

JoeSandbox Cloud BASIC



ID: 458794

Sample Name: pRcHGIVekw

Cookbook: default.jbs

Time: 18:49:29

Date: 03/08/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report pRcHGIVekw	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: GuLoader	3
Yara Overview	3
Memory Dumps	3
Sigma Overview	3
Jbx Signature Overview	3
AV Detection:	4
Networking:	4
Data Obfuscation:	4
Malware Analysis System Evasion:	4
Anti Debugging:	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	7
Contacted Domains	7
Contacted URLs	7
Contacted IPs	7
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	8
Static PE Info	9
General	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	9
Imports	9
Version Infos	9
Possible Origin	9
Network Behavior	9
Code Manipulations	9
Statistics	10
System Behavior	10
Analysis Process: pRcHGIVekw.exe PID: 5816 Parent PID: 5636	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

Windows Analysis Report pRcHGIVekw

Overview

General Information

Sample Name:	pRcHGIVekw (renamed file extension from none to exe)
Analysis ID:	458794
MD5:	d2cb32f7c7f384b..
SHA1:	355acb5af5caaeb..
SHA256:	2bd846bdda945d..
Tags:	32 exe
Infos:	
Most interesting Screenshot:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

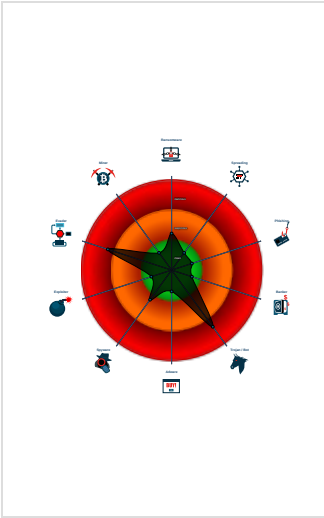
GuLoader

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm...
- Yara detected GuLoader
- C2 URLs / IPs found in malware con...
- Found potential dummy code loops (...)
- Machine Learning detection for samp...
- Tries to detect virtualization through...
- Abnormal high CPU Usage
- Contains functionality for execution ...
- Contains functionality to call native f...
- Contains functionality to read the PEB
- Creates a DirectInput object (often fo...

Classification



Process Tree

- System is w10x64
- pRcHGIVekw.exe (PID: 5816 cmdline: 'C:\Users\user\Desktop\pRcHGIVekw.exe' MD5: D2CB32F7C7F384B4BAA8DD13D6B5BBAB)
- cleanup

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL ": "http://101.99.94.119/WEALTH_fkHgIQyCX0188.binkw"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.730158990.000000000074 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

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:

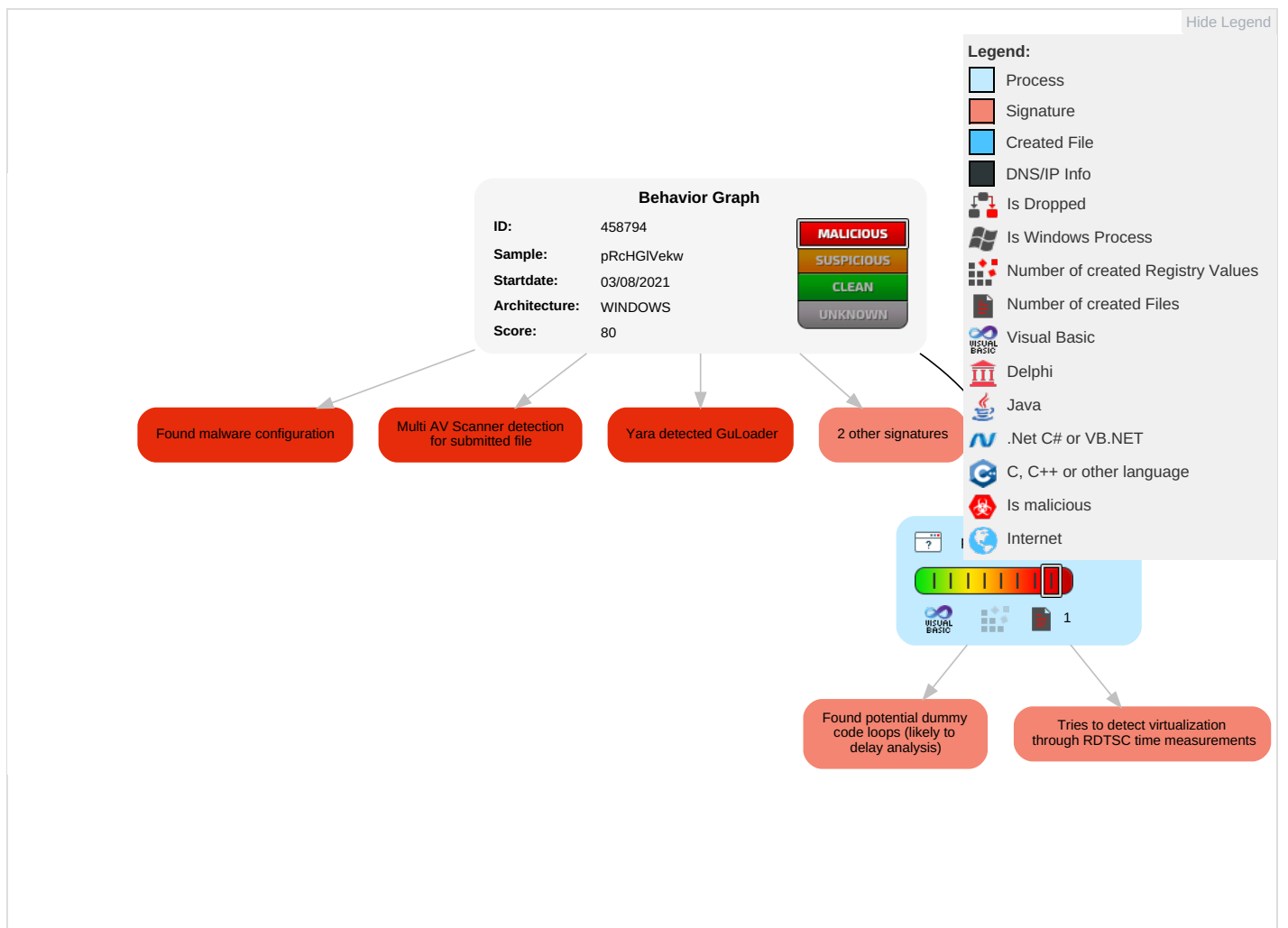


Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Recovery
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	Recovery
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Software Packing 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	Recovery
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 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	Recovery
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	System Information Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Recovery

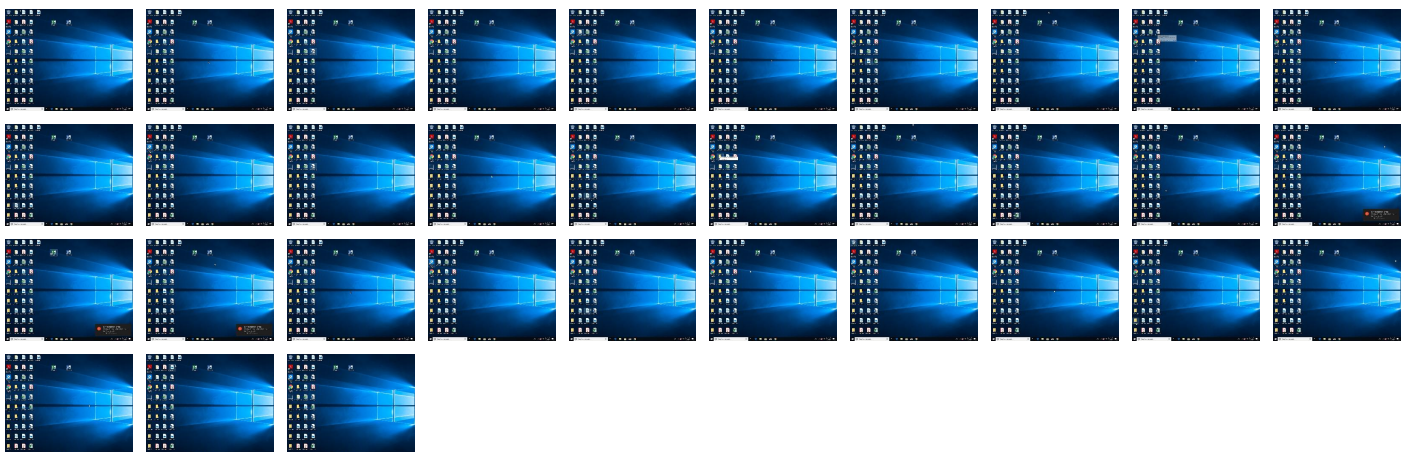
Behavior Graph



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
pRcHGIVekw.exe	32%	Virustotal		Browse
pRcHGIVekw.exe	17%	ReversingLabs	Win32.Trojan.Fragtor	
pRcHGIVekw.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://101.99.94.119/WEALTH_fkWglQyCXO188.binkw	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://101.99.94.119/WEALTH_fkWglQyCXO188.binkw	true	<ul style="list-style-type: none">Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458794
Start date:	03.08.2021
Start time:	18:49:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	pRcHGIvekw (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:	30
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:	<ul style="list-style-type: none">HCA enabledEGA enabledHDC enabledAMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">Successful, ratio: 23.2% (good quality ratio 6%)Quality average: 12.9%Quality standard deviation: 24.4%
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none">Adjust boot timeEnable AMSIOverride 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

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.662154130313104
TrID:	<ul style="list-style-type: none">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:	pRcHGIvekw.exe
File size:	114688
MD5:	d2cb32f7c7f384b4baa8dd13d6b5bbab
SHA1:	355acb5af5caaeb59fd7c9e0a54b501c24d47919
SHA256:	2bd846bdda945dc48a21c9bda1497feb9e67df8cfb024cc8669041490c7c9a90
SHA512:	0d620354c0c94604a37277c2029832d4aff586918821edc58f94fd0ab02817f7e9e48a4b53f221b0bb9617e9f5f349b0494e678694ac1d9053bb30f6b3766913
SSDEEP:	1536:MfPqE74qa95aAmpcPTDo9flG6kPl9NlcGCp9bZYuQmiPY/peaja9QNE7YP:Mf5sR94AWc7Do3G60IM49eM/ptO9QeE
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L...IG.T.....@.....D.....P....@.....

File Icon



Icon Hash:	6a4a266a2a3a2a2a
------------	------------------

Static PE Info

General

Entrypoint:	0x401144
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x54A54749 [Thu Jan 1 13:10:33 2015 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:	5565993a5a9f2bfb76f28ab304be6bc1

Entrypoint Preview

Data Directories

Sections


Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x13dd4	0x14000	False	0.651550292969	data	7.08042704515	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0x115c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0x5b8e	0x6000	False	0.545694986979	data	6.03858270221	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
Chinese	Taiwan	

Network Behavior

No network behavior found

Code Manipulations

Code Manipulations

Statistics

System Behavior

Analysis Process: pRcHGIVekw.exe PID: 5816 Parent PID: 5636

General

Start time:	18:50:17
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\pRcHGIVekw.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\pRcHGIVekw.exe'
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	D2CB32F7C7F384B4BAA8DD13D6B5BBAB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none">Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.730158990.0000000000740000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis