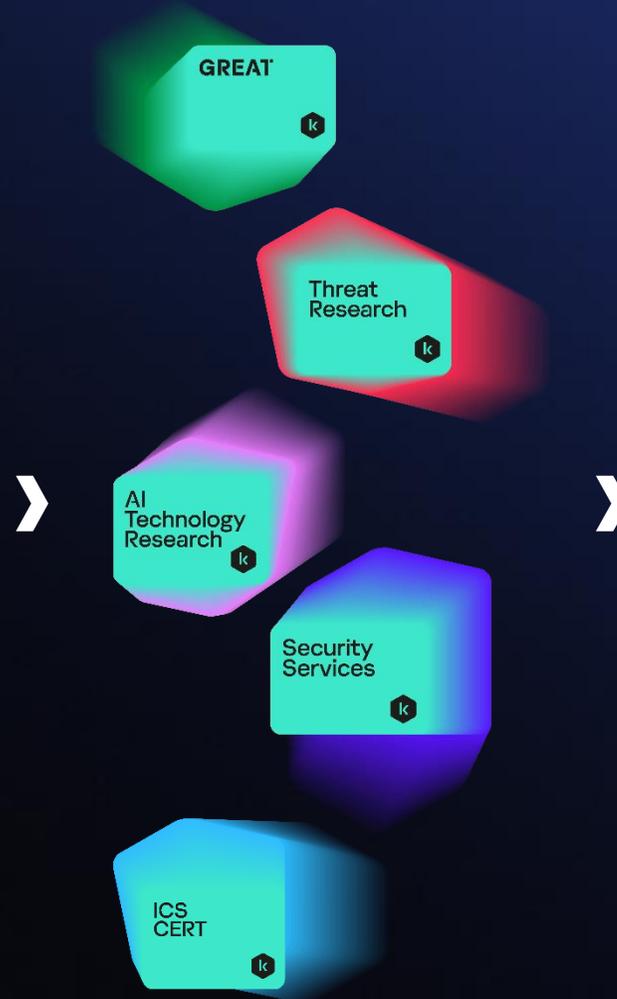
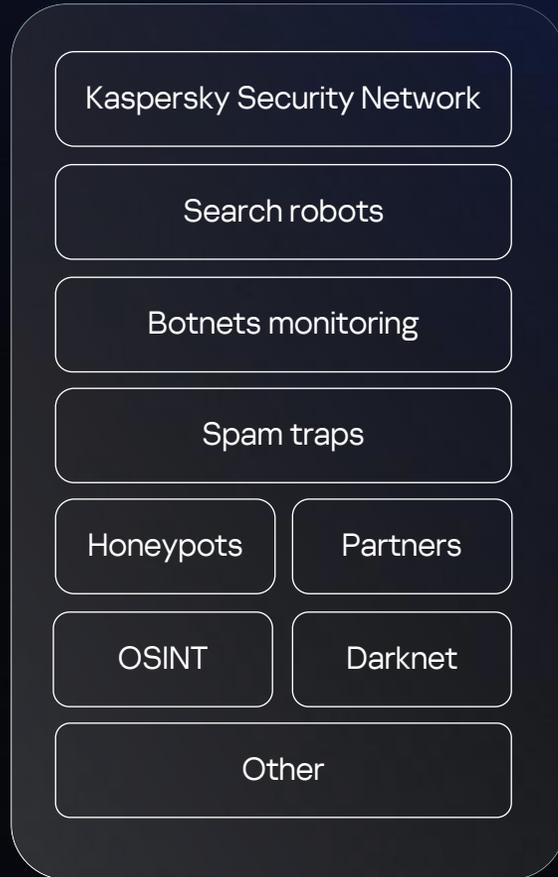




How Threat Actors Deceive Researchers via Unpopular Software

Georgy Kucherin
Kaspersky

About what I do



Deception how it is



Attacker

**It's a real
machine!**

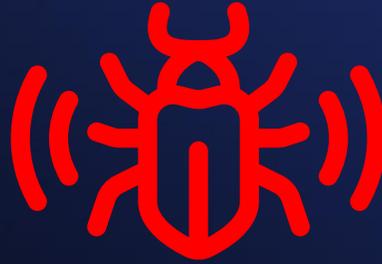


Honeypot

Deception how it is

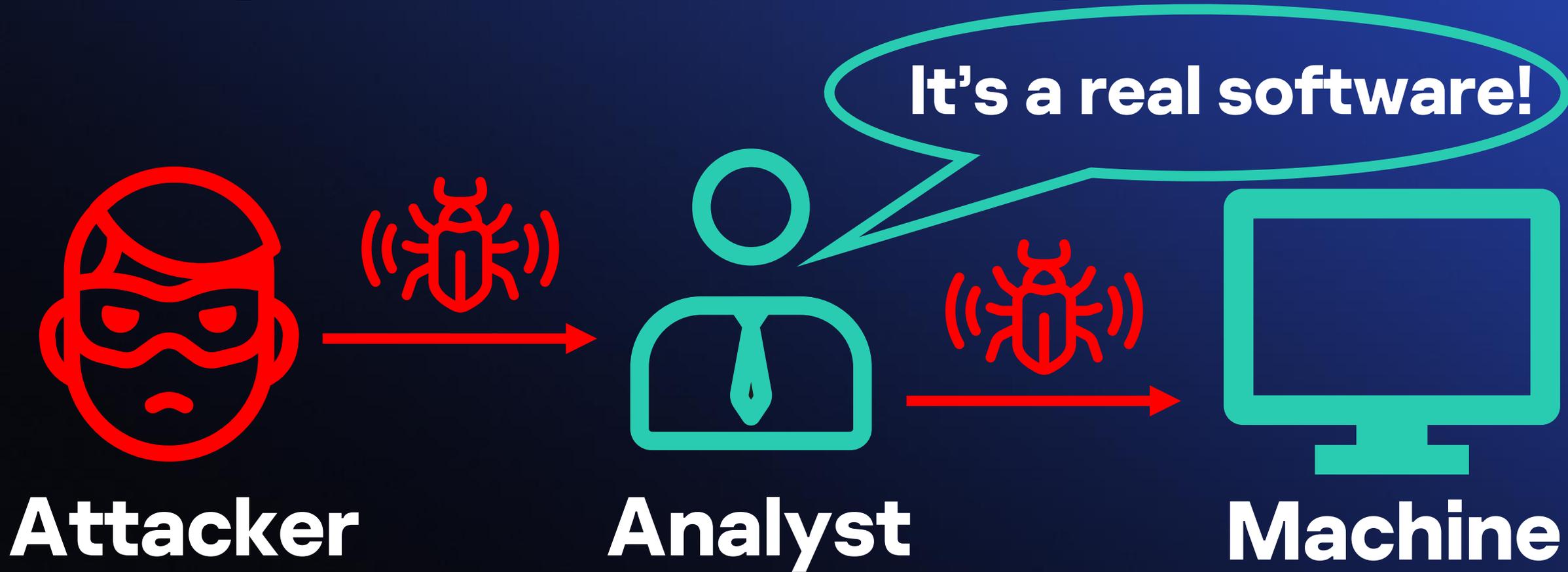


Attacker



Honeypot

Deception the other way



Malware visible in plain sight

**You see the
malware on the
filesystem.**

**You see the
malware in
memory.**

Still, you don't realize it's malware.

The case for today

You are a network analyst.

Your job is to inspect suspicious domains and check if they are related to malware.

Domain name from SIEM: eventuallogic[.]com

Objectives for today:

- **Is the domain malicious?**
- **If so, what is the infection chain?**
- **If so, what is the malware type?**

Checking the domain

eventuallogic.com	1 / 94	104.21.48.1	104.21.16.1	104.21.112.1	...
www.eventuallogic.com	1 / 94	104.21.32.1	104.21.48.1	104.21.16.1	...

URLs (2) ⓘ

Scanned	Detections	Status	URL
2025-05-02	1 / 97	404	http://www.eventuallogic.com/
2025-05-02	1 / 97	404	http://eventuallogic.com/

Downloaded Files (1) ⓘ

Scanned	Detections	Type	Name
2025-05-20	0 / 63	HTML).

**Not many clues. 1 detection out of 97
may be a false positive**

Checking the domain

Overview

General Information

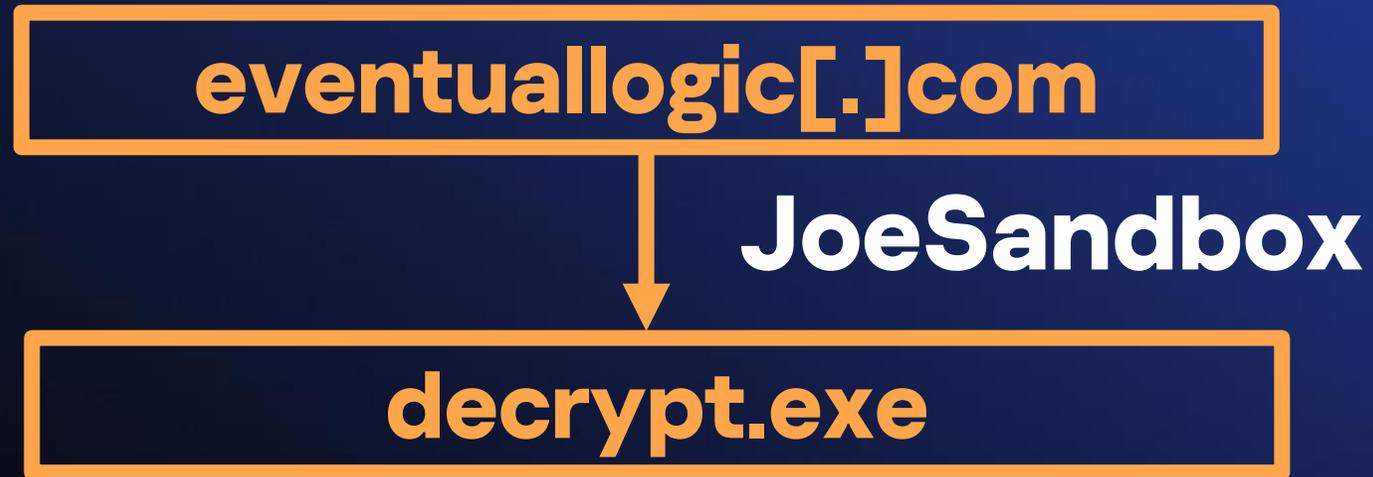
Sample name:	decrypt.exe 
Analysis ID:	1582909 
MD5:	0a08cc36... 
SHA1:	580ccc43... 
SHA256:	db433f67... 
Infos:	  

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

ponding DNS lookups

DNS traffic detected: DNS query: www.eventuallogic.com

Relations graph



Checking out decrypt.exe



Community Score

! 5/72 security vendors flagged this file as malicious

🔔 Follow ▾ 🔄 Reanalyze 📄 Download ▾ ≈ Similar ▾ More ▾

db433f673eeacd8e905cca9ef3b283d30c466ab6...
C:\Windows\ceuzqfydmn.exe

Size: 16.33 MB | Last Analysis Date: 1 day ago

EXE

peexe checks-user-input idle signed overlay

Compressed Parents (2) ⓘ 📄

Scanned	Detections	Type	Name
2025-05-16	0 / 63	ZIP	decrypt.zip

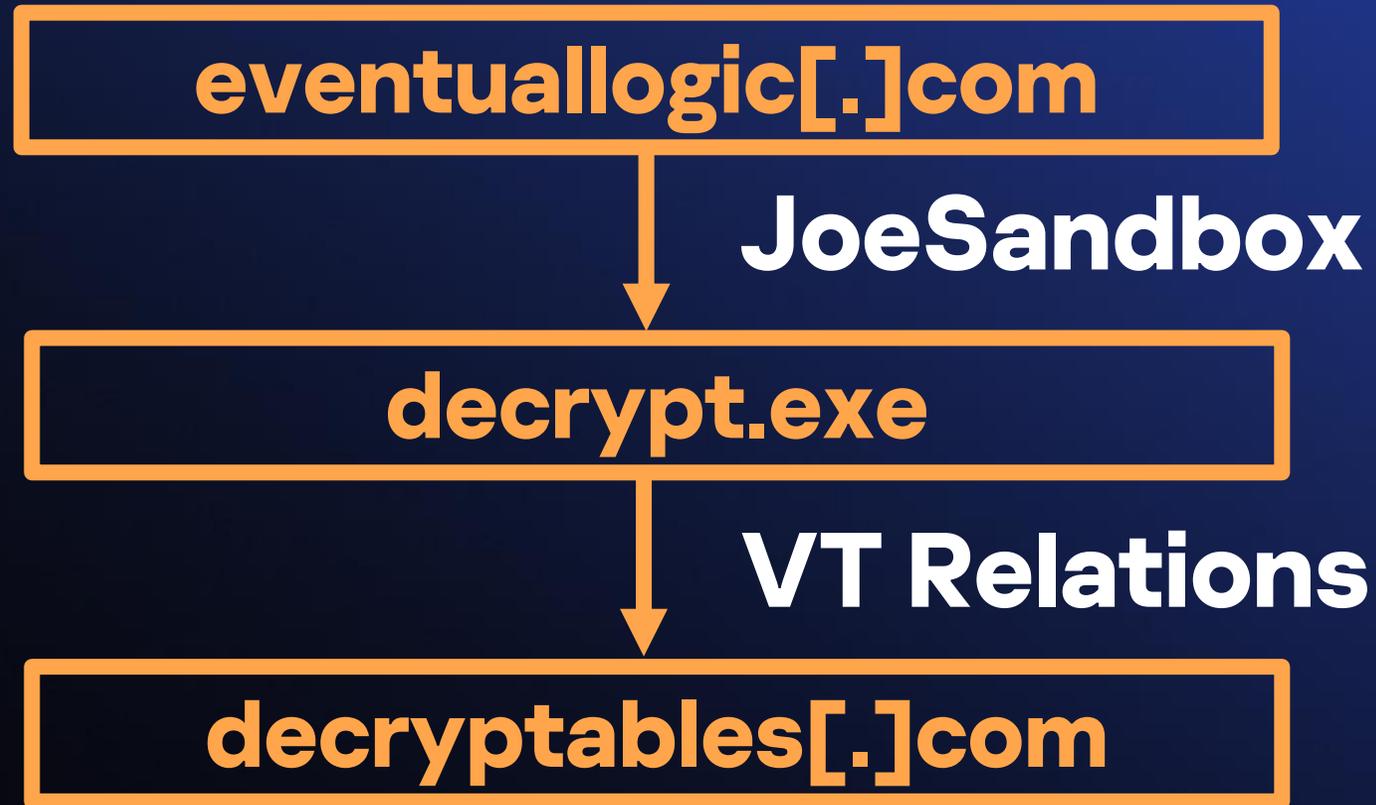
Was found inside a decrypt.zip file

Checking out decrypt.zip

ITW Urls (2) ⓘ				
Scanned	Detections	Status	URL	
2025-02-13	1 / 96	403	http://decryptables.com/ decrypt.zip	
2025-05-20	2 / 97	403	https://decrypta- bles.com/decrypt.zip	

**decrypt.zip was downloaded from
decryptables[.]com**

Relations graph



Checking out decryptables[.]com

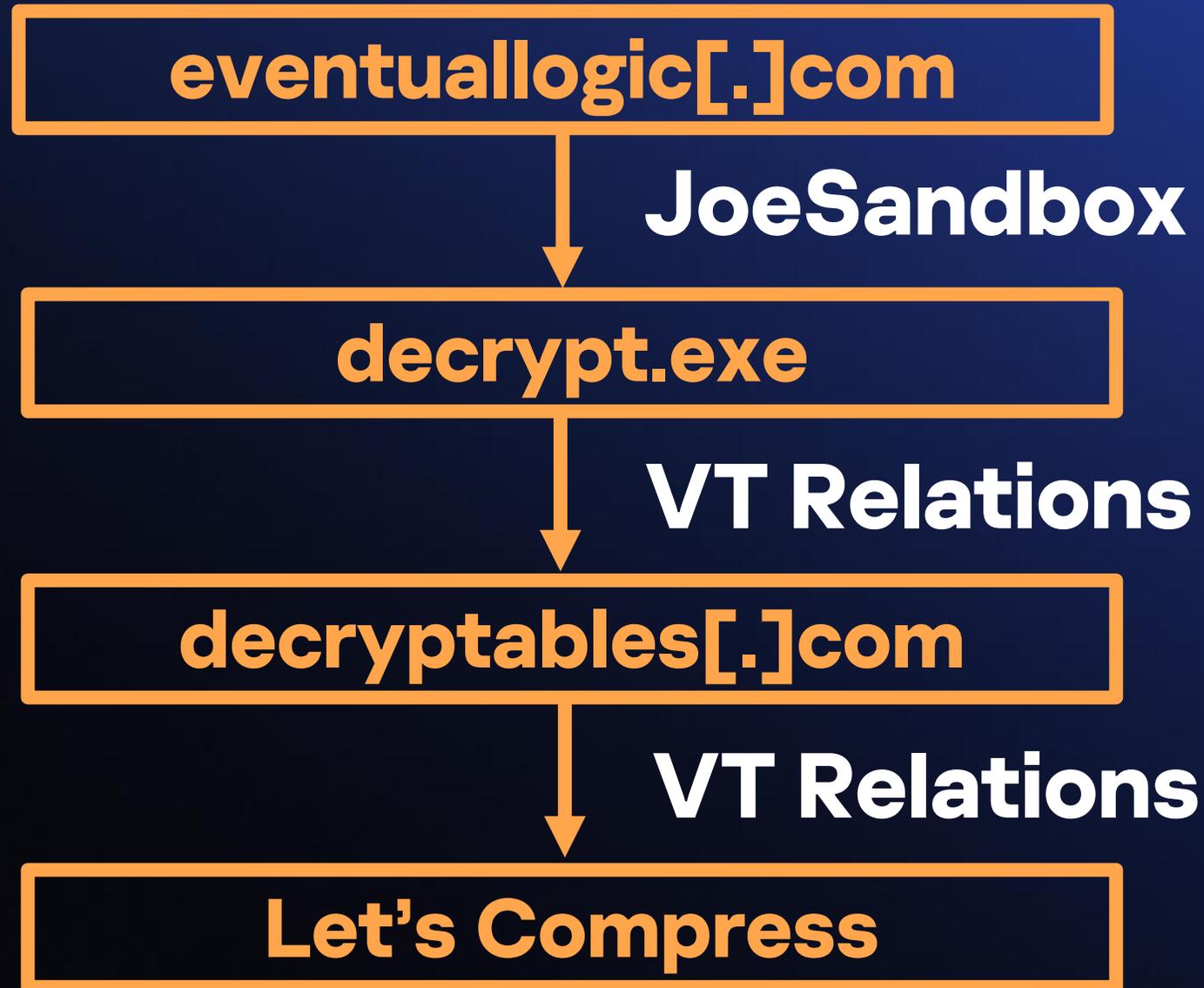
Communicating Files (10/11)



Name	Detections	Type	Communicated date
<p>0a6deb9496cf8fb61a78dd5f576296a8a15e54493f4c1ef9fda0d7d292c43d9a</p> <p> <i>No meaningful names</i></p> <p>peexe signed overlay detect-debug-environment long-sleeps calls-wmi 64bits</p>	10 / 73	Win32 EXE	2024-09-03 19:51:23 UTC
<p>2255d95429cf568bd73483ff86ed7526cfdcb6759f313fe7743de128ac53094e</p> <p> Let's Compress.exe</p> <p>peexe overlay long-sleeps calls-wmi signed checks-usb-bus detect-debug-environment</p>	6 / 73	Win32 EXE	2024-12-06 18:16:41 UTC

**decryptables[.]com communicates
With “Let’s Compress.exe”**

Relations graph



Checking out Let's Compress



⚠️ 6/72 security vendors flagged this file as malicious

🔔 Follow ▾

🔄 Reanalyze

⬇️ Download ▾

🏠 Similar ▾

⋮ More ▾

2255d95429cf568bd73483ff86ed75...

Size

14.65 MB

Last Analysis Date

2 months ago



Let's Compress.exe

Arctic Wolf

⚠️ Unsafe

K7AntiVirus

⚠️ Riskware (00584baa1)

K7GW

⚠️ Riskware (00584baa1)

Kaspersky

⚠️ Trojan.Win32.Agent.xbuujw

Sophos

⚠️ Utility Access (PUA)

Zillya

⚠️ Downloader.Banload.Win32.103708

6 detections, some of them related to PUAs

Malware vs. PUA

Malware

Software that clearly conducts malicious actions (e.g. backdoors, ransomware)

PUA

Software that is not malicious by itself but is still unwanted (e.g. adware)

Checking out Let's Compress

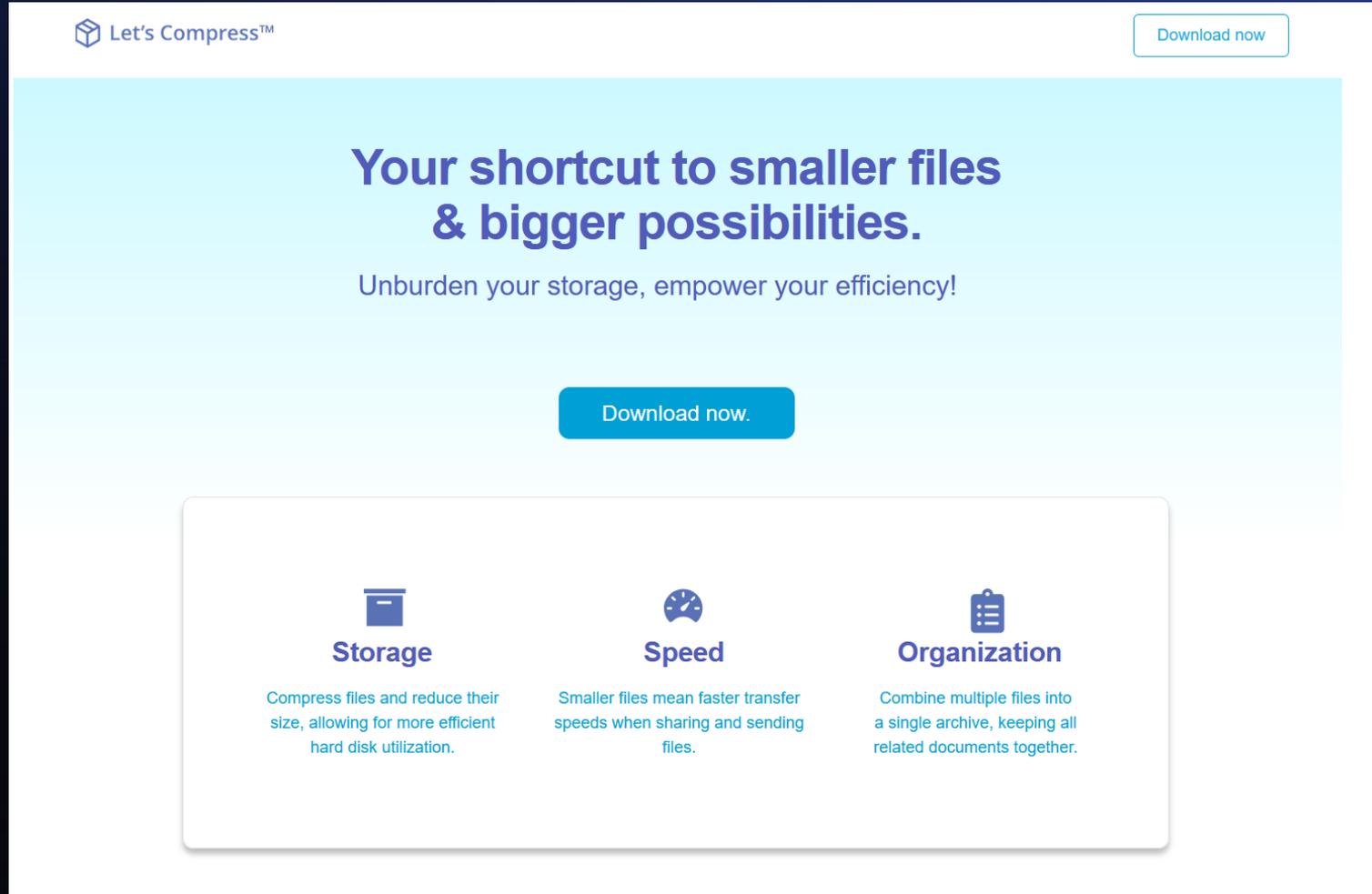
Signers

— UTILITY ACCESS (SMC-PRIVATE) LIMITED

Name	UTILITY ACCESS (SMC-PRIVATE) LIMITED
Issuer	GlobalSign GCC R45 EV CodeSigning CA 2020
Valid From	12:37 PM 09/26/2024
Valid To	12:37 PM 09/27/2025
Valid Usage	Code Signing
Algorithm	sha256RSA
Thumbprint	24097FB790D82FE390B9DCB3456675F96CEF4B2B
Serial Number	46 BC 9E 64 8B 50 DD B3 39 0A 8A 8A

This file is signed!

Checking out Let's Compress



The screenshot shows the landing page for 'Let's Compress'. At the top left is the logo 'Let's Compress™' and at the top right is a 'Download now' button. The main headline reads 'Your shortcut to smaller files & bigger possibilities.' followed by the sub-headline 'Unburden your storage, empower your efficiency!'. A large blue 'Download now.' button is centered below the text. The bottom section features three columns: 'Storage' with a folder icon and text 'Compress files and reduce their size, allowing for more efficient hard disk utilization.', 'Speed' with a speedometer icon and text 'Smaller files mean faster transfer speeds when sharing and sending files.', and 'Organization' with a clipboard icon and text 'Combine multiple files into a single archive, keeping all related documents together.'

Let's Compress™ [Download now](#)

Your shortcut to smaller files & bigger possibilities.

Unburden your storage, empower your efficiency!

[Download now.](#)



Storage

Compress files and reduce their size, allowing for more efficient hard disk utilization.



Speed

Smaller files mean faster transfer speeds when sharing and sending files.



Organization

Combine multiple files into a single archive, keeping all related documents together.

It's a real tool!

Checking out Let's Compress



Domain Information

Domain: letscompress.com

Registered On: 2024-05-23

23 May 2024

Expires On: 2026-05-23

Updated On: 2025-05-08

web.archive.org/web/20240729150650/https://www.letscompress.com/#expand

https://www.letscompress.com/ Go

25 captures
17 Jan 2020 - 6 Sep 2024

MAR 2023 JUL 29 2024

Let's Compress™

29 July 2024

Download now

**Your shortcut to smaller files
& bigger possibilities.**

Unburden your storage, empower your efficiency!

A discussion on X / Twitter



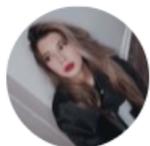
Aura

@SecurityAura

30 December 2024 ...

There's something going on with this (caught earlier this week by our SOC). I don't know what that is but it looks like it's masquerading Let's Compress?

Doesn't look legitimate at all. Gotta jump for now but I'll dig more into this later. cc [@RussianPanda9xx](#)



RussianPanda



@RussianPanda9xx

Suivre



ahh, it's a PUA, all it does is just archiving the files you fetch to it, I think.

[Traduire le post](#)

A discussion on X / Twitter



Aura @SecurityAura · 29 déc. 2024



I can see that at some point it uses 7z.exe to decrypt a password protected (PW is 123456 IIRC) 7z named decrypt.7z.

It's all bits and pieces since I was in a hurry. But that initial command I showed is encoded and launched through PS. There's a lot of suspicious stuff here 😂



RussianPanda 🐼 🇺🇦 🟡 @RussianPanda9xx · 29 déc. 2024



If you look for the signature on VT, they have another PUA too (signature:"UTILITY ACCESS (SMC-PRIVATE) LIMITED") - Flip Player :D
[virustotal.com/gui/file/edbe2...](https://www.virustotal.com/gui/file/edbe2...)

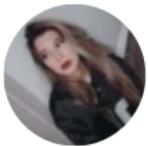


A discussion on X / Twitter



Aura @SecurityAura · 30 déc. 2024

I went down the OSINT route and found that Utility Access is just one of many companies that are owned/directed by the same person. All seems to be in the customer support, web design, digital marketing field. It probably goes deeper than that but yeah, PUA it would be 😂

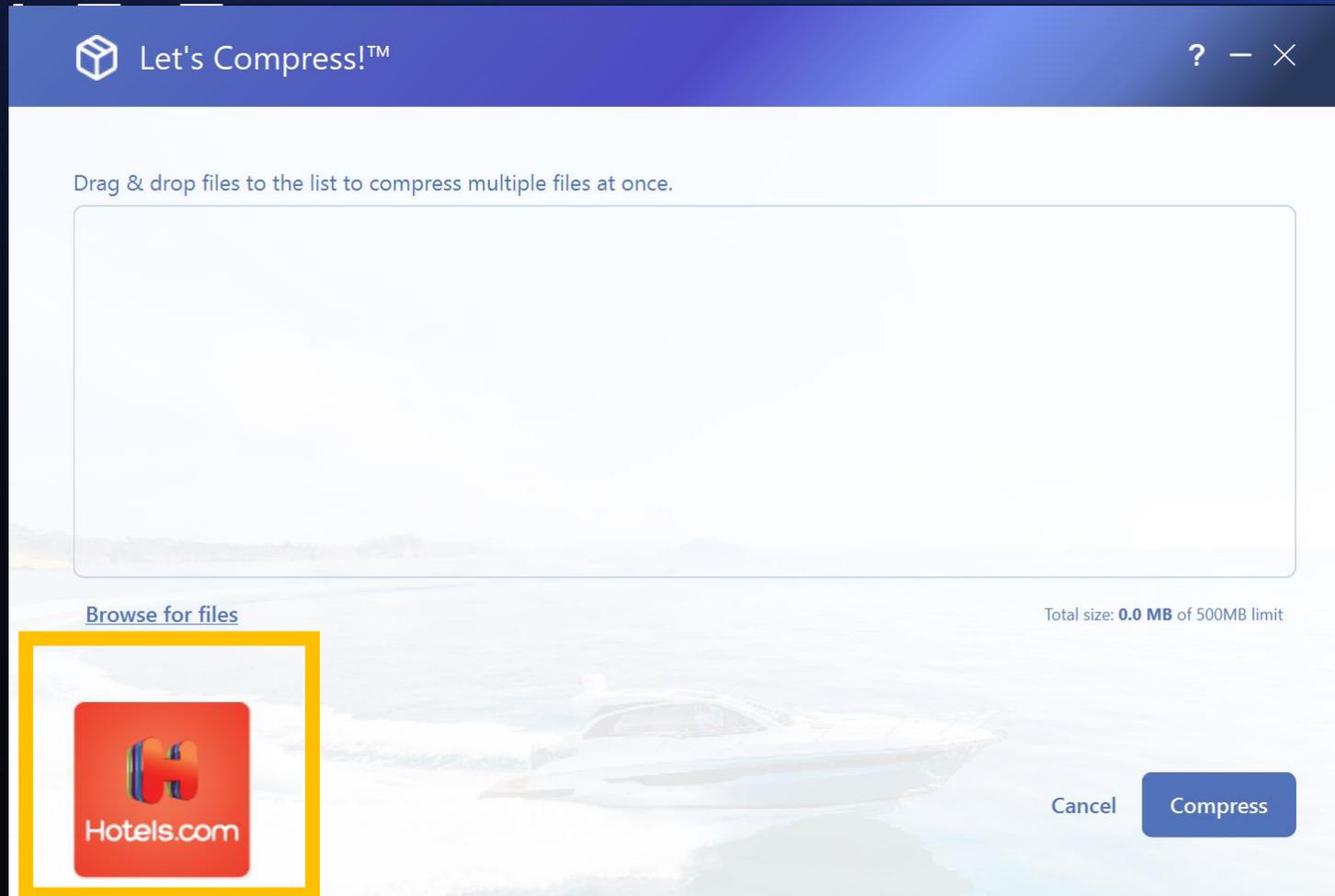


RussianPanda 🐼 🇺🇦 🟡 @RussianPanda9xx · 30 déc. 2024

Nice find as always ❤️
You should tag me more 😊



Software window



Sign of a PUA

Is Let's Encrypt a PUA or a malware? What do you think?

It's a PUA, we
start examining
other clues

It's malware,
we continue
looking at it

Communicating Files (10/11)				
Name	Detections	Type	Communicated date	
0a6deb9496cf8fb61a78dd5f576296a8a15e54493f4...	10 / 73	Win32 EXE	2024-09-03 19:51:23 UTC	
<i>No meaningful names</i>				
peexe signed overlay detect-debug-environment ...				

Relations graph

eventuallogic[.]com

decrypt.exe

decryptables[.]com

Let's Compress

```
graph BT; A[Let's Compress] -.-> B[decryptables[.]com]; B --> C[decrypt.exe]; C --> D[eventuallogic[.]com]
```

Folder contents



iconengines



imageformats



platforms



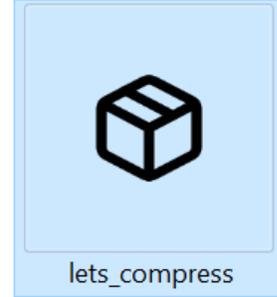
styles



translations



util



lets_compress



msvc140.dll



msvc140_1.dll



msvc140_2.dll



Qt6Core.dll



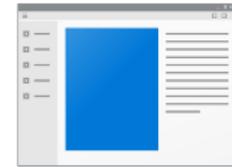
Qt6Gui.dll



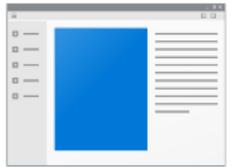
Qt6Svg.dll



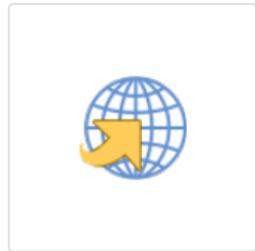
Qt6Widgets.dll



upd



update



updater



updater



vcruntime140.dll



vcruntime140_1.dll

Let's scan them for the domain name we saw!

Folder contents

```
rule decryptables {
strings:
    $s1 = "decryptables.com" ascii wide
condition:
    all of them
}
```

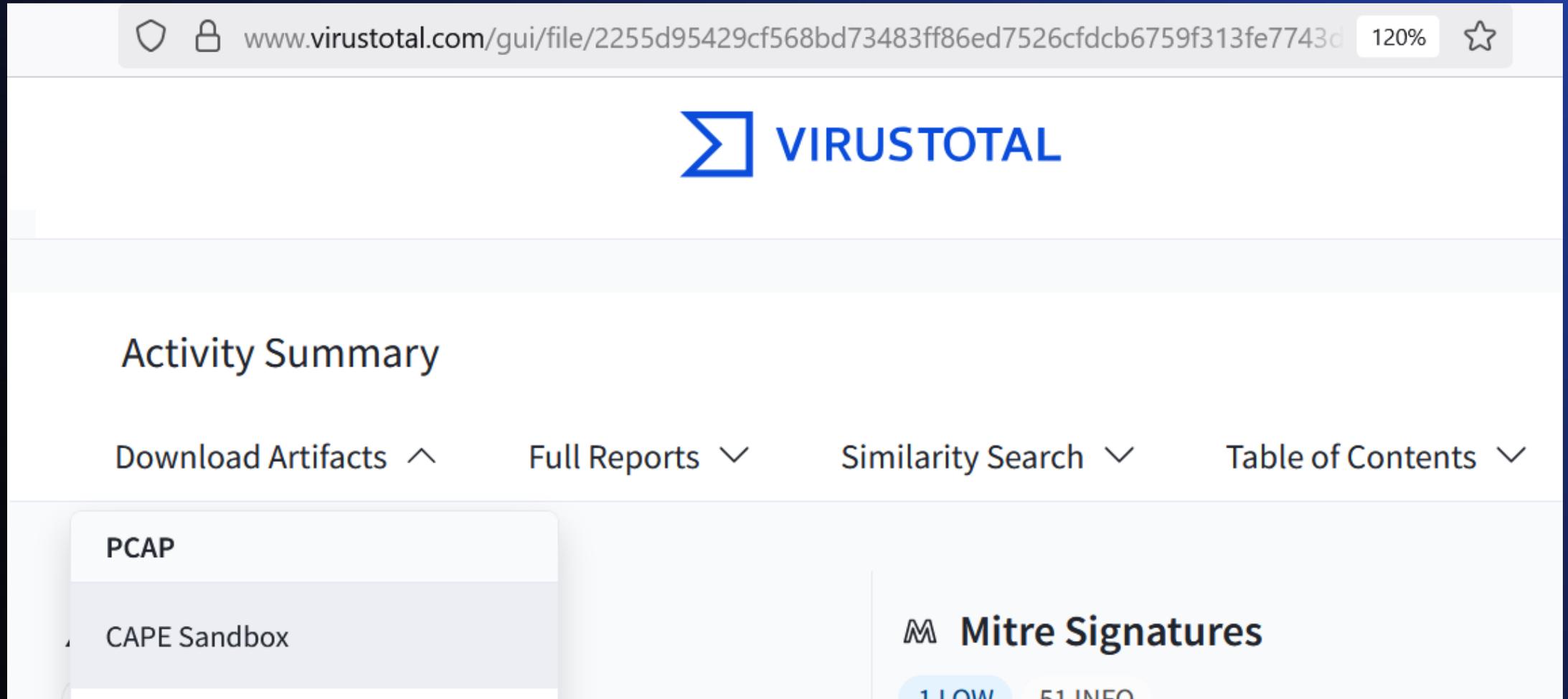
Folder contents

```
rule decryptables {  
  strings:  
    $s1 = "decryptables.com" ascii wide  
  condition:  
    all of them  
}
```

```
C:\Users\user\Desktop>yara64.exe decryptables.yara "C:\Users\user\AppData\Roaming\Let's Compress"  
decryptables C:\Users\user\AppData\Roaming\Let's Compress\update.exe
```

Found an executable named "update.exe"

Getting the PCAPs



The screenshot shows the VirusTotal web interface. At the top, the browser address bar displays the URL: www.virustotal.com/gui/file/2255d95429cf568bd73483ff86ed7526cfdcb6759f313fe7743d. The page features the VirusTotal logo and a navigation bar with the following options: [Download Artifacts](#) (with an upward arrow), [Full Reports](#) (with a downward arrow), [Similarity Search](#) (with a downward arrow), and [Table of Contents](#) (with a downward arrow). A dropdown menu is open under 'Download Artifacts', listing 'PCAP' and 'CAPE Sandbox'. To the right, the 'Mitre Signatures' section is partially visible, showing a '1 LOW' indicator and '51 INFO'.

Download sandbox PCAP from VT

Traffic analysis

```
256 GET /letscompress_finish_install HTTP/1.1
581 HTTP/1.1 200 OK
239 GET /update.txt HTTP/1.1
1098 HTTP/1.1 200 OK (text/html)
244 GET /starting_script HTTP/1.1
581 HTTP/1.1 200 OK
245 GET /script_succeeded HTTP/1.1
206 GET /decrypt.zip HTTP/1.1
581 HTTP/1.1 200 OK
```

decrypt.zip in sight

Traffic analysis

[Update]

Name = Let's Compress

NoGUICommandLineSwitch = /exenoui /qn

ProductVersion = 1.4.2.0

URL = https://compressing-lets-3.com/lets_compress_390.exe

Size = 15338144

CommandLine = /qn

ServerFileName = Let's Compress.exe

Flags = NoCache|Advertises

RegistryKey = HKUD\Software\Let's Compress\Let's Compress\Ve

rsion

Version = 1.4.2.0

AdditionalAttributes=c=dXBkYXR1LmV4ZQ==

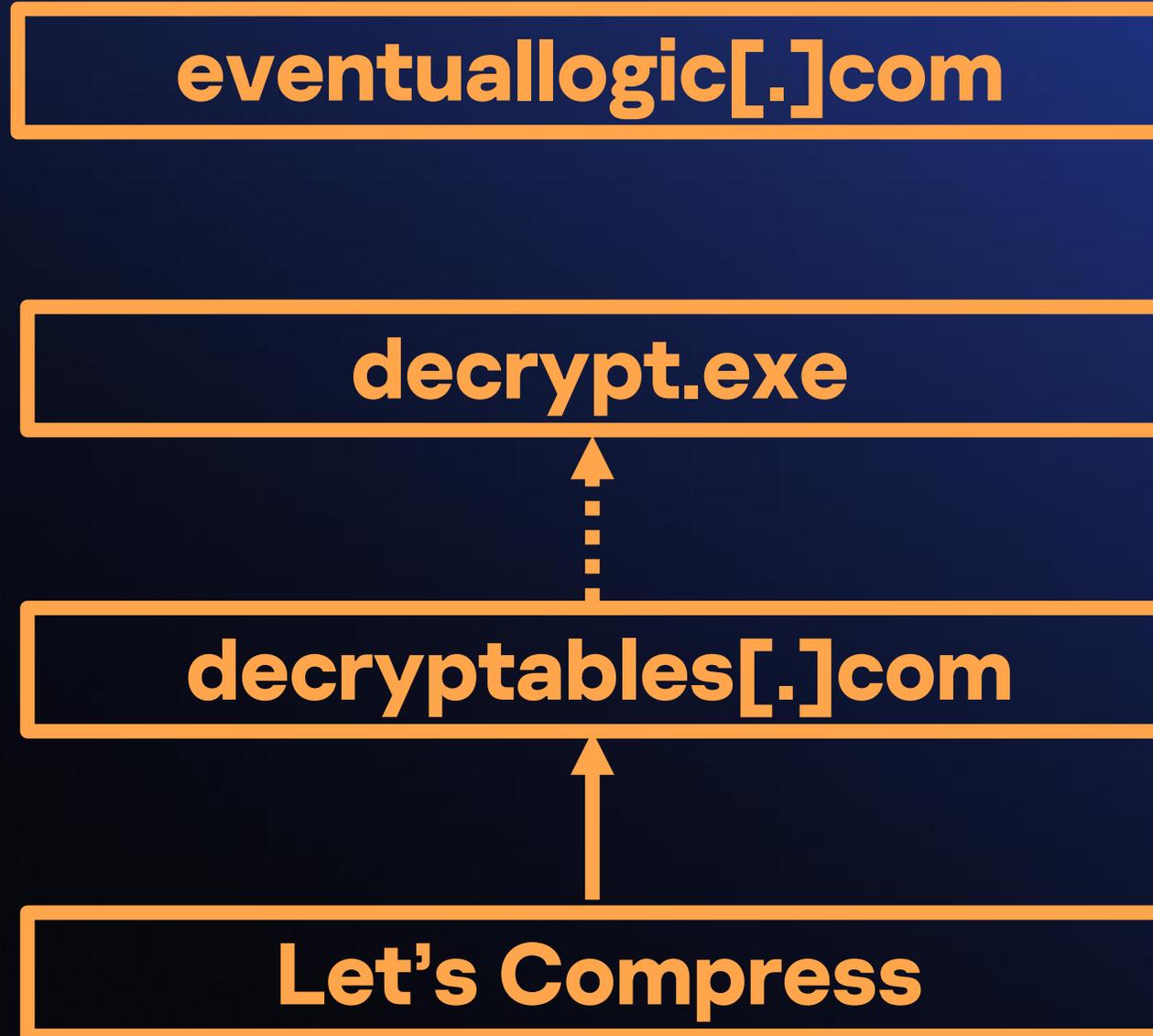
Find an anomaly here

Traffic analysis

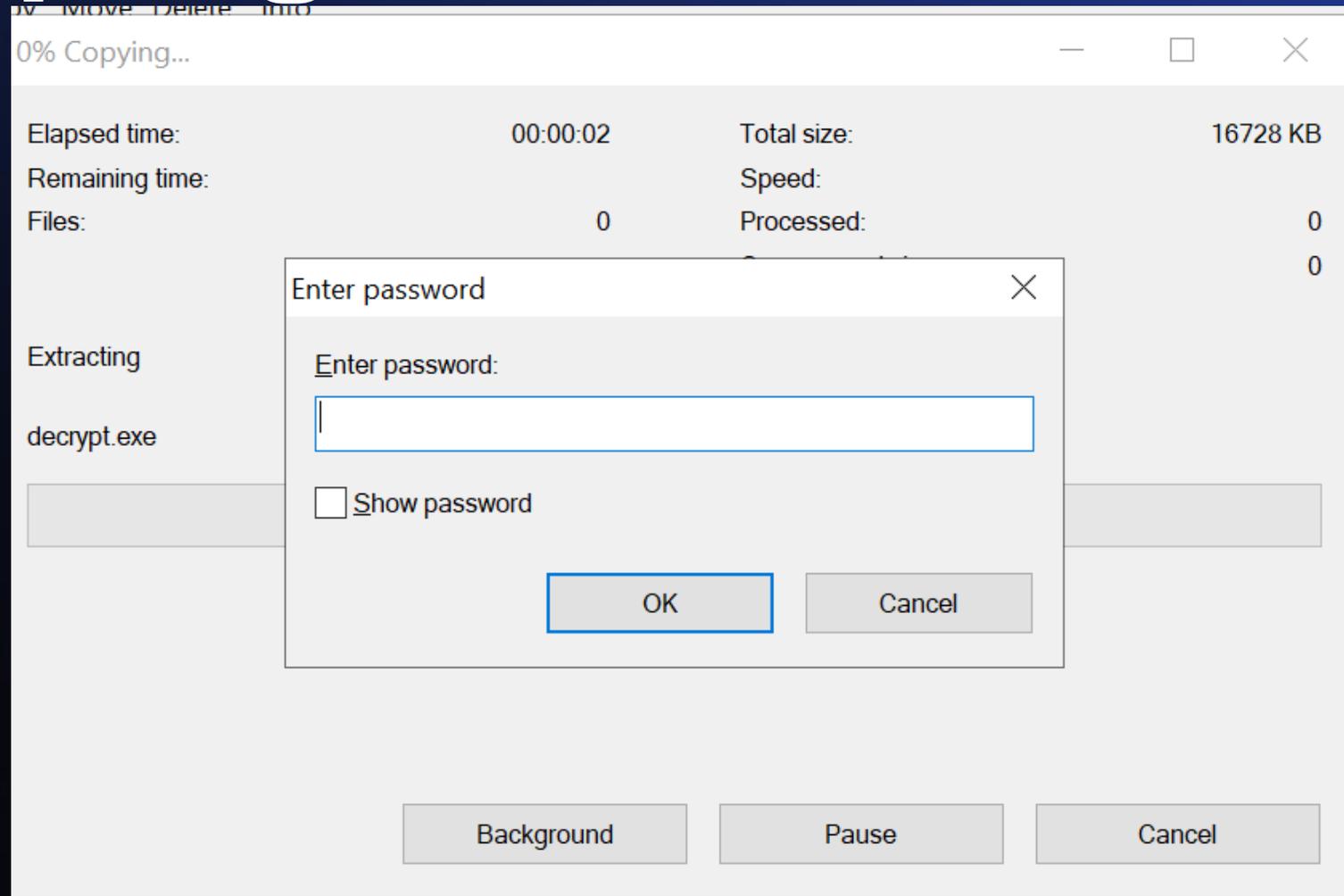
```
[Update]
Name = Let's Compress
NoGUICommandLineSwitch = /exenoui /qn
ProductVersion = 1.4.2.0
URL = https://compressing-lets-3.com/lets_compress_390.exe
Size = 15338144
CommandLine = /qn
ServerFileName = Let's Compress.exe
Flags = NoCache|Advertises
RegistryKey = HKUD\Software\Let's Compress\Let's Compress\Ve
rsion
Version = 1.4.2.0
AdditionalAttributes=c=dXBkYXR1LmV4ZQ==
```

Base64("update.exe")

Relations graph

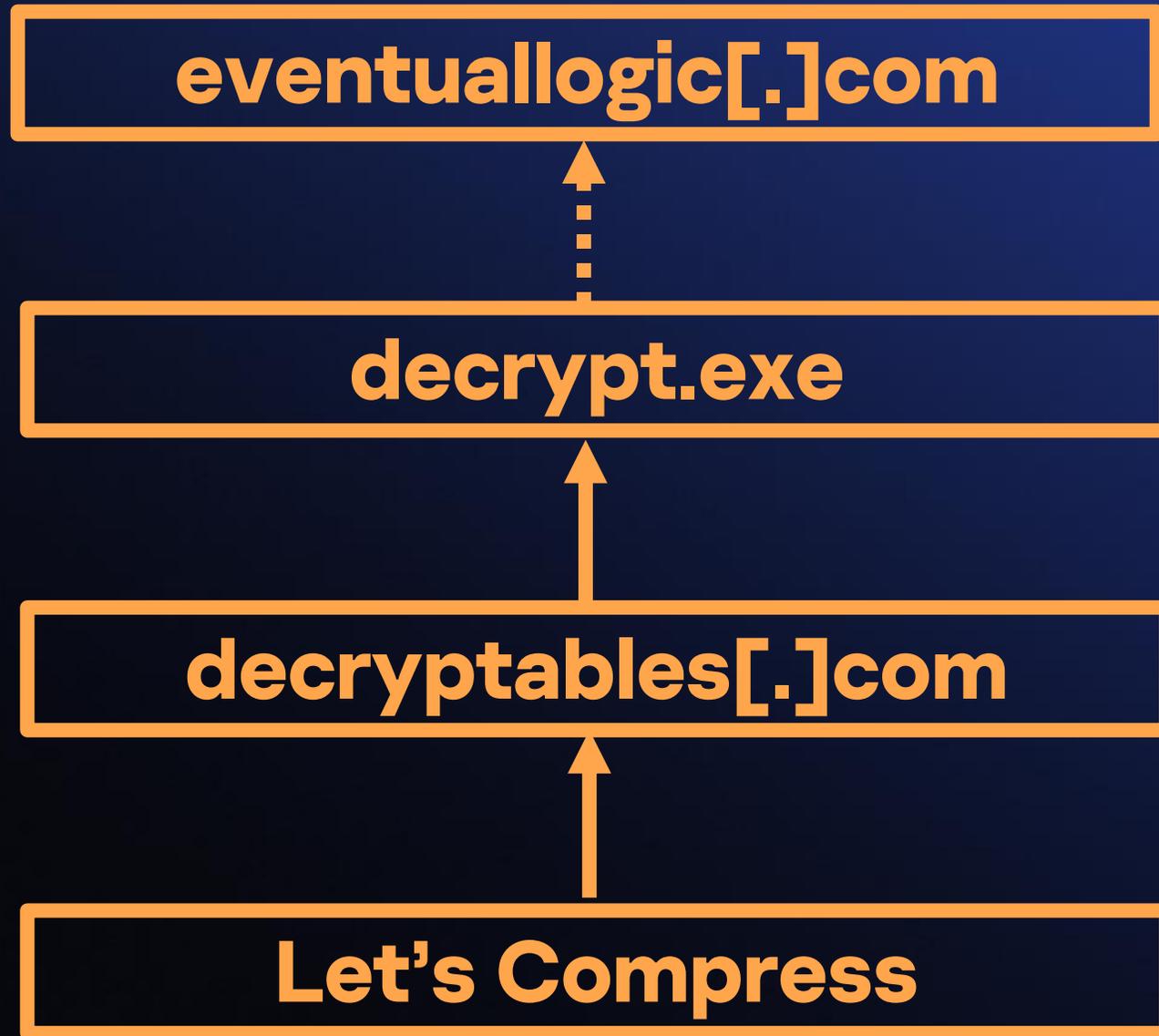


Decrypting the archive

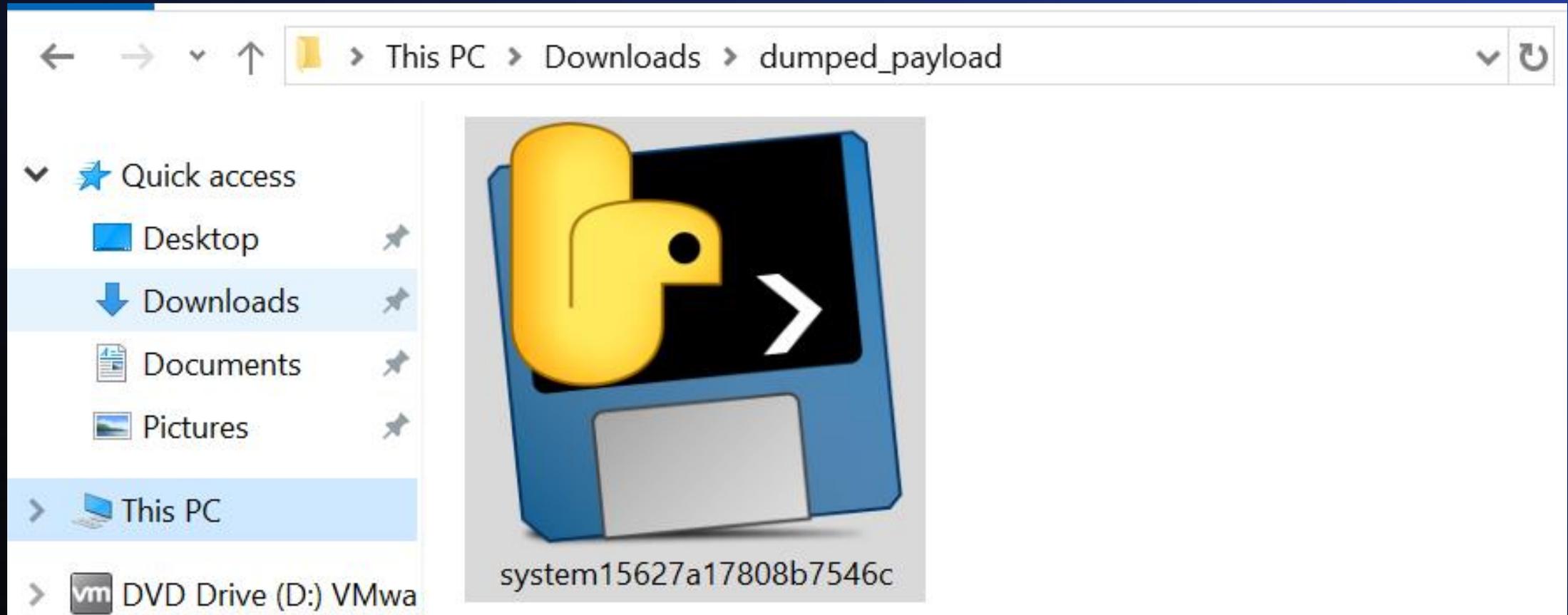


What is the archive password?

Relations graph



Dumped file contents



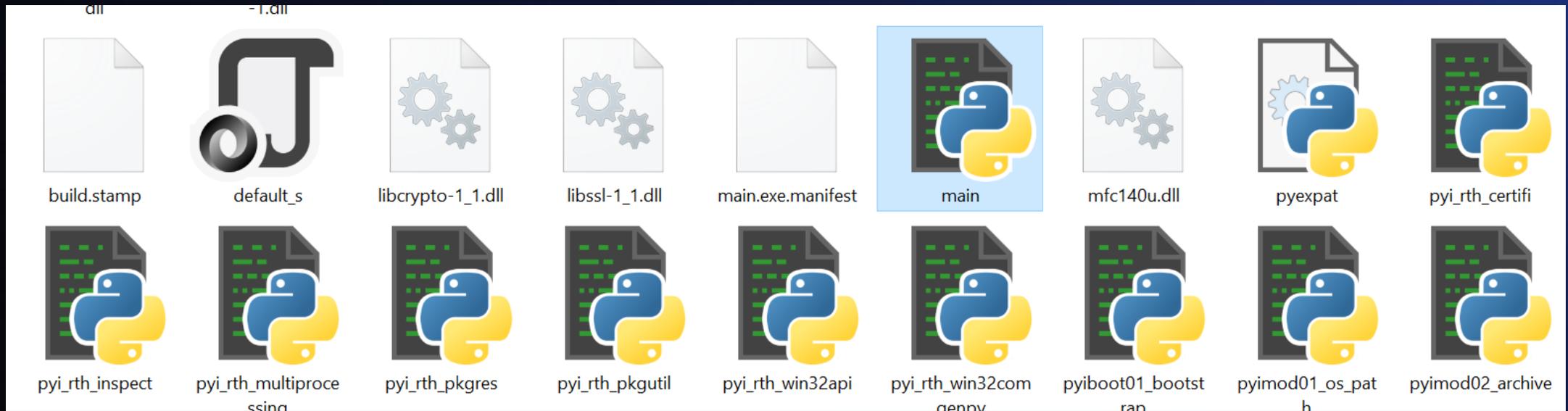
Python compiled file (PyInstaller)

Python malware analysis

**Step 1: extract executable contents
with the pyinstxtractor tool**

Python malware analysis

**Step 1: extract executable contents
with the pyinstxtractor tool**



Step outcome

Python malware analysis

Step 2: convert main.pyc to Python code

Python malware analysis

Step 2: convert main.pyc to Python code

```
C:\Users\user\Downloads\dumped_payload>uncompyle6 system15627a1780
8b7546c.exe_extracted\main.pyc
# uncompyle6 version 3.9.2
# Python bytecode version base 3.7.0 (3394)
# Decompiled from: Python 3.7.0 (v3.7.0:1bf9cc5093, Jun 27 2018, 0
4:59:51) [MSC v.1914 64 bit (AMD64)]
# Embedded file name: dist\obf\main.py
from pytransform import pyarmor_runtime
pyarmor_runtime()
__pyarmor__(__name__, __file__, b'PYARMOR\x00\x00\x03\x07\x00B\r\r
```

Step outcome: file is obfuscated

Python malware analysis

Step 3: deobfuscate file with bonedensity tool

Python malware analysis

Step 3: deobfuscate file with bonedensity tool

```
def main():  
    global browser_whitelist  
    events.set_active_browser('none')  
    config = utils.config(True, **('check_hash',))  
    if utils.is_cloud_mode():  
        cloudconfig = None
```

Step outcome: can read Python code

Python malware analysis

```
def descramble_string(key, data):  
    ret = ''.join((lambda .0: pass)(zip(data, cycle(key))))  
    return ret
```

Incorrect decompilation

Python malware analysis

[Disassembly]

```
0      LOAD_FAST           0: .0
2      FOR_ITER           30 (to 34)
4      UNPACK_SEQUENCE    2
6      STORE_FAST        1: c
8      STORE_FAST        2: k
10     LOAD_GLOBAL        0: chr
12     LOAD_GLOBAL        1: ord
14     LOAD_FAST          1: c
16     CALL_FUNCTION      1
18     LOAD_GLOBAL        1: ord
20     LOAD_FAST          2: k
22     CALL_FUNCTION      1
24     BINARY_XOR
26     CALL_FUNCTION      1
28     YIELD_VALUE
30     POP_TOP
32     JUMP_ABSOLUTE      2
34     LOAD_CONST         0: None
```

Decrypted configuration

```
    "noconfighash",  
    "cloud"  
  ],  
  "partner":  
  {},  
  "cloud_api": "https://www.eventuallogic.com",  
  "token": "dfbe082364bf46b195d49915634886da",  
  "if_platform":  
  {  
    "windows":  
    {  
      "i": "i"  
    }  
  }  
}
```

Outcome

Objectives for today:

- **Is the domain malicious?**
- **If so, what is the infection chain?**
- **If so, what is the malware type?**

Outcome

The
eventuallogic[.]com
domain name
is malicious.

Infection chain: user
downloads Let's
Encrypt software with
a malicious updater

Malicious capabilities:
backdoor, infostealer

Lessons learned

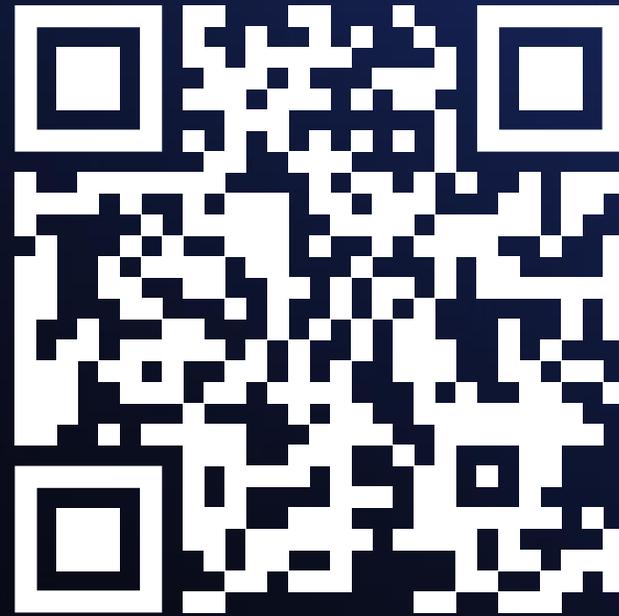
**Keep PUAs
out of your network.**

**They can deceive you
very easily.**

Thank you!



Feedback form



My LinkedIn

<https://linkedin.com/in/georgy-kucherin>



My Twitter / X

<https://x.com/kucher1n>