ID: 528518
Sample Name:
Zr26f1rL6r.danger
Cookbook: default.jbs
Time: 12:43:41
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2021

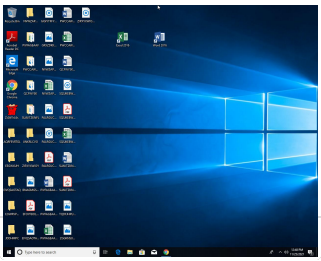
Windows Analysis Report Zr26f1rL6r.danger

Overview

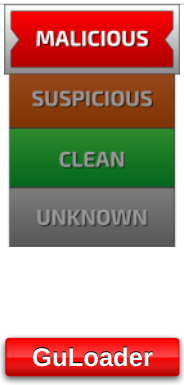
General Information

Sample Name:	Zr26f1rL6r.danger (renamed file extension from danger to exe)
Analysis ID:	528518
MD5:	812181df251e064.
SHA1:	aa38a567ee4848..
SHA256:	4d6c910a379d00..
Infos:	

Most interesting Screenshot:



Detection

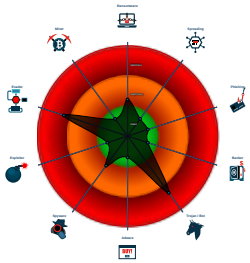


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Found potential dummy code loops (…
- Creates a DirectInput object (often fo…
- Uses 32bit PE files
- Sample file is different than original …
- Contains functionality to read the PEB
- Uses code obfuscation techniques (…
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- Zr26f1rL6r.exe (PID: 7096 cmdline: "C:\Users\user\Desktop\Zr26f1rL6r.exe" MD5: 812181DF251E06433BF2F4F6A0C0F0F4)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://atseasonals.com/GHrtt/bin_k"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.804770184.0000000002A60000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Copyright Joe Security LLC 2021

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

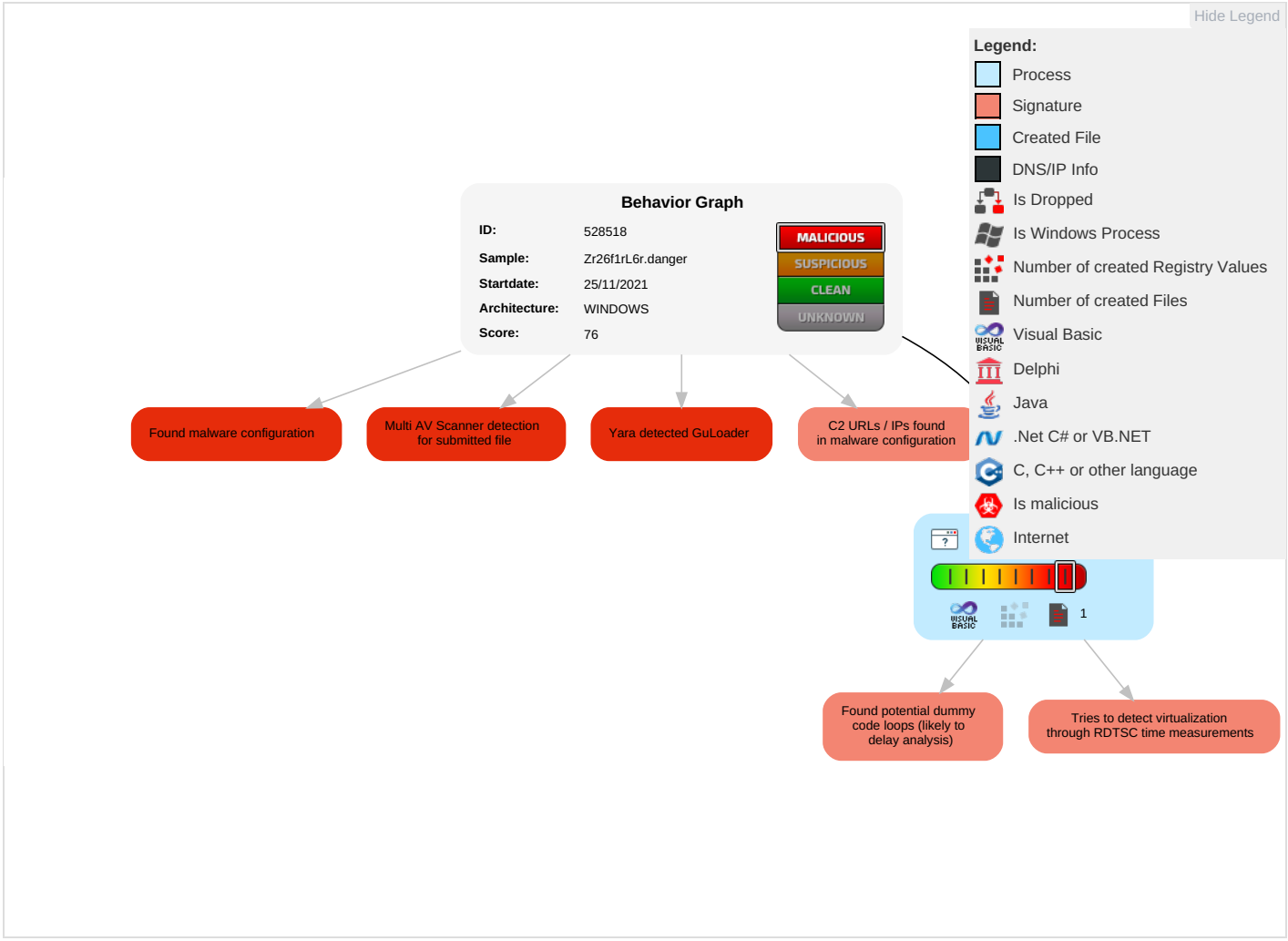
Anti Debugging:

Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Ef
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	Input Capture 1	Security Software Discovery 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Re Tr W Au
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Re W W Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Ol De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

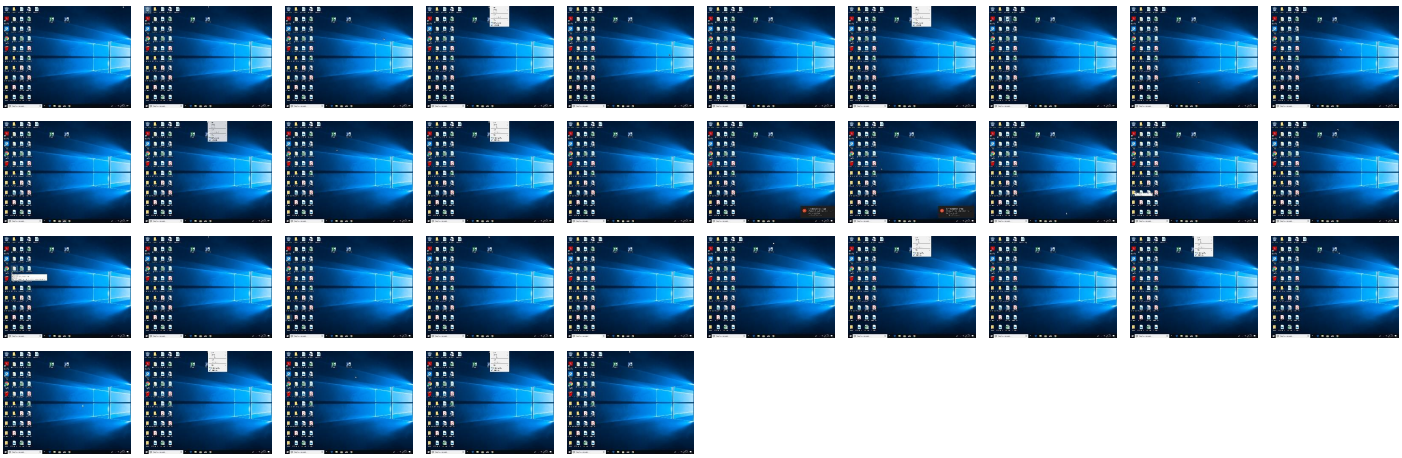
Behavior Graph



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
Zr26f1rL6r.exe	40%	Virustotal		Browse
Zr26f1rL6r.exe	20%	ReversingLabs	Win32.Trojan.GuLoader	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://atseasonals.com/GHrtt/bin_k	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://atseasonals.com/GHrtt/bin_k	true	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528518
Start date:	25.11.2021
Start time:	12:43:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Zr26f1rL6r.danger (renamed file extension from danger 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:	26
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:	mal76.troj.evad.winEXE@1/1@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 6.4% (good quality ratio 2.5%) • Quality average: 21% • Quality standard deviation: 29.7%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption
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

C:\Users\user\AppData\Local\Temp\~DFD789DA64D34966AA.TMP	
Process:	C:\Users\user\Desktop\Zr26f1rL6r.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.021204976774085
Encrypted:	false
SSDEEP:	48:rJSq2Upu8metqPrIXHimU7zdvP1vnRecR:VSKUpACLF0
MD5:	E9F7C24086FE230572BB84C262385677
SHA1:	16B4D54B227860CD7942CB26F607C2464F69B416
SHA-256:	1F1B9BB21DBBE012A4824C25111BAB849BE0E7BCED9234527701823A68C65374
SHA-512:	4F82F38C3A3D93FED9E1D0A27D1993FAA723CD2C0AD08241F1FC8C93E1DFAF47E035A94A2075B828AD12D41C6860150C3B42EE79B060912EBC44D340C8CDA4 2
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.18115352999971
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	Zr26f1rL6r.exe
File size:	144472

General

MD5:	812181df251e06433bf2f4f6a0c0f0f4
SHA1:	aa38a567ee48483d98966622fd320c791bc45871
SHA256:	4d6c910a379d00f329e55ad98a7817de0370695566443a74a9a02c85d2463a9d
SHA512:	4d34981930ed3e40572cfc761dcb78e59494d8e33f2e6615ed3e53d3e17945718d7d627abca099167e188e2e76973a550c64c54a3f6700bb6bbb7b13bbd0cf47
SSDEEP:	3072:txD6tQfQC/nHcs0lZ8+g81AYe22uQCNIJXmeL5A2m:txDQgvHyY80oQCNQm
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7b..s...s...s.....r...<!..v...E%..r...Richs.....PE..L....H.X.....0.....@

File Icon

Icon Hash:	6ce8fac8c8e46868

Static PE Info

General

Entrypoint:	0x4013b4
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x58DD4808 [Thu Mar 30 18:01:44 2017 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:	0db4e1fdede6848b7d67f260c767df5d

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=Knyste6@Eximiousne3.BRY, CN=Siphonalet4, OU=Dehumanise5, O=octocorall, L=Myomatous7, S=FAHLORE, C=TD
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 11/24/2021 4:22:16 AM 11/24/2022 4:22:16 AM
Subject Chain	• E=Knyste6@Eximiousne3.BRY, CN=Siphonalet4, OU=Dehumanise5, O=octocorall, L=Myomatous7, S=FAHLORE, C=TD
Version:	3
Thumbprint MD5:	3EA4D95D319B3BCDDF3A916A0A7F25DF
Thumbprint SHA-1:	827D80430EC06C8058A205E7E710FFF3EB2A03DE
Thumbprint SHA-256:	7824D156B89CF1BF25F923BECB9DCE0EF3F49C821D270075A626DE65497E77AD
Serial:	00

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1e6c0	0x1f000	False	0.523012222782	data	6.34448502446	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x20000	0x1a40	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0xf77	0x1000	False	0.367431640625	data	4.13632936066	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Zr26f1rL6r.exe PID: 7096 Parent PID: 5300

General

Start time:	12:44:33
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\Zr26f1rL6r.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Zr26f1rL6r.exe"
Imagebase:	0x400000
File size:	144472 bytes
MD5 hash:	812181DF251E06433BF2F4F6A0C0F0F4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.804770184.0000000002A60000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities | Show Windows behavior

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021