sdmp, Author: Thomas Barabosch, Telekom Security • Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 00000004.00000002.744528892.0000023BAE180000.00000040.00000001.sdmp, Author: Joe Security • Rule: MAL_IcedId_Core_LDR_202104, Description: 2021 loader for Bokbot / Icedid core (license.dat), Source: 00000004.00000002.744526075.0000023BAE170000.00000040.00000001.sdmp, Author: Thomas Barabosch, Telekom Security • Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 00000004.00000002.744526075.0000023BAE170000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 4728 Parent PID: 3116**General**

Start time:	04:27:56
Start date:	02/12/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\Glowcosi64.dll",#1
Imagebase:	0x7ff7680d0000
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: MAL_IcedId_Core_LDR_202104, Description: 2021 loader for Bokbot / Icedid core (license.dat), Source: 00000005.00000002.753734569.000002BB4AA80000.00000040.00000001.sdmp, Author: Thomas Barabosch, Telekom Security • Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 00000005.00000002.753734569.000002BB4AA80000.00000040.00000001.sdmp, Author: Joe Security • Rule: MAL_IcedId_Core_LDR_202104, Description: 2021 loader for Bokbot / Icedid core (license.dat), Source: 00000005.00000002.753421493.000002BB4AA70000.00000040.00000001.sdmp, Author: Thomas Barabosch, Telekom Security • Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 00000005.00000002.753421493.000002BB4AA70000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6528 Parent PID: 5112**General**

Start time:	04:28:00
-------------	----------

Start date:	02/12/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\Glowcosi64.dll,GeogtrHfbokouxgzMvmrq
Imagebase:	0x7ff7680d0000
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: MAL_IcedId_Core_LDR_202104, Description: 2021 loader for Bokbot / Icedid core (license.dat), Source: 00000006.00000002.760108318.000002CA7BEE0000.00000040.00000001.sdmp, Author: Thomas Barabosch, Telekom Security - Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 00000006.00000002.760108318.000002CA7BEE0000.00000040.00000001.sdmp, Author: Joe Security - Rule: MAL_IcedId_Core_LDR_202104, Description: 2021 loader for Bokbot / Icedid core (license.dat), Source: 00000006.00000002.760094169.000002CA7BED0000.00000004.00000001.sdmp, Author: Thomas Barabosch, Telekom Security - Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 00000006.00000002.760094169.000002CA7BED0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6600 Parent PID: 5112

General

Start time:	04:28:05
Start date:	02/12/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\Glowcosi64.dll,MabefshhHuruaftdQzntqpmiqf
Imagebase:	0x7ff7680d0000
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: MAL_IcedId_Core_LDR_202104, Description: 2021 loader for Bokbot / Icedid core (license.dat), Source: 00000009.00000002.760340152.000002332F2C0000.00000004.00000001.sdmp, Author: Thomas Barabosch, Telekom Security - Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 00000009.00000002.760340152.000002332F2C0000.00000004.00000001.sdmp, Author: Joe Security - Rule: MAL_IcedId_Core_LDR_202104, Description: 2021 loader for Bokbot / Icedid core (license.dat), Source: 00000009.00000002.760354110.000002332F2D0000.00000004.00000001.sdmp, Author: Thomas Barabosch, Telekom Security - Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 00000009.00000002.760354110.000002332F2D0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 616 Parent PID: 5112

General

Start time:	04:28:46
Start date:	02/12/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\Glowcosi64.dll",DllMain
Imagebase:	0x7ff7680d0000
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: MAL_IcedId_Core_LDR_202104, Description: 2021 loader for Bokbot / Icedid core (license.dat), Source: 0000000A.00000002.826876248.000001C801D60000.00000040.00000001.sdmp, Author: Thomas Barabosch, Telekom Security • Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 0000000A.00000002.826876248.000001C801D60000.00000040.00000001.sdmp, Author: Joe Security • Rule: MAL_IcedId_Core_LDR_202104, Description: 2021 loader for Bokbot / Icedid core (license.dat), Source: 0000000A.00000002.826795548.000001C801D10000.00000004.00000001.sdmp, Author: Thomas Barabosch, Telekom Security • Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 0000000A.00000002.826795548.000001C801D10000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 744 Parent PID: 5112

General

Start time:	04:28:47
Start date:	02/12/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\Giowcosi64.dll",GeogrHfbokouxgzMvmrq
Imagebase:	0x7ff7680d0000
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: MAL_IcedId_Core_LDR_202104, Description: 2021 loader for Bokbot / Icedid core (license.dat), Source: 0000000C.00000002.824770074.000001473BB10000.00000040.00000001.sdmp, Author: Thomas Barabosch, Telekom Security • Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 0000000C.00000002.824770074.000001473BB10000.00000040.00000001.sdmp, Author: Joe Security • Rule: MAL_IcedId_Core_LDR_202104, Description: 2021 loader for Bokbot / Icedid core (license.dat), Source: 0000000C.00000002.824761939.000001473BB00000.00000004.00000001.sdmp, Author: Thomas Barabosch, Telekom Security • Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 0000000C.00000002.824761939.000001473BB00000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6840 Parent PID: 5112

General

Start time:	04:28:47
Start date:	02/12/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\Giowcosi64.dll",MabefshhHuruaftdQzntqpmiqf
Imagebase:	0x360000
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: MAL_IcedId_Core_LDR_202104, Description: 2021 loader for Bokbot / Icedid core (license.dat), Source: 0000000D.00000002.825167289.00000136B1430000.00000004.00000001.sdmp, Author: Thomas Barabosch, Telekom Security • Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 0000000D.00000002.825167289.00000136B1430000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_IcedId_Core_LDR_202104, Description: 2021 loader for Bokbot / Icedid core (license.dat), Source: 0000000D.00000002.825171186.00000136B1440000.00000040.00000001.sdmp, Author: Thomas Barabosch, Telekom Security • Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 0000000D.00000002.825171186.00000136B1440000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Disassembly

Code Analysis