ID: 355735
Sample Name: GqSL8M2a72
Cookbook: default.jbs
Time: 15:03:09
Date: 21/02/2021
Version: 31.0.0 Emerald

Table of Contents

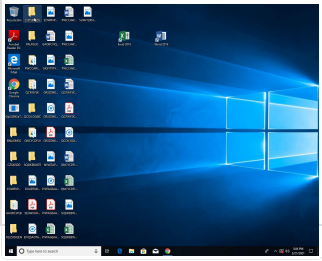
Analysis Report GqSL8M2a72

Overview

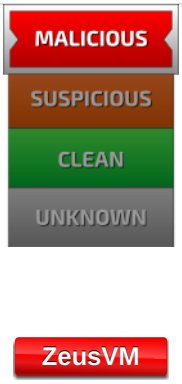
General Information

Sample Name:	GqSL8M2a72 (renamed file extension from none to exe)
Analysis ID:	355735
MD5:	4fc29198fcc9a9f…
SHA1:	5b112c77ea208d..
SHA256:	98d8b13f297953a.
Tags:	uncategorized ZeuS

Most interesting Screenshot:



Detection

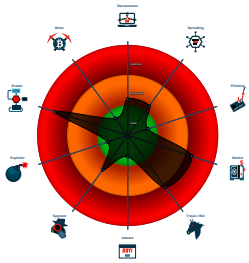


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected ZeusVM e-Banking Trojan
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Multi AV Scanner detection for subm…
- Contains VNC / remote desktop func…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Antivirus or Machine Learning detec…
- Contains functionality to access load…
- Contains functionality to call native f…
- Contains functionality to dynamically…

Classification



Startup

- **System is w10x64**
- GqSL8M2a72.exe (PID: 1832 cmdline: 'C:\Users\user\Desktop\GqSL8M2a72.exe' MD5: 4FC29198FCC9A9FE3B31F7549D54D8E9)
  - GqSL8M2a72.exe (PID: 5864 cmdline: 'C:\Users\user\Desktop\GqSL8M2a72.exe' MD5: 4FC29198FCC9A9FE3B31F7549D54D8E9)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

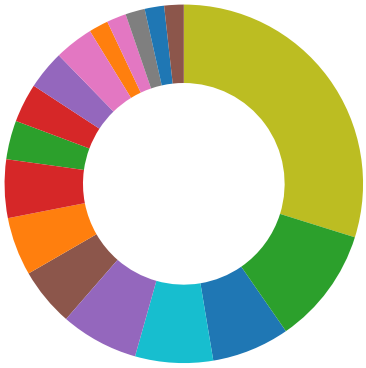
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Cryptography
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud



- Protection of GUI
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Uses 32bit PE files

E-Banking Fraud:

Detected ZeusVM e-Banking Trojan

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Remote Access Functionality:

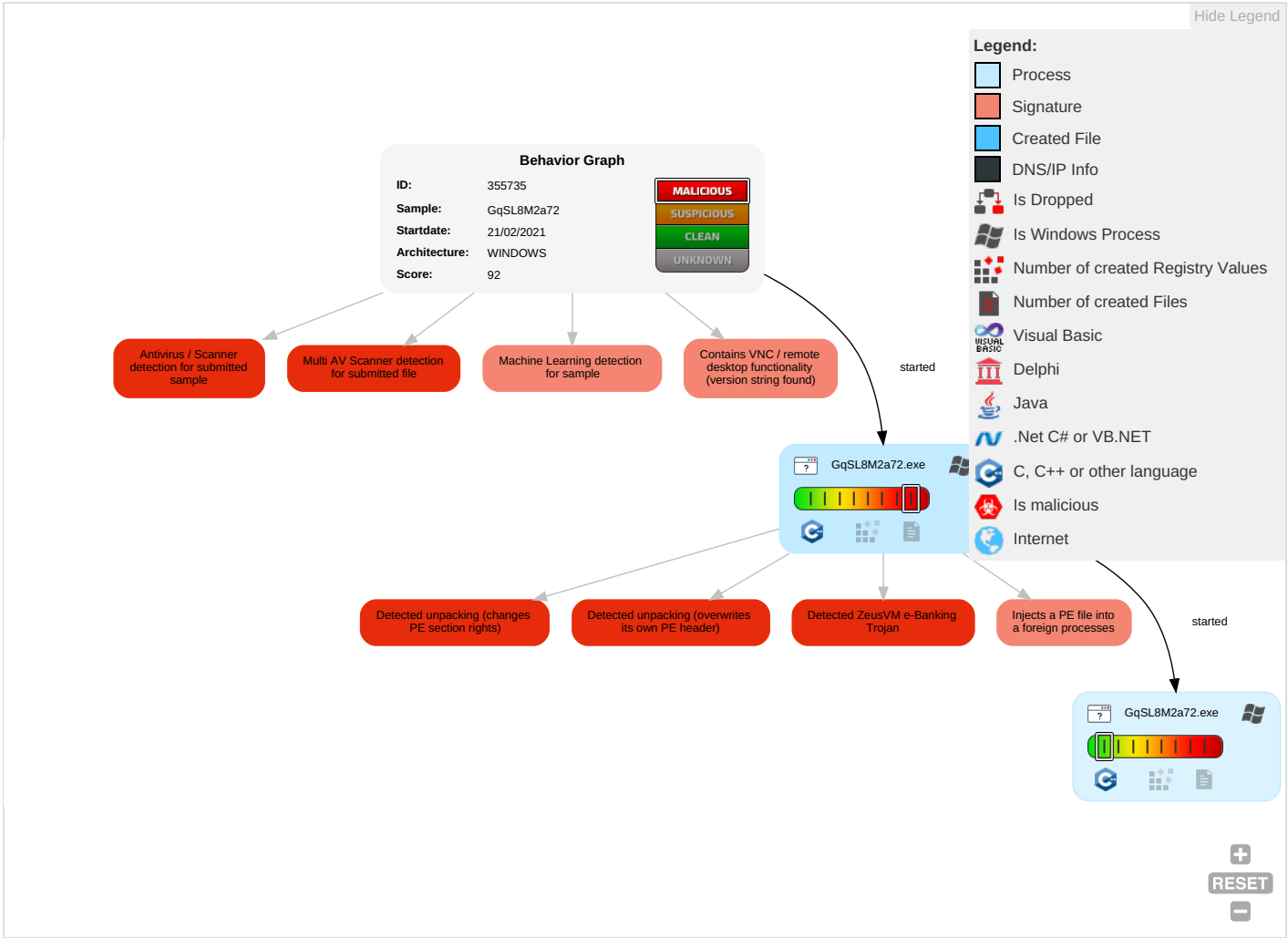
Contains VNC / remote desktop functionality (version string found)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts 1	Native API 1	DLL Side-Loading 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	Input Capture 2 1	System Time Discovery 2	Remote Desktop Protocol 1	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Application Shimming 1	Application Shimming 1	Obfuscated Files or Information 2	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Encrypted Channel 2	Exploit SS7 t Redirect Pho Calls/SMS

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Domain Accounts	At (Linux)	Create Account 1	Valid Accounts 1	Install Root Certificate 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Remote Access Software 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Valid Accounts 1	Access Token Manipulation 1 1	Software Packing 2 2	NTDS	System Information Discovery 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Process Injection 1 1 1	DLL Side-Loading 1	LSA Secrets	Network Share Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Security Software Discovery 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1 1	DCSync	Process Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 1	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
GqSL8M2a72.exe	86%	Virustotal		Browse
GqSL8M2a72.exe	78%	Metadefender		Browse
GqSL8M2a72.exe	88%	ReversingLabs	Win32.Trojan.Zeus	
GqSL8M2a72.exe	100%	Avira	HEUR/AGEN.1108096	
GqSL8M2a72.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.GqSL8M2a72.exe.400000.0.unpack	100%	Avira	TR/Kazy.MK		Download File
2.0.GqSL8M2a72.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108090		Download File

Source	Detection	Scanner	Label	Link	Download
1.0.GqSL8M2a72.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108090		Download File
1.2.GqSL8M2a72.exe.5e0000.1.unpack	100%	Avira	TR/Kazy.MK		Download File
1.2.GqSL8M2a72.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108090		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	355735
Start date:	21.02.2021
Start time:	15:03:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	GqSL8M2a72 (renamed file extension from none to exe)
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:	3
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:	mal92.bank.troj.evad.winEXE@3/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 92.4%) • Quality average: 82.2% • Quality standard deviation: 29.9%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated

Warnings:	Show All • Exclude process from analysis (whitelisted): svchost.exe

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 (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.080431308237134
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:	GqSL8M2a72.exe
File size:	161962
MD5:	4fc29198fcc9a9fe3b31f7549d54d8e9
SHA1:	5b112c77ea208d570eedaad0d5880e6fc19cffbc
SHA256:	98d8b13f297953a0b4f915e55cd527f0f1461d42b917b77aa99f05446f6fdd12

General

SHA512:	a023c11edff4e1059bb3e22edb53d9774c66b44379c3121 b761e9fa276eae42aca7b15b82b45aef4fc829095c2c264 728147bb840f36650e4566136a79f6fead
SSDEEP:	3072:sK9smc3K+aCj93AnXGaNkdrgm9nl0JdqFJG2Gzt R07IVgfXs7ZsFz6x:JfcVho2eaJnl0JoLGtzz074IsYOx
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....%...a...a ...a.....c.....`.....c...h...|...a...1.....).`.....`...Richa..... .....PE..L.....<.....^.

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40156c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NO_ISOLATION
Time Stamp:	0x3CAFB40C [Sun Apr 7 02:50:52 2002 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	3d72c2249f14f4cc74dd098fd236f98a

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 1Ch
push 0042713Ch
call dword ptr [00427024h]
test eax, eax
jne 00007F7554D791E7h
call 00007F7554D79239h
push edi
xor edi, edi
cmp dword ptr [004294ECh], edi
je 00007F7554D79221h
call 00007F7554D78FACh
test eax, eax
je 00007F7554D79218h
push esi
push 004270C4h
call 00007F7554D78C5Dh
mov esi, dword ptr [00427080h]
pop ecx
jmp 00007F7554D791F6h
lea eax, dword ptr [ebp-1Ch]
push eax
call dword ptr [00427088h]
lea eax, dword ptr [ebp-1Ch]

Instruction
push eax
call dword ptr [00427060h]
push edi
push edi
push edi
lea eax, dword ptr [ebp-1Ch]
push eax
call esi
test eax, eax
jne 00007F7554D791C1h
pop esi
mov eax, dword ptr [00428278h]
pop edi
leave
retn 000Ch
push 004270C4h
call 00007F7554D78C1Eh
pop ecx
push 00000000h
push 0016FCD8h
push 00000000h
call dword ptr [0042702Ch]
mov dword ptr [0042A4F4h], eax
test eax, eax
jne 00007F7554D791F1h
call dword ptr [00427030h]
mov dword ptr [0042A4F4h], eax
test eax, eax
je 00007F7554D791FDh
call 00007F7554D78BEAh
mov eax, dword ptr [eax+30h]
mov dword ptr [004294ECh], eax
test eax, eax
je 00007F7554D791ECh
mov eax, dword ptr [00428278h]
jmp 00007F7554D791E6h
ret
mov eax, dword ptr [004294ECh]
mov eax, dword ptr [eax+10h]
mov ecx, dword ptr [eax+44h]

Rich Headers

Programming Language:	• [LNK] VS2010 build 30319 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x271e0	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
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	0x27000	0xac	.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	0x25dc6	0x25e00	False	0.732924659653	data	5.98756571788	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x27000	0x632	0x800	False	0.43115234375	zlib compressed data	4.18800845972	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x28000	0x2538	0x400	False	0.626953125	data	4.83990809034	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	LocalAlloc, GetModuleHandleA, OutputDebugStringA, lstrcpyA, LoadLibraryA, GetProcAddress, HeapCreate, GetProcessHeap, ExitProcess, SetUnhandledExceptionFilter, HeapAlloc, lstrlenA
USER32.dll	GetActiveWindow, DispatchMessageW, UpdateWindow, SetWindowPos, CreateWindowExA, MessageBoxA, ShowWindow, FindWindowA, MessageBoxW, GetMessageW, SetFocus, TranslateMessage, DefWindowProcW
POWRPROF.dll	GetPwrCapabilities, IsPwrShutdownAllowed, IsPwrHibernateAllowed, GetActivePwrScheme
WINTRUST.dll	WintrustGetRegPolicyFlags
CRYPT32.dll	CryptStringToBinaryA, CertCreateCertificateChainEngine
imagehlp.dll	ImageEnumerateCertificates
WINMM.dll	mciSendStringW
CLUSAPI.dll	ClusterEnum

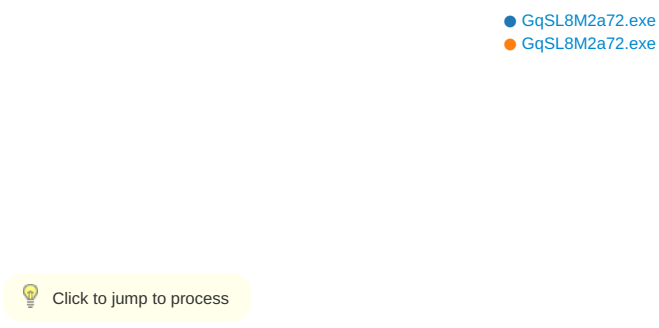
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: GqSL8M2a72.exe PID: 1832 Parent PID: 5716

General

Start time:	15:03:53
Start date:	21/02/2021
Path:	C:\Users\user\Desktop\GqSL8M2a72.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\GqSL8M2a72.exe'
Imagebase:	0x400000
File size:	161962 bytes
MD5 hash:	4FC29198FCC9A9FE3B31F7549D54D8E9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: GqSL8M2a72.exe PID: 5864 Parent PID: 1832

General

Start time:	15:03:54
Start date:	21/02/2021
Path:	C:\Users\user\Desktop\GqSL8M2a72.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\GqSL8M2a72.exe'
Imagebase:	0x400000
File size:	161962 bytes
MD5 hash:	4FC29198FCC9A9FE3B31F7549D54D8E9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis