ID: 829723
Sample Name:
gozi_loader.bin.exe
Cookbook: default.jbs
Time: 06:48:05
Date: 19/03/2023
Version: 37.0.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report gozi_loader.bin.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Threat Intel 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Signatures 5
Memory Dumps 5
Sigma Signatures 5
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Key, Mouse, Clipboard, Microphone and Screen Capturing 6
E-Banking Fraud 6
System Summary 6
Hooking and other Techniques for Hiding and Protection 6
Malware Analysis System Evasion 6
Anti Debugging 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 9
Public IPs 10
General Information 10
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 11
General 11
File Icon 12
Static PE Info 12
General 12
Entrypoint Preview 12
Rich Headers 13
Data Directories 13
Sections 14
Imports 14
Network Behavior 14
Network Port Distribution 14
TCP Packets 15
UDP Packets 15
DNS Queries 15
DNS Answers 15
Statistics 15
System Behavior 15
Analysis Process: gozi_loader.bin.exePID: 5828, Parent PID: 3452 15
General 15

File Activities 16
Disassembly 16

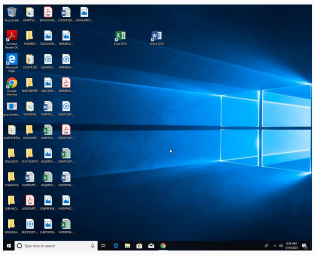
Windows Analysis Report

gozi_loader.bin.exe

Overview

General Information

Sample Name:	gozi_loader.bin.exe
Analysis ID:	829723
MD5:	700d3ea5098e..
SHA1:	8796dfe929e1f..
SHA256:	061c271c0617…
Tags:	7709 exe gozi
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

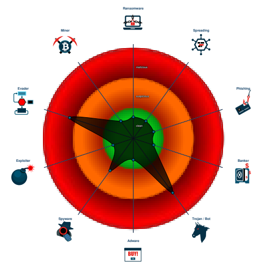
Ursnif

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

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- Malicious sample detected (through…
- Yara detected Ursnif
- Found evasive API chain (may stop…
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Found API chain indicative of debug…
- Machine Learning detection for sam…
- Creates a DirectInput object (often f…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- gozi_loader.bin.exe (PID: 5828 cmdline: C:\Users\user\Desktop\gozi_loader.bin.exe MD5: 700D3EA5098E7B7F45FCEEC4DF9DF798)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Gozi, Ursnif	2000 Ursnif aka Snifula2006 Gozi v1.0, Gozi CRM, CRM, Papras2010 Gozi v2.0, Gozi ISFB, ISFB, Pandemyia(*)-> 2010 Gozi Prinimalka -> Vawtrak/NeverquestIn 2006, Gozi v1.0 ('Gozi CRM' aka 'CRM') aka Papras was first observed.It was offered as a CaaS, known as 76Service. This first version of Gozi was developed by Nikita Kurmin, and he borrowed code from Ursnif aka Snifula, a spyware developed by Alexey Ivanov around 2000, and some other kits. Gozi v1.0 thus had a formgrabber module and often is classified as Ursnif aka Snifula.In September 2010, the source code of a particular Gozi CRM dll version was leaked, which led to Vawtrak/Neverquest (in combination with Pony) via Gozi Prinimalka (a slightly modified Gozi v1.0) and Gozi v2.0 (aka 'Gozi ISFB' aka 'ISFB' aka Pandemyia). This version came with a webinject module.	No Attribution	http://blog.malwaremustdie.org/2013/02/the-infection-of-styx-exploit-kit.htmlhttp://researchcenter.paloaltonetworks.com/2017/02/unit42-banking-trojans-ursnif-global-distribution-networks-identified/https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/https://blog.gdatasoftware.com/2016/11/29325-analysis-ursnif-spying-on-your-data-since-2007https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.gozi

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"X0CjtxCEKhyWPVzp/ypnuYDLNIOhkqPDio0ZyqaAtAnkFEsoQnBwh+tF9ICcDX0ifMDWcBjhwZoirN+aTqJXJlbhk0Ve6q6ZbFlkkvZMgxosr3pMdiauYeQ90ivavpHebCxhRZxAtsp2ORNHCEiYgF72+cVEjuJDfG0Ix9Z30gBFauUE
bEbx4aeIvTonSjXG3aF3/+WexILzZBT8G6LohnVlt8mcAM//OC6cXwk1gyscR6PxkpD1IRbzi9V6b1oxKje1De4hIMx1QizHvXbcQQK+/sLO0kr23FfUgVRhjnHWAGKHyANFU1dIviwuls3MsDx7dUZbdioQXIUlQY7nSWTk+HvbCX58k
e9Hwzn2SHs=",
  "c2_domain": [
    "checklist.skype.com",
    "62.173.141.252",
    "31.41.44.33",
    "109.248.11.112"
  ],
  "botnet": "7709",
  "server": "50",
  "serpent_key": "pThBpljTg5GSXpa1",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.389853004.0000000001348000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.389853004.0000000001348000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0x1228:$a1: /C ping localhost -n %u && del "%s" • 0xea8:$a2: /C "copy "%s" "%s" /y && "%s" "%s" • 0xf00:$a3: /C "copy "%s" "%s" /y && rundll32 "%s",%S" • 0xa9c:$a5: filename="%.4u.%lu" • 0x63a:$a7: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0x876:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xbb7:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xe6d:$a9: &whoami=%s • 0xe56:$a10: %u.%u_%u_%u_x%u • 0xd63:$a11: size=%u&hash=0x%08x • 0xb1d:$a12: &uptime=%u • 0x6fb:$a13: %systemroot%\system32\c_1252.nls • 0x1298:$a14: IE10RunOnceLastShown_TIMESTAMP
00000000.00000003.389853004.0000000001348000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0xb54:$a1: soft=%u&version=%u&user=%08x%08x%08x%08x&server=%u&id=%u&crc=%x • 0x63a:$a2: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0xa68:$a3: Content-Disposition: form-data; name="upload_file"; filename="%.4u.%lu" • 0xcf2:$a5: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT %u.%u%s) • 0xd96:$a9: Software\AppDataLow\Software\Microsoft\ • 0x1c80:$a9: Software\AppDataLow\Software\Microsoft\
00000000.00000003.389784429.0000000001348000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.389784429.0000000001348000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0x1228:$a1: /C ping localhost -n %u && del "%s" • 0xea8:$a2: /C "copy "%s" "%s" /y && "%s" "%s" • 0xf00:$a3: /C "copy "%s" "%s" /y && rundll32 "%s",%S" • 0xa9c:$a5: filename="%.4u.%lu" • 0x63a:$a7: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0x876:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xbb7:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xe6d:$a9: &whoami=%s • 0xe56:$a10: %u.%u_%u_%u_x%u • 0xd63:$a11: size=%u&hash=0x%08x • 0xb1d:$a12: &uptime=%u • 0x6fb:$a13: %systemroot%\system32\c_1252.nls • 0x1298:$a14: IE10RunOnceLastShown_TIMESTAMP

Click to see the 25 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

Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

System Summary

Malicious sample detected (through community Yara rule)

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Malware Analysis System Evasion

Found evasive API chain (may stop execution after checking system information)

Anti Debugging

Found API chain indicative of debugger detection

Stealing of Sensitive Information

Yara detected Ursnif

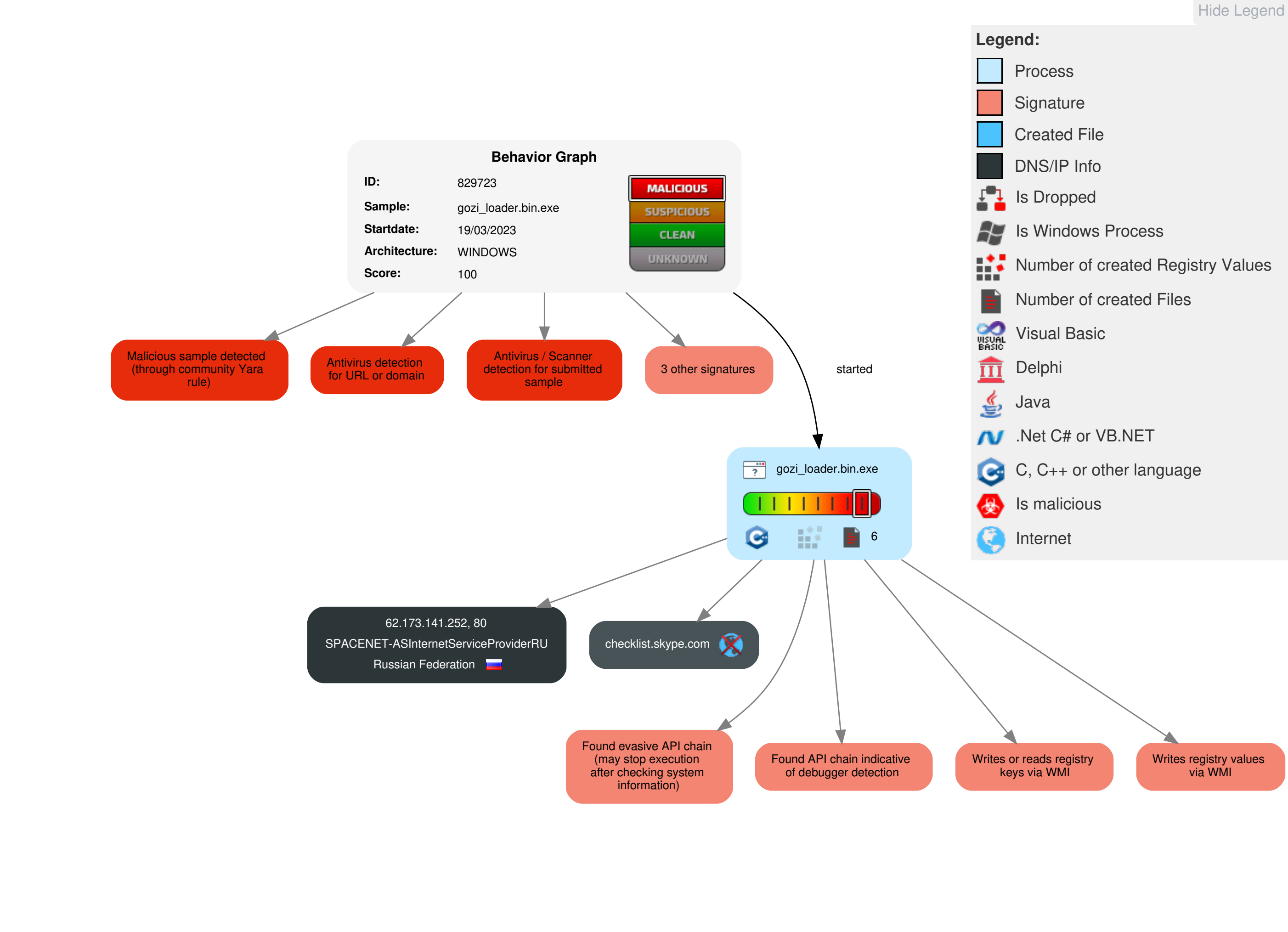
Remote Access Functionality

Yara detected Ursnif

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	2 Windows Management Instrumentation	Path Interception	Path Interception	1 Virtualization/Sandbox Evasion	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Non-Application Layer Protocol	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 1 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Software Packing	LSASS Memory	1 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 1 4 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	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

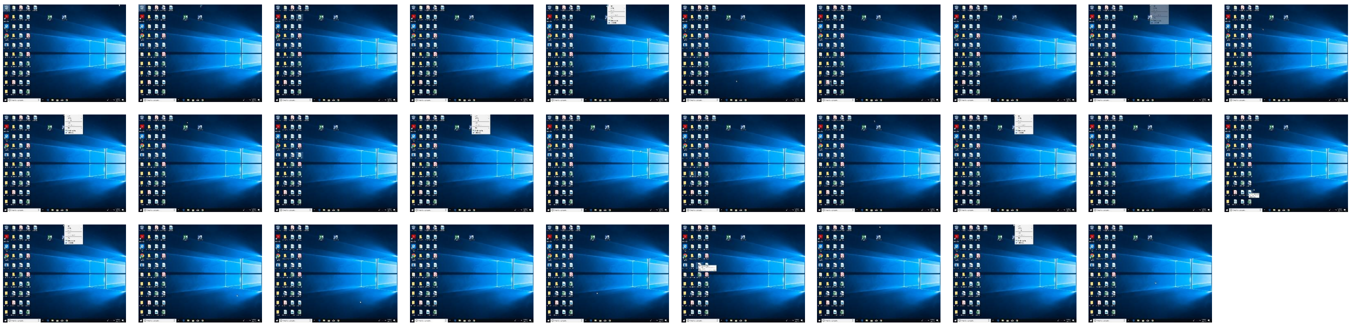
Behavior Graph



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
gozi_loader.bin.exe	62%	ReversingLabs	Win32.Trojan.Razy	
gozi_loader.bin.exe	100%	Avira	TR/Crypt.XPACK.Gen7	
gozi_loader.bin.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.gozi_loader.bin.exe.570000.1.unpack	100%	Avira	HEUR/AGEN.1245293		Download File
0.2.gozi_loader.bin.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.0.gozi_loader.bin.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://62.173.141.252/t	100%	Avira URL Cloud	malware	
http://62.173.141.252/drew/y3O_2BnUepUaUzeF4C/FRcN_2F0g/JenmUZWHq05STtkRb5sf/OjHYpR2L_2F2jEOkrjw/2V_	100%	Avira URL Cloud	malware	
http://ctldl.windowsup-k	0%	Avira URL Cloud	safe	
http://62.173	0%	Avira URL Cloud	safe	
http://62.173	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
checklist.skype.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://checklist.skype.com/drew/YJnT5wK9lbi_2FYe8Kf5y/QYTs_2B6r_2FF8l0/fLw2xZG1XgX5PrO/q_2Bnf6Otc_2F	gozi_loader.bin.exe, 00000000.00000002.512142359.0000000000775000.00000004.00000020.00020000.00000000.sdmp	false		high
http://62.173.141.252/drew/y3O_2BnUepUaUzeF4C/FRcN_2F0g/JenmUZWHq05STtkRb5sf/OjHYpR2L_2F2jEOkrjw/2V_	gozi_loader.bin.exe, 00000000.00000002.512142359.0000000000775000.00000004.00000020.00020000.00000000.sdmp, gozi_loader.bin.exe, 00000000.00000002.512142359.0000000000783000.00000004.00000020.00020000.00000000.sdmp, gozi_loader.bin.exe, 00000000.00000002.512142359.0000000000736000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://62.173	gozi_loader.bin.exe, 00000000.00000002.512447276.0000000000E4C000.00000004.00000010.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	low
http://ctldl.windowsup-k	gozi_loader.bin.exe, 00000000.00000002.512142359.0000000000736000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://62.173.141.252/t	gozi_loader.bin.exe, 00000000.00000002.512142359.0000000000736000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
62.173.141.252	unknown	Russian Federation		34300	SPACENET-ASInternetServiceProviderRU	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	829723
Start date and time:	2023-03-19 06:48:05 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, 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
Sample file name:	gozi_loader.bin.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@1/0@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 100%) • Quality average: 89% • Quality standard deviation: 15.4%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

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 (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.18633160544667
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	gozi_loader.bin.exe

File size:	40960
MD5:	700d3ea5098e7b7f45fceec4df9df798
SHA1:	8796dfe929e1f9d507a4c7da048fb80eeaed94eb
SHA256:	061c271c0617e56aeb196c834fcab2d24755afa50cd95cc6a299d76be496a858
SHA512:	ae66c4be081a5e2e33ab1b729fc7790fe79568063a6611eb9dcb957eb581b97260e7e2ffdd40cdbd4f127e7b8a8cb53b57f3228eb292659994060ca87861ccea
SSDEEP:	768:4gYKd2Usr2yS5PLHBjderMpEvpZi7/kMPWq9aky77XTm9:4fKdpfh5zHzeApsnI/eZDLI
TLSH:	2403E1230D24A0ABEB0FC7F0675FA1BED3F9810536149867D6223A366DB3475823B685
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......Y..+...x...x...x..lx...x...xQ..x...x...x..vx...x..kx...x..nx...xRich...x........PE..L......c...................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x401de1
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x63D2C3B3 [Thu Jan 26 18:17:23 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	1640d668d1471f340cbe565fe63522f6

Entrypoint Preview

Instruction
push esi
xor esi, esi
push esi
push 00400000h
push esi
call dword ptr [0040303Ch]
mov dword ptr [00404160h], eax
cmp eax, esi
je 00007FA17CC64B87h
push esi
call dword ptr [00403008h]
mov dword ptr [00404170h], eax
call dword ptr [00403044h]
call 00007FA17CC64745h
push dword ptr [00404160h]
mov esi, eax
call dword ptr [00403040h]
push esi
call dword ptr [00403048h]
pop esi
push ebp

Instruction
mov ebp, esp
sub esp, 24h
mov ecx, 43175AC3h
sub ecx, dword ptr [ebp+0Ch]
push ebx
push esi
mov esi, dword ptr [ebp+08h]
mov dword ptr [ebp-0Ch], ecx
mov dword ptr [ebp-1Ch], ecx
mov dword ptr [ebp-04h], ecx
mov ebx, ecx
mov dword ptr [ebp-08h], ecx
mov cl, byte ptr [eax]
mov byte ptr [esi], cl
lea ecx, dword ptr [esi+01h]
lea eax, dword ptr [eax+01h]
push edi
mov dword ptr [ebp-10h], ecx
mov dword ptr [ebp-24h], eax
jne 00007FA17CC64CE1h
mov esi, dword ptr [ebp+0Ch]
lea edx, dword ptr [ebp-24h]
call 00007FA17CC63EAEh
test eax, eax
je 00007FA17CC64CAFh
call 00007FA17CC63EA1h
test eax, eax
je 00007FA17CC64BD6h
call 00007FA17CC63E98h
xor ebx, ebx
test eax, eax
je 00007FA17CC64B9Ch
mov edi, 43175AC7h
sub edi, esi
je 00007FA17CC64B85h
mov esi, dword ptr [ebp+0Ch]
lea edx, dword ptr [ebp-24h]
call 00007FA17CC63E7Eh
dec edi
lea ebx, dword ptr [eax+ebx*2]
jne 00007FA17CC64B51h
test ebx, ebx
je 00007FA17CC64B70h
mov eax, dword ptr [ebp-10h]
mov ecx, dword ptr [ebp+00h]

Rich Headers

Programming Language:	• [IMP] VS2008 SP1 build 30729 • [LNK] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x30e8	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6000	0x10	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x7000	0xe4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x3000	0xa8	.rdata
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	0x102c	0x1200	False	0.6649305555555556	data	6.219365687330024	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x3000	0x4c0	0x600	False	0.4635416666666667	data	4.465242332731156	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x4000	0x194	0x200	False	0.056640625	data	0.12227588125913882	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.bss	0x5000	0x2df	0x400	False	0.767578125	data	6.319685755564182	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x6000	0x10	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7000	0x8000	0x7200	False	0.9724506578947368	data	7.864170679978452	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Imports

DLL	Import
ntdll.dll	_snwprintf, memset, NtQuerySystemInformation, _aulldiv
KERNEL32.dll	GetModuleHandleA, GetLocaleInfoA, GetSystemDefaultUILanguage, HeapAlloc, HeapFree, WaitForSingleObject, Sleep, ExitThread, lstrlenW, GetLastError, VerLanguageNameA, GetExitCodeThread, CloseHandle, HeapCreate, HeapDestroy, GetCommandLineW, ExitProcess, SetLastError, TerminateThread, SleepEx, GetModuleFileNameW, CreateThread, OpenProcess, CreateEventA, GetLongPathNameW, GetVersion, GetCurrentProcessId, GetProcAddress, LoadLibraryA, VirtualProtect, MapViewOfFile, GetSystemTimeAsFileTime, CreateFileMappingW, QueueUserAPC
ADVAPI32.dll	ConvertStringSecurityDescriptorToSecurityDescriptorA

Network Behavior

Network Port Distribution

Total Packets: 4

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 19, 2023 06:50:26.118061066 CET	49699	80	192.168.2.3	62.173.141.252
Mar 19, 2023 06:50:29.126327038 CET	49699	80	192.168.2.3	62.173.141.252
Mar 19, 2023 06:50:35.127047062 CET	49699	80	192.168.2.3	62.173.141.252

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 19, 2023 06:49:05.965269089 CET	61787	53	192.168.2.3	8.8.8.8
Mar 19, 2023 06:49:05.985430002 CET	53	61787	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 19, 2023 06:49:05.965269089 CET	192.168.2.3	8.8.8.8	0x549b	Standard query (0)	checklist.skype.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 19, 2023 06:49:05.985430002 CET	8.8.8.8	192.168.2.3	0x549b	Name error (3)	checklist.skype.com	none	none	A (IP address)	IN (0x0001)	false

Statistics

No statistics

System Behavior

Analysis Process: gozi_loader.bin.exe PID: **5828**, Parent PID: **3452**

General

Target ID:	0
Start time:	06:48:56
Start date:	19/03/2023
Path:	C:\Users\user\Desktop\gozi_loader.bin.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\gozi_loader.bin.exe
Imagebase:	0x400000
File size:	40960 bytes
MD5 hash:	700D3EA5098E7B7F45FCEEC4DF9DF798
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.389853004.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.389853004.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.389853004.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.389784429.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.389784429.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.389784429.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.512474249.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000002.512474249.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000002.512474249.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.389835658.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.389835658.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.389835658.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.389702984.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.389702984.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.389702984.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.389820029.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.389820029.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.389820029.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.389734905.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.389734905.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.389734905.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.389803220.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.389803220.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.389803220.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.389762139.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000000.00000003.389762139.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000000.00000003.389762139.0000000001348000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly