Analyzing Cobalt Strike Beacons, Servers and Traffic

Didier Stevens

Didier is Senior Analyst, working in the Cyber Resilience team and Research & Development team.

Next to his professsional activities at NVISO, Didier is also a Microsoft MVP (2011-2016 awarded MVP Consumer Security, 2016-2022 awarded MVP Windows Insider) and a SANS Internet Storm Center Senior Handler.

He is an expert in malicious documents (PDF and Microsoft Office), pioneering research into maldocs and authoring free, open-source analysis tools and private red team tools.

Didier Stevens

dstevens@nviso.be

didierstevens

Intro

Introduction to Cobalt Strike for Blue Teamers

Beacon Analysis

Analysis of Cobalt Strike beacons

Q&A

Feel free to ask questions at any moment

Network traffic analysis

Analysis of the encrypted network traffic between a Cobalt Strike beacon and a Team Server

Intro

Introduction to Cobalt Strike for Blue Teamers

Intro


cobaltstrike
by HelpSystems
Download
Community Kit
Contact Us
BUY NOW
FEATURES
SCREENSHOTS
TRAINING
SUPPORT
Software for
Adversary Simulations and Red Team Operations
DOWNLOAD
BUY NOW
Adversary Simulations and Red Team Operations are security assessments that replicate the tactics and techniques of an advanced adversary in a network. While penetration tests focus on unpatched vulnerabilities and misconfigurations, these assessments benefit security operations and incident response.

Blue Team Perspective

Intro

INCIDENT RESPONSE

BLOG

Defining Cobalt Strike Components So You Can BEA-CONfident in Your Analysis

ALYSSA RAHMAN

OCT 12, 2021 | 23 MINS READ

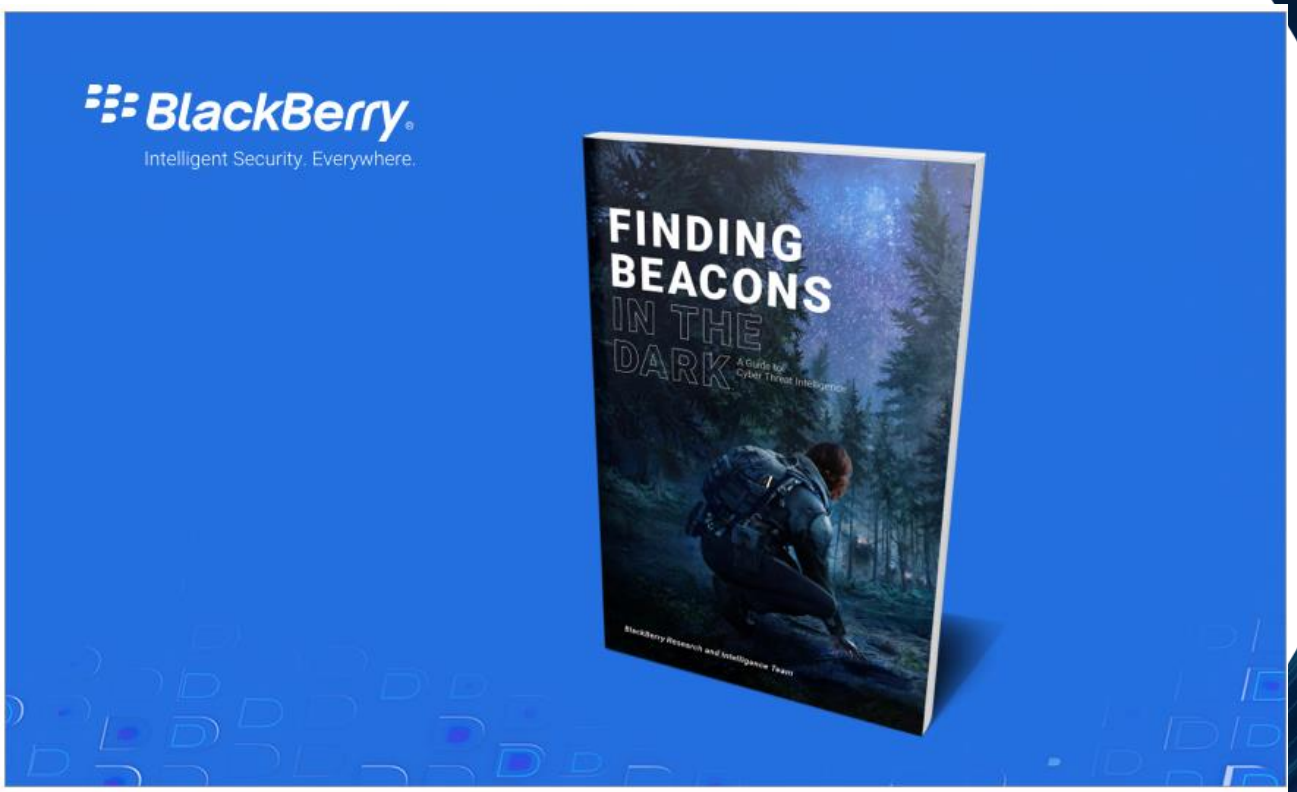
#MALWARE #THREAT RESEARCH

Cobalt Strike is a commercial adversary simulation software that is marketed to red teams but is also stolen and actively used by a wide range of threat actors from ransomware operators to espionage-focused Advanced Persistent Threats (APTs). Many network defenders have seen Cobalt Strike payloads used in intrusions, but for those who have not had the opportunity to use Cobalt Strike as an operator, it can be challenging to understand the many components and features included in this framework.

In this blog post, we will walk through important definitions and concepts to help defenders understand Cobalt Strike and, hopefully, identify new ways to hunt for, respond to, and attribute malicious actors using this tool.

Intro

https://blogs.blackberry.com/en/2021/10/blackberry-shines-spotlight-on-evolving-cobalt-strike-threat-in-new-book



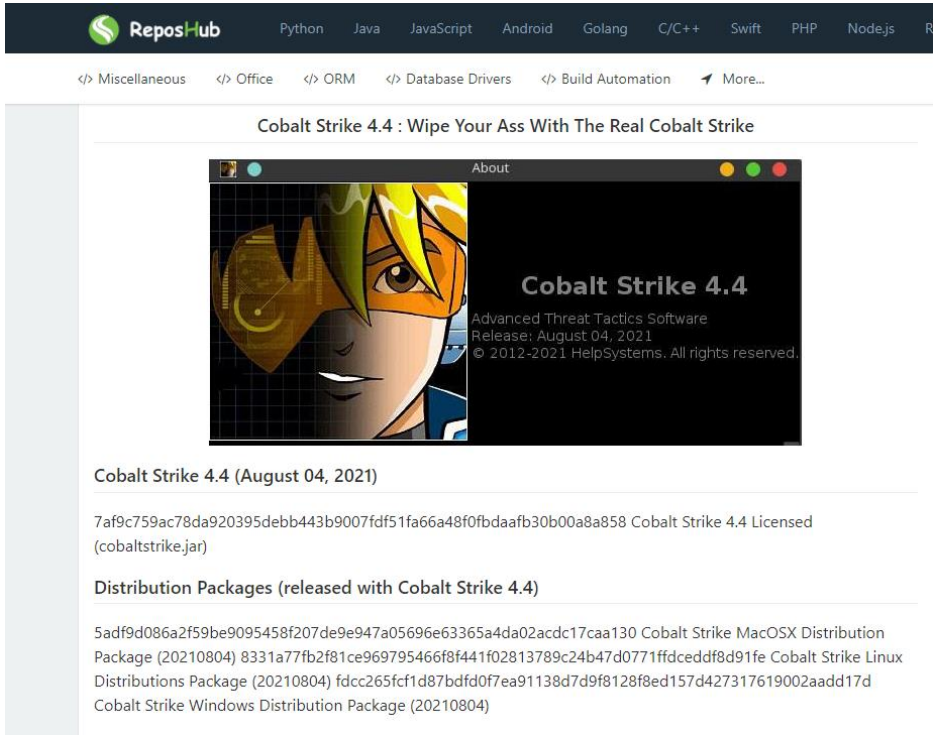
Intro


Cobalt Strike 4.4
Advanced Threat Tactics Software
Release: August 04, 2021
© 2012-2021 HelpSystems. All rights reserved.

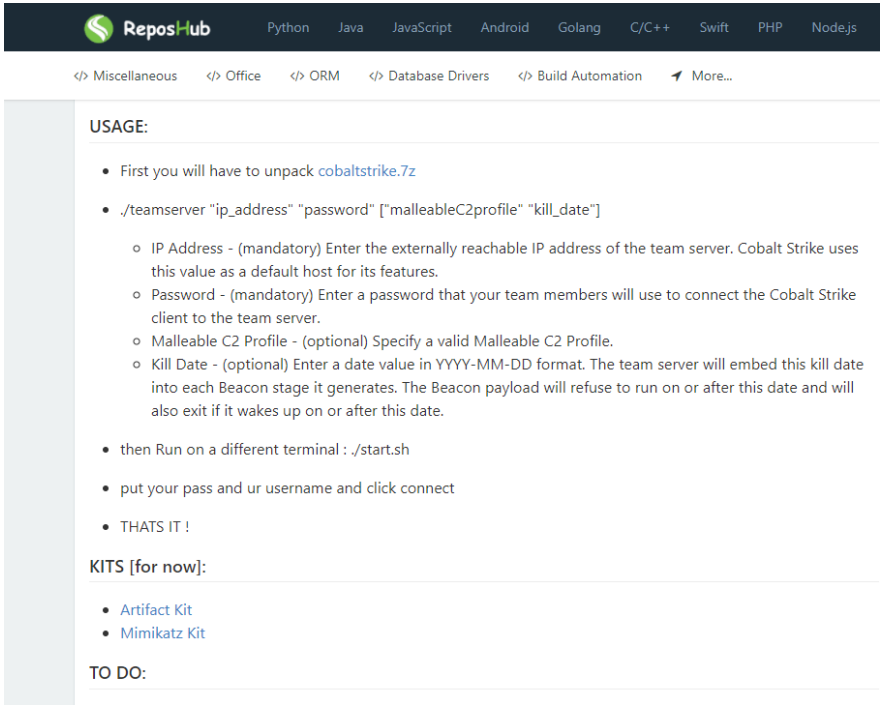
Intro


Cobalt Strike 4.4
Advanced Threat Tactics Software
Release: August 04, 2021
© 2012-2021 HelpSystems. All rights reserved.

Intro


ReposHub
Python
Java
JavaScript
Android
Golang
C/C++
Swift
PHP
Node.js
Miscellaneous
Office
ORM
Database Drivers
Build Automation
More...
Cobalt Strike 4.4 : Wipe Your Ass With The Real Cobalt Strike
About
Cobalt Strike 4.4
Advanced Threat Tactics Software
Release: August 04, 2021
© 2012-2021 HelpSystems. All rights reserved.
Cobalt Strike 4.4 (August 04, 2021)
7af9c759ac78da920395debb443b9007fdf51fa66a48f0fbdaafb30b00a8a858 Cobalt Strike 4.4 Licensed (cobaltstrike.jar)
Distribution Packages (released with Cobalt Strike 4.4)
5adf9d086a2f59be9095458f207de9e947a05696e63365a4da02acdc17caa130 Cobalt Strike MacOSX Distribution Package (20210804) 8331a77fb2f81ce969795466f8f441f02813789c24b47d0771ffdceddf8d91fe Cobalt Strike Linux Distributions Package (20210804) fdcc265fcf1d87bdfd0f7ea91138d7d9f8128f8ed157d427317619002aadd17d Cobalt Strike Windows Distribution Package (20210804)

Intro



ReposHub Python Java JavaScript Android Golang C/C++ Swift PHP Node.js

</> Miscellaneous </> Office </> ORM </> Database Drivers </> Build Automation More...

USAGE:

- First you will have to unpack cobaltstrike.7z
- ./teamserver "ip_address" "password" ["malleableC2profile" "kill_date"]
  - IP Address - (mandatory) Enter the externally reachable IP address of the team server. Cobalt Strike uses this value as a default host for its features.
  - Password - (mandatory) Enter a password that your team members will use to connect the Cobalt Strike client to the team server.
  - Malleable C2 Profile - (optional) Specify a valid Malleable C2 Profile.
  - Kill Date - (optional) Enter a date value in YYYY-MM-DD format. The team server will embed this kill date into each Beacon stage it generates. The Beacon payload will refuse to run on or after this date and will also exit if it wakes up on or after this date.
- then Run on a different terminal : ./start.sh
- put your pass and ur username and click connect
- THATS IT !

KITS [for now]:

- Artifact Kit
- Mimikatz Kit

TO DO:

Intro

Cobalt strike
MANUALS_V2
Active Directory

I Tier . Increasing privileges and collecting information

1 . Initial exploration

1.1 . Search for company income

Finding the company's website
On Google : SITE + revenue (mycorporation.com + revenue) ("mycorporation.com" "revenue")
check more than 1 site, if possible
(owler, manta, zoominfo, dnb, rocketrich)

1.2 . Defined by AB

1.3 . **shell whoami** < ===== who am I

1.4 . **shell whoami / groups** -> my rights on the bot (if the bot came with a blue monik)

1.5 . 1 . **shell nltest / dclist:** <===== domain controllers

Intro

Team Server = C2 Server

Beacon = Bot

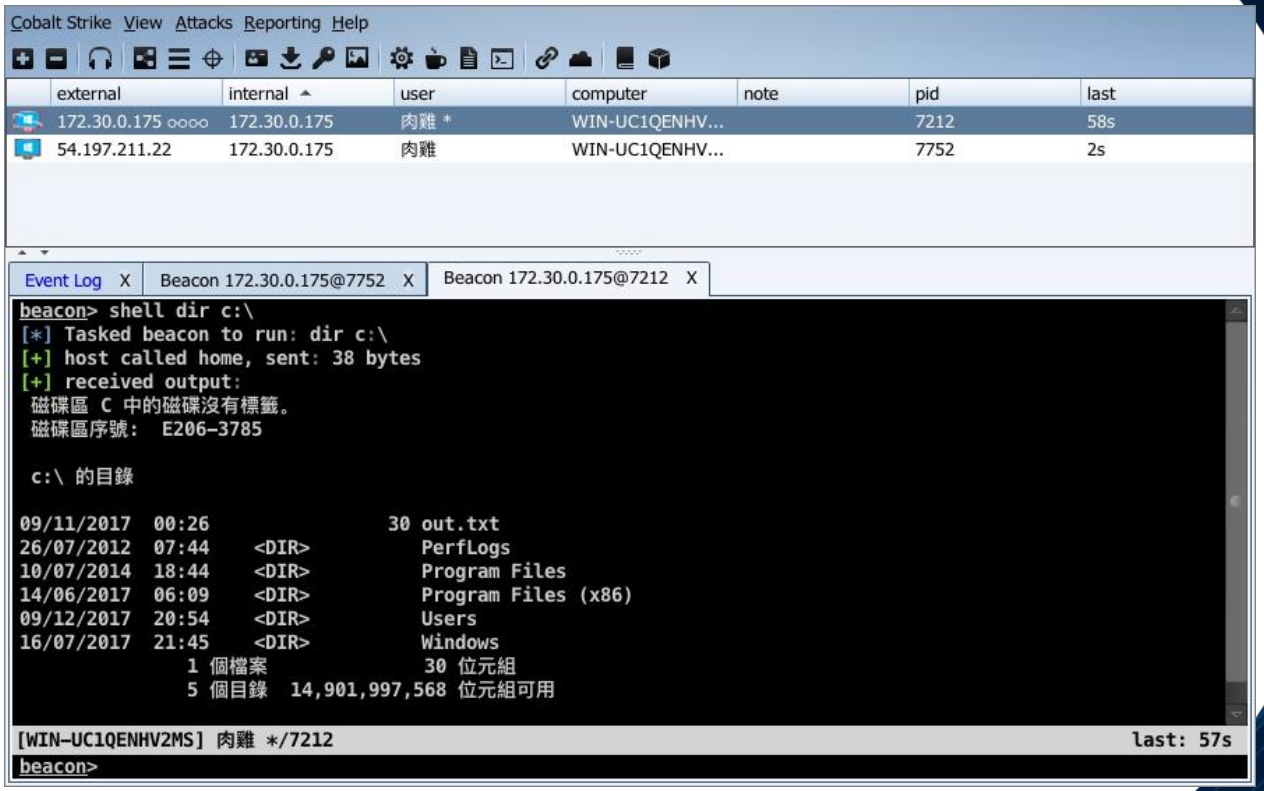
nviso

Team Server = Management Server

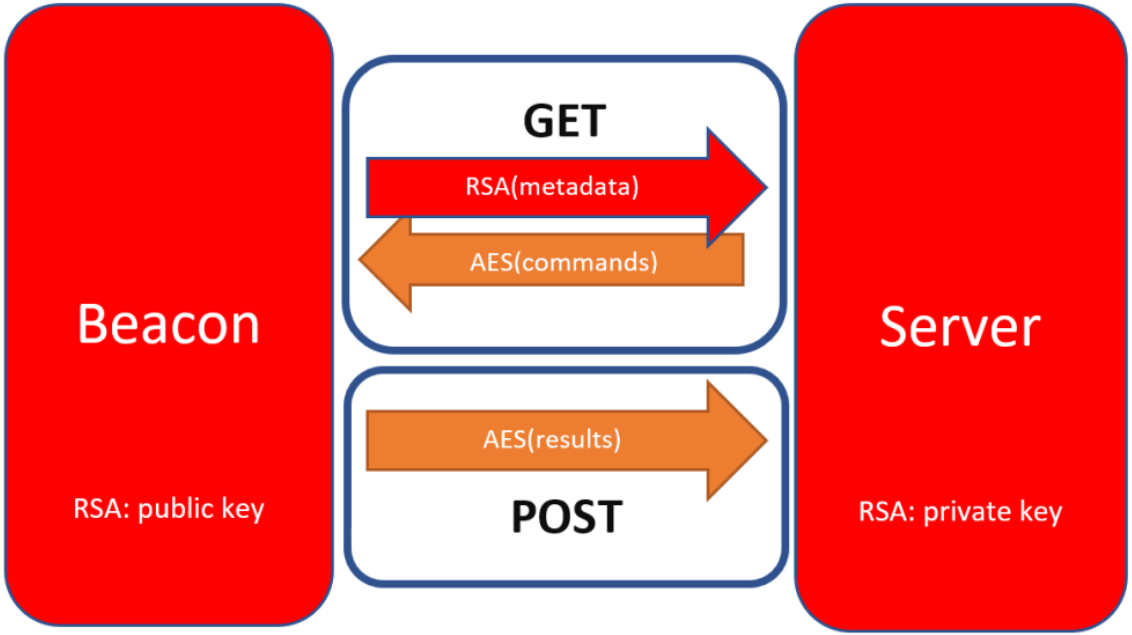
Beacon = Agent

Intro

Intro


Cobalt Strike View Attacks Reporting Help
external internal user computer note pid last
172.30.0.175 172.30.0.175 肉雞 * WIN-UC1QENHV... 7212 58s
54.197.211.22 172.30.0.175 肉雞 WIN-UC1QENHV... 7752 2s
Event Log X
Beacon 172.30.0.175@7752 X
Beacon 172.30.0.175@7212 X
beacon> shell dir c:\
[*] Tasked beacon to run: dir c:\
[+] host called home, sent: 38 bytes
[+] received output:
磁碟區 C 中的磁碟沒有標籤。
磁碟區序號: E206-3785
c:\ 的目錄
09/11/2017 00:26 30 out.txt
26/07/2012 07:44 <DIR> PerfLogs
10/07/2014 18:44 <DIR> Program Files
14/06/2017 06:09 <DIR> Program Files (x86)
09/12/2017 20:54 <DIR> Users
16/07/2017 21:45 <DIR> Windows
1 個檔案 30 位元組
5 個目錄 14,901,997,568 位元組可用
[WIN-UC1QENHV2MS] 肉雞 */7212 last: 57s
beacon>

Intro


Beacon
RSA: public key
GET
RSA(metadata)
AES(commands)
AES(results)
POST
Server
RSA: private key

NVISO Labs

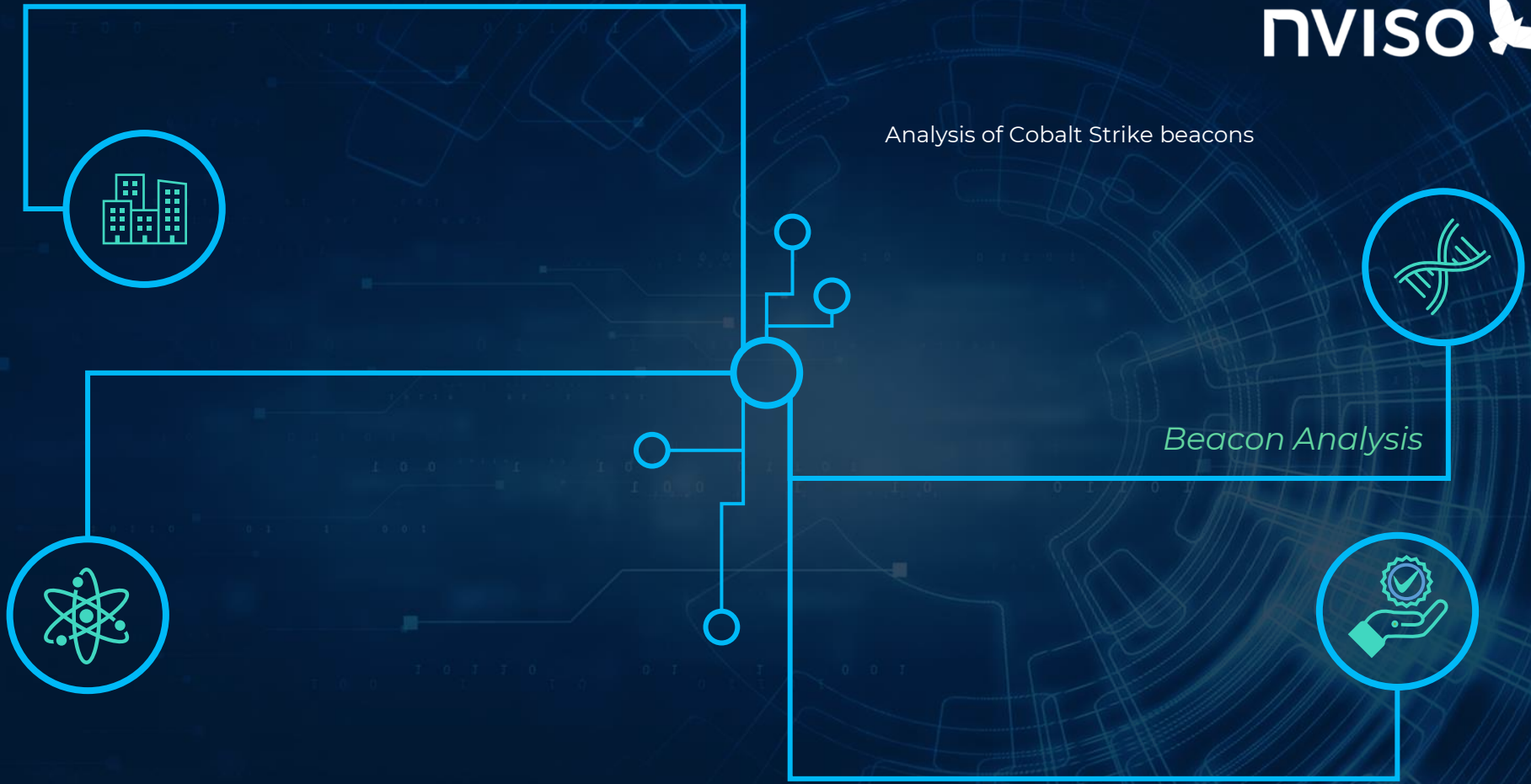
Cyber security research, straight from the lab!

Cobalt Strike: Using Known Private Keys To Decrypt Traffic – Part 1

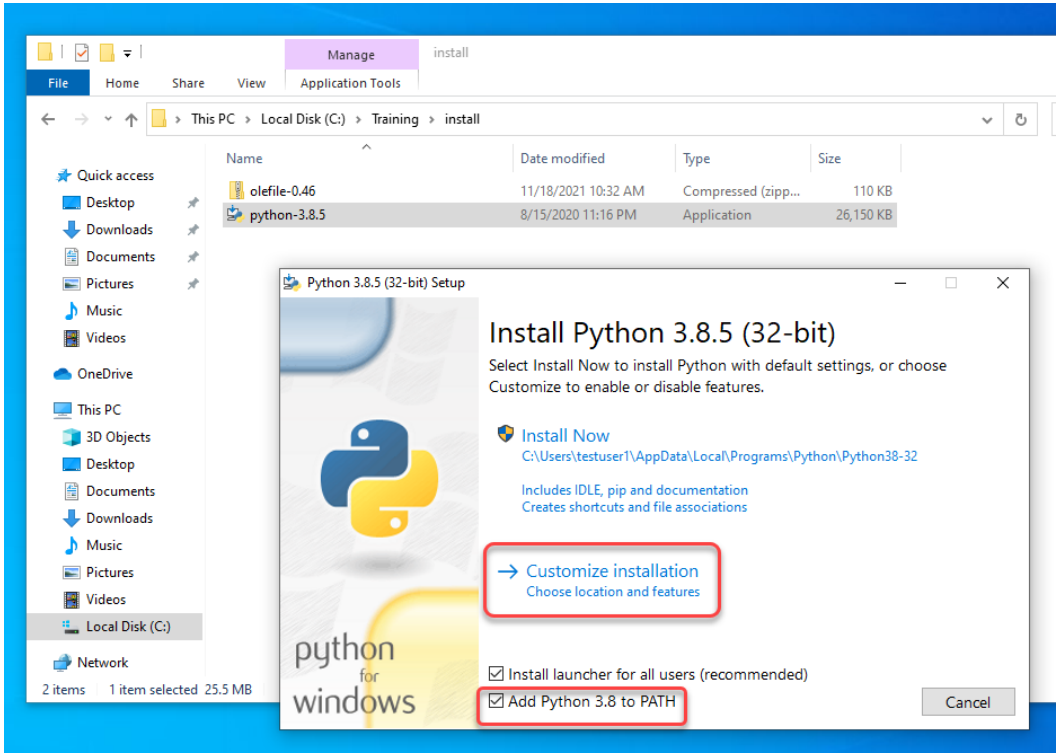
Didier Stevens | cyber threats, Forensics | October 21, 2021 | 2 Minutes

We found 6 private keys for rogue Cobalt Strike software, enabling C2 network traffic decryption.

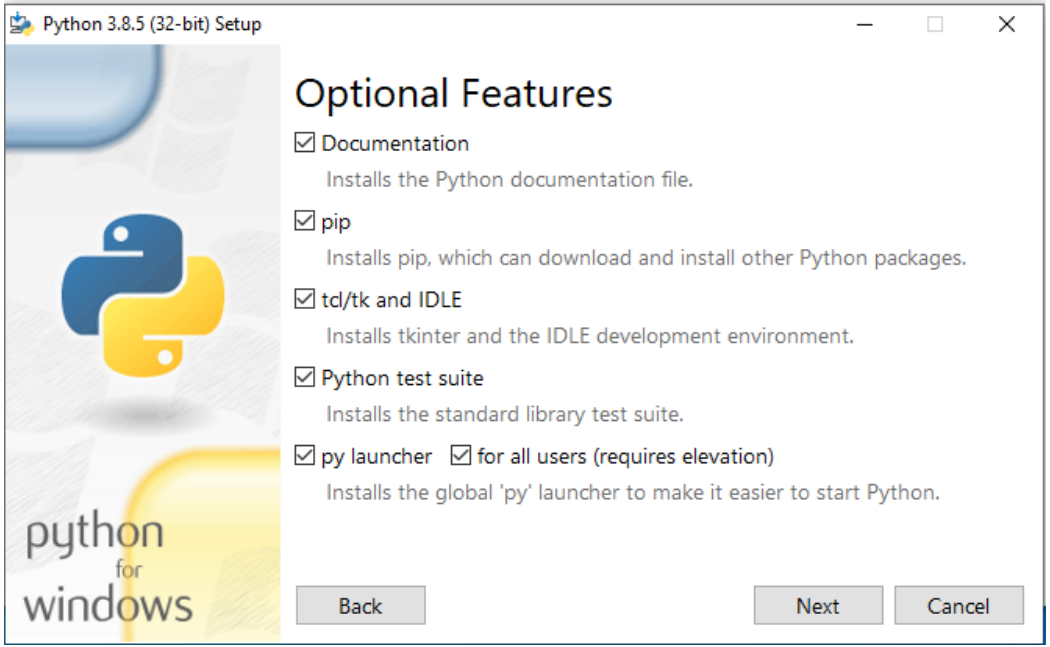
The communication between a Cobalt Strike beacon (client) and a Cobalt Strike team server (C2) is encrypted with AES (even when it takes place over HTTPS). The AES key is generated by the beacon, and communicated to the C2 using an encrypted metadata blob (a cookie, by default).


Beacon Analysis

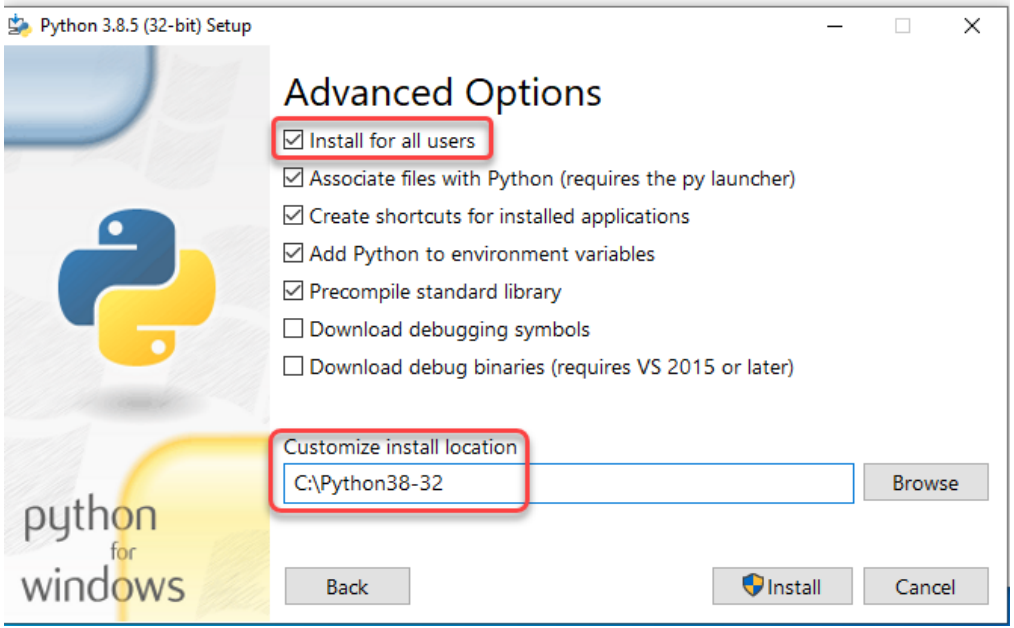
Beacon analysis



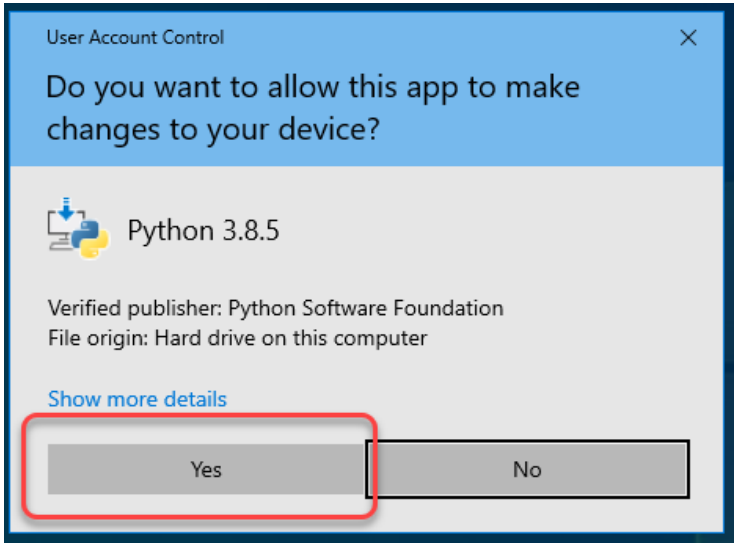
Beacon analysis



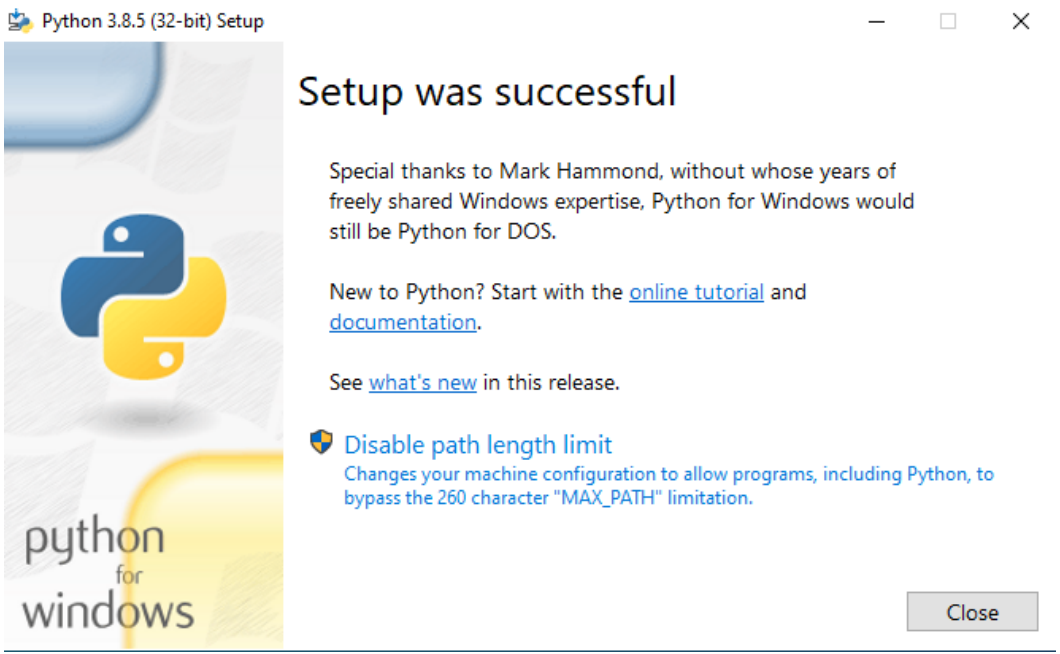
Beacon analysis



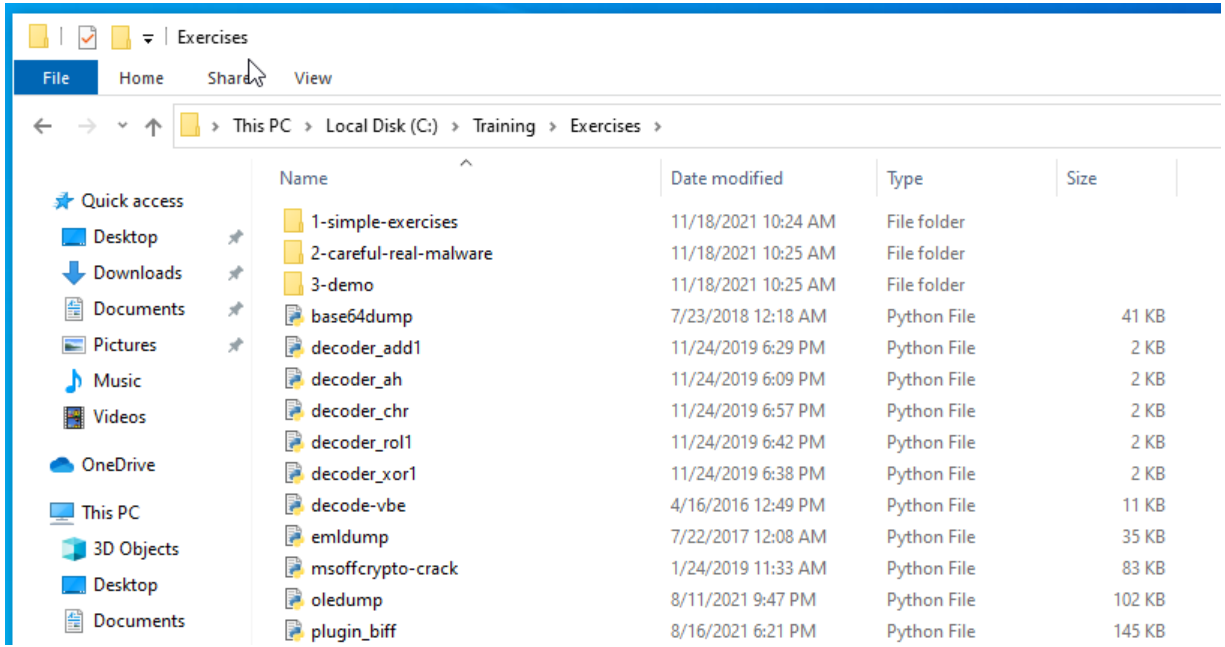
Beacon analysis



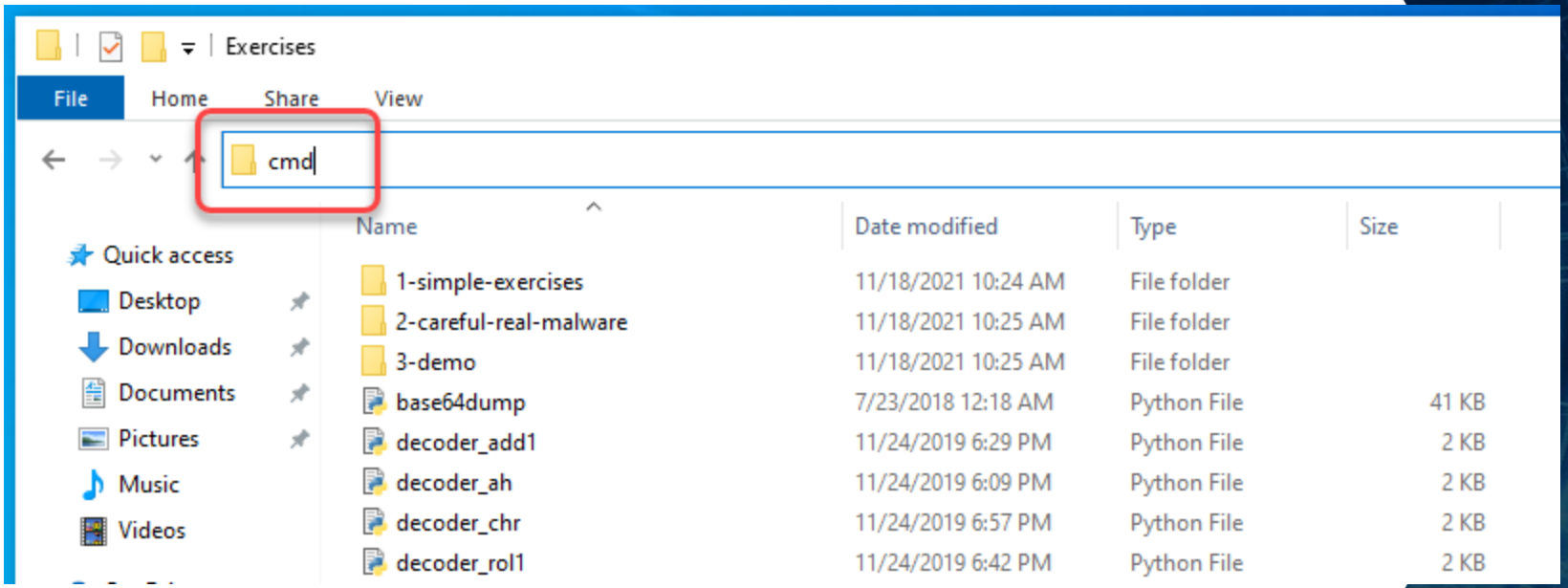
Beacon analysis



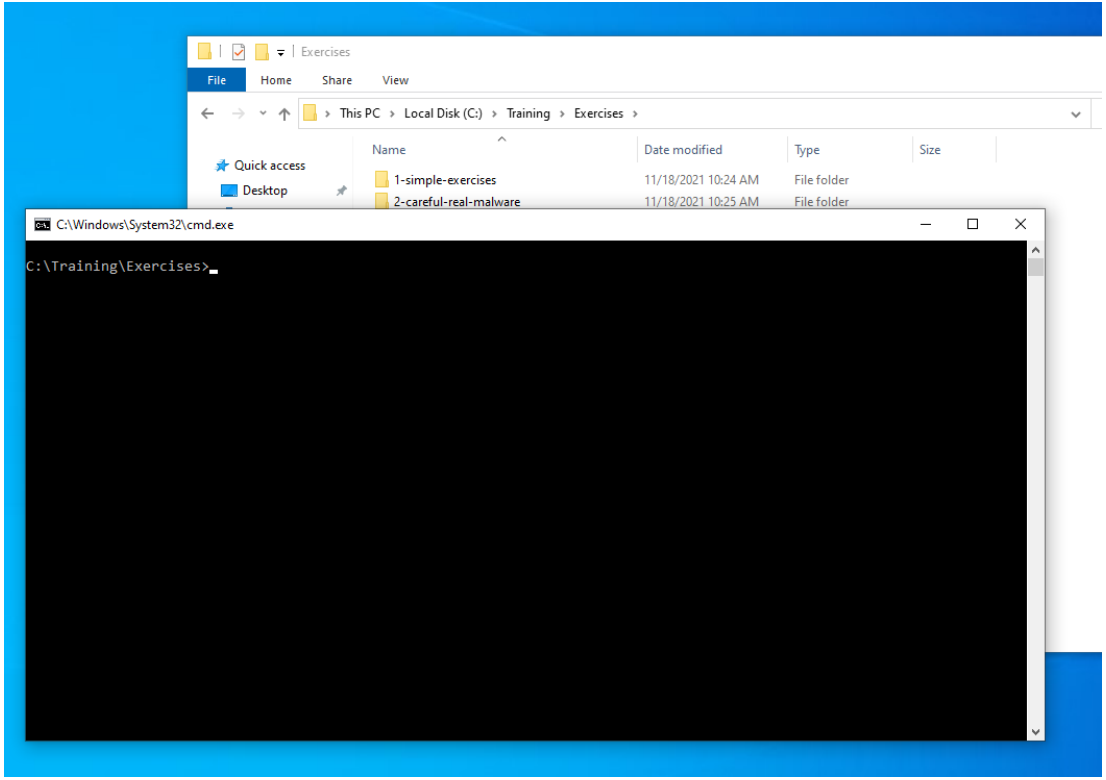
Beacon analysis



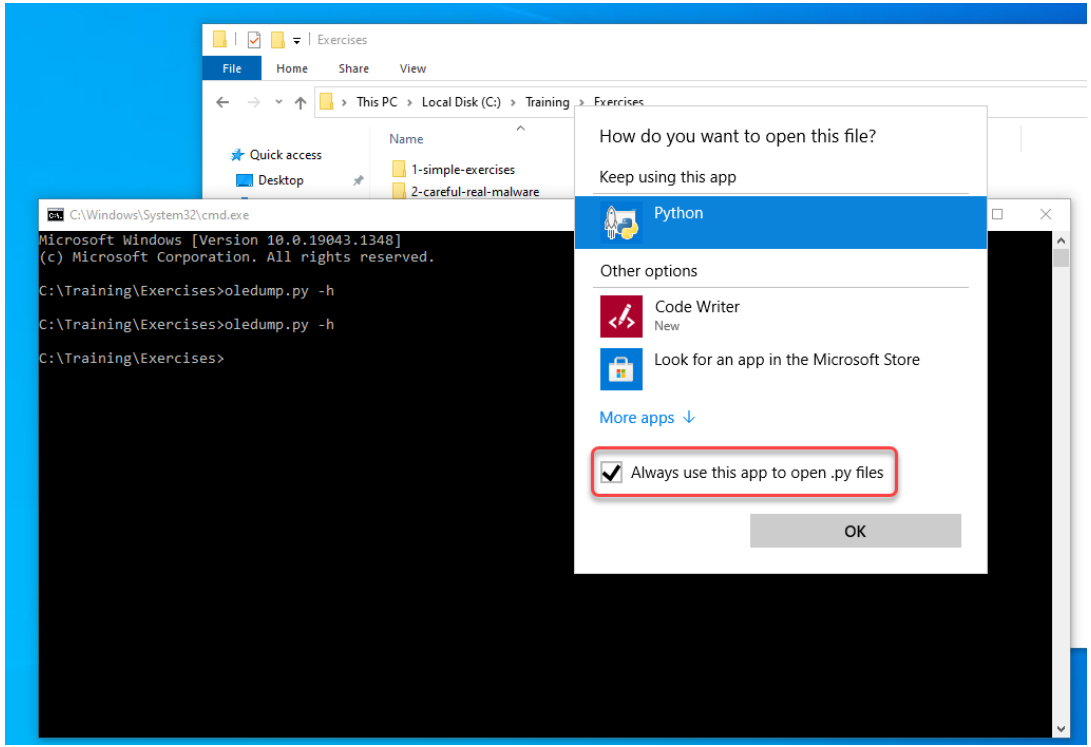
Beacon analysis



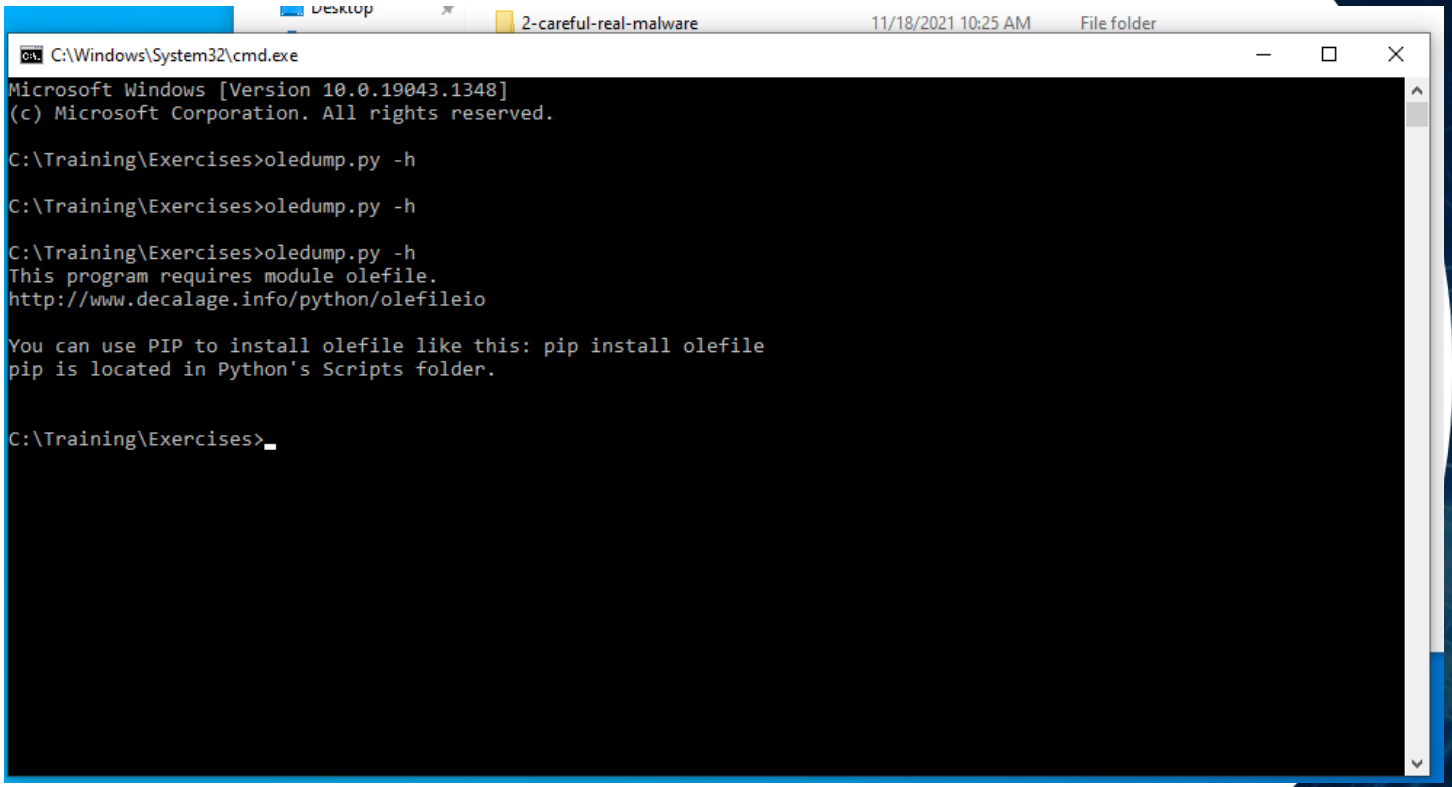
Beacon analysis



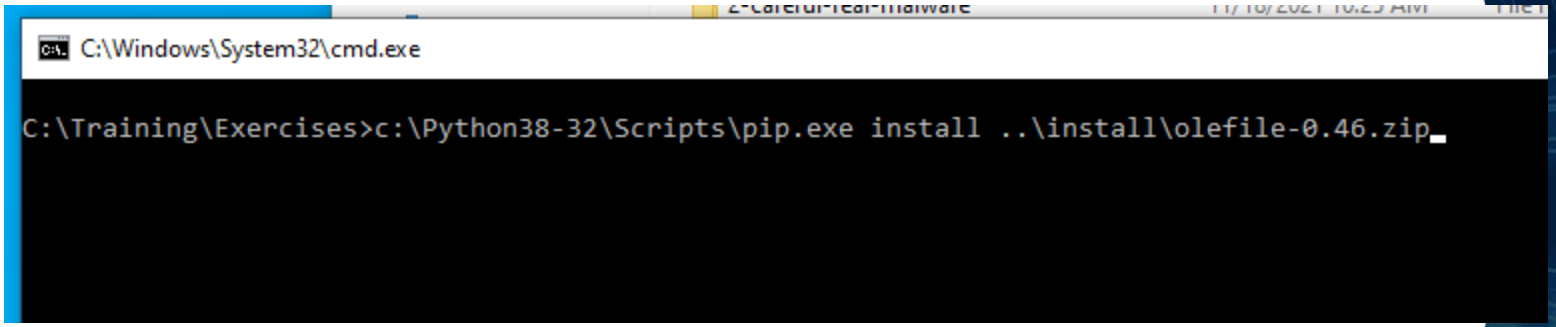
Beacon analysis



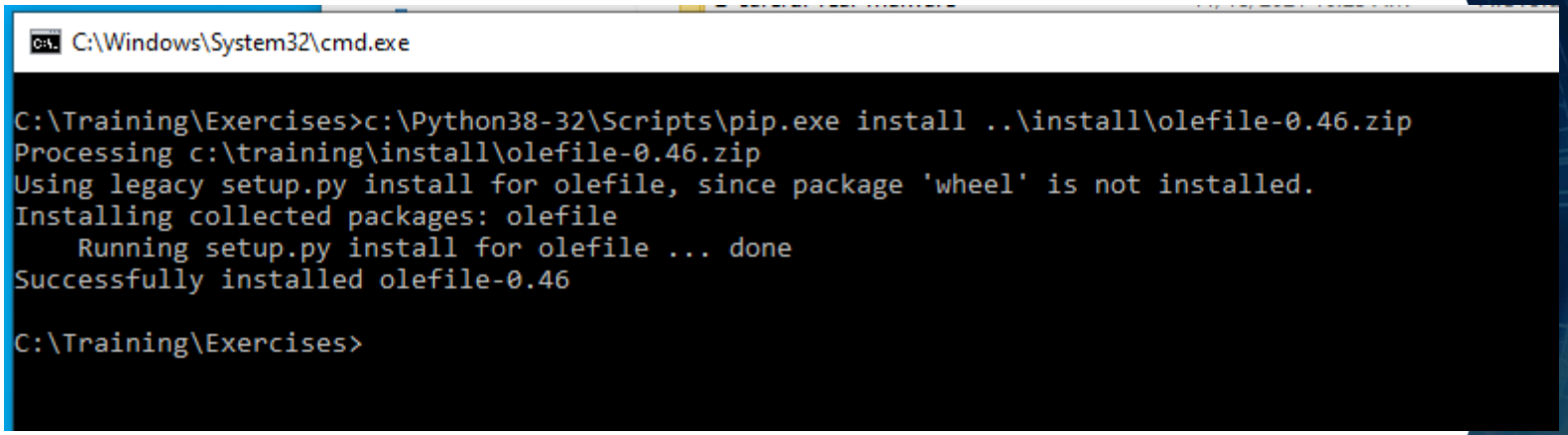
Beacon analysis



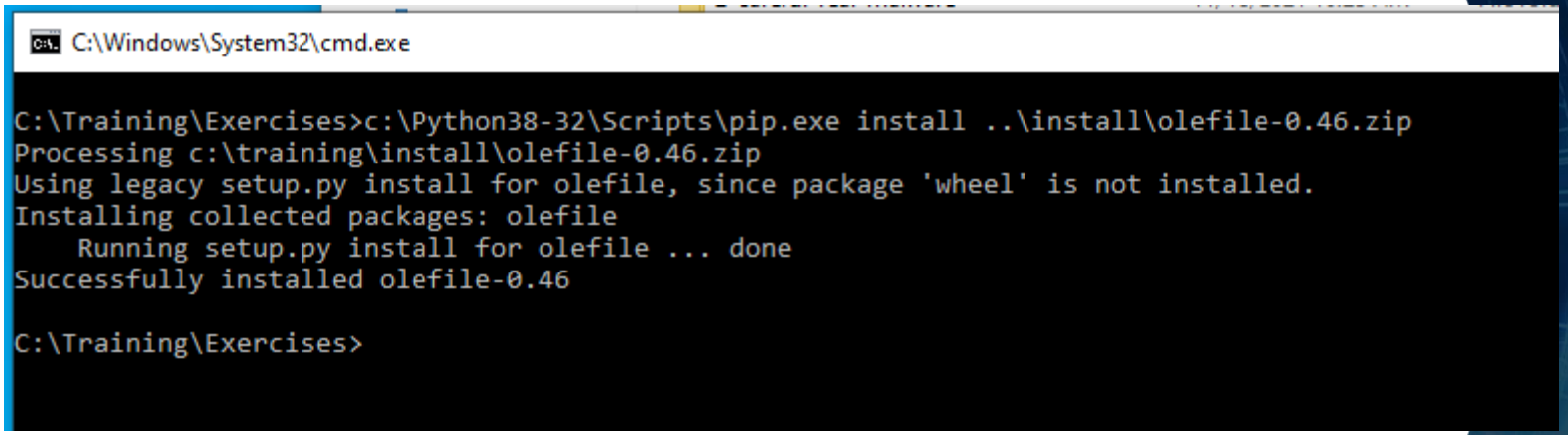
Beacon analysis



Beacon analysis



Beacon analysis



Practical & Hands-on

Beacon analysis

1768.Py

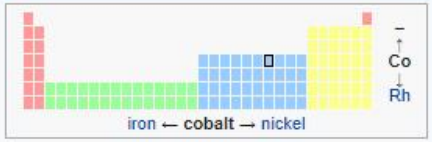
c:\Python38-32\Scripts\pip.exe install pefile

Beacon analysis

Cobalt, $_{27}$Co

Cobalt	
Pronunciation	/ˈkoʊbɒlt/ (listen)[1]
Appearance	hard lustrous bluish gray metal
Standard atomic weight $A_{r,\,std}$(Co)	58.933 194(3)[2]

Cobalt in the periodic table

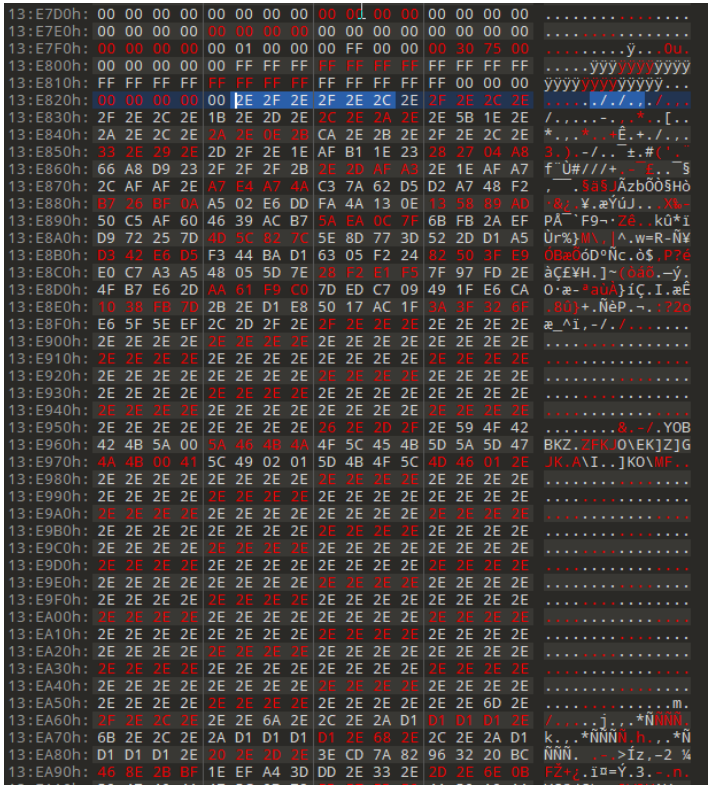


Physical properties	
Phase at STP	solid
Melting point	1768 K (1495 °C, 2723 °F)
Boiling point	3200 K (2927 °C, 5301 °F)
Density (near r.t.)	8.90 g/cm^3
when liquid (at m.p.)	8.86 g/cm^3
Heat of fusion	16.06 kJ/mol
Heat of vaporization	377 kJ/mol
Molar heat capacity	24.81 J/(mol·K)

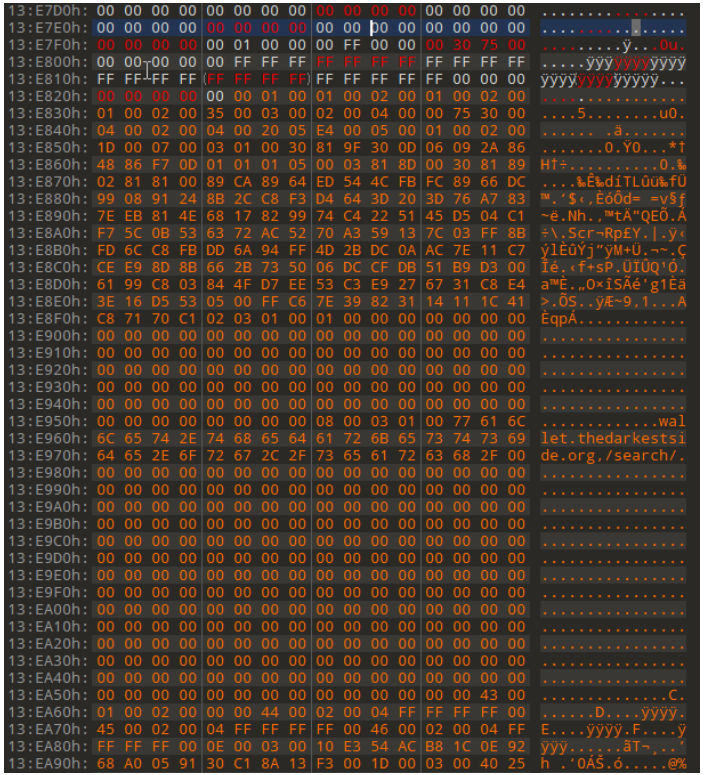
Vapor pressure

P (Pa)	1	10	100	1 k	10 k	100 k
at T (K)	1790	1960	2165	2423	2755	3198

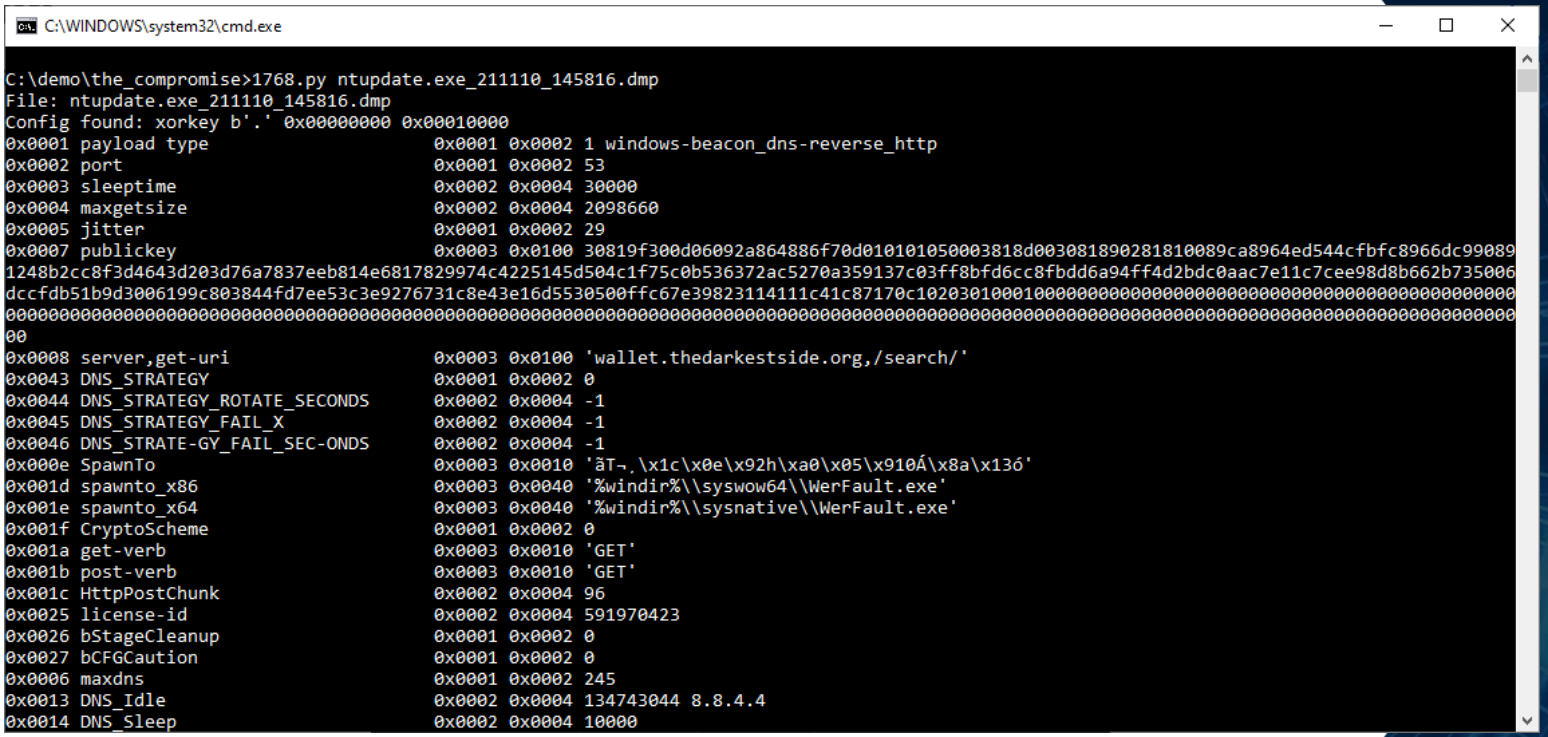
Beacon analysis



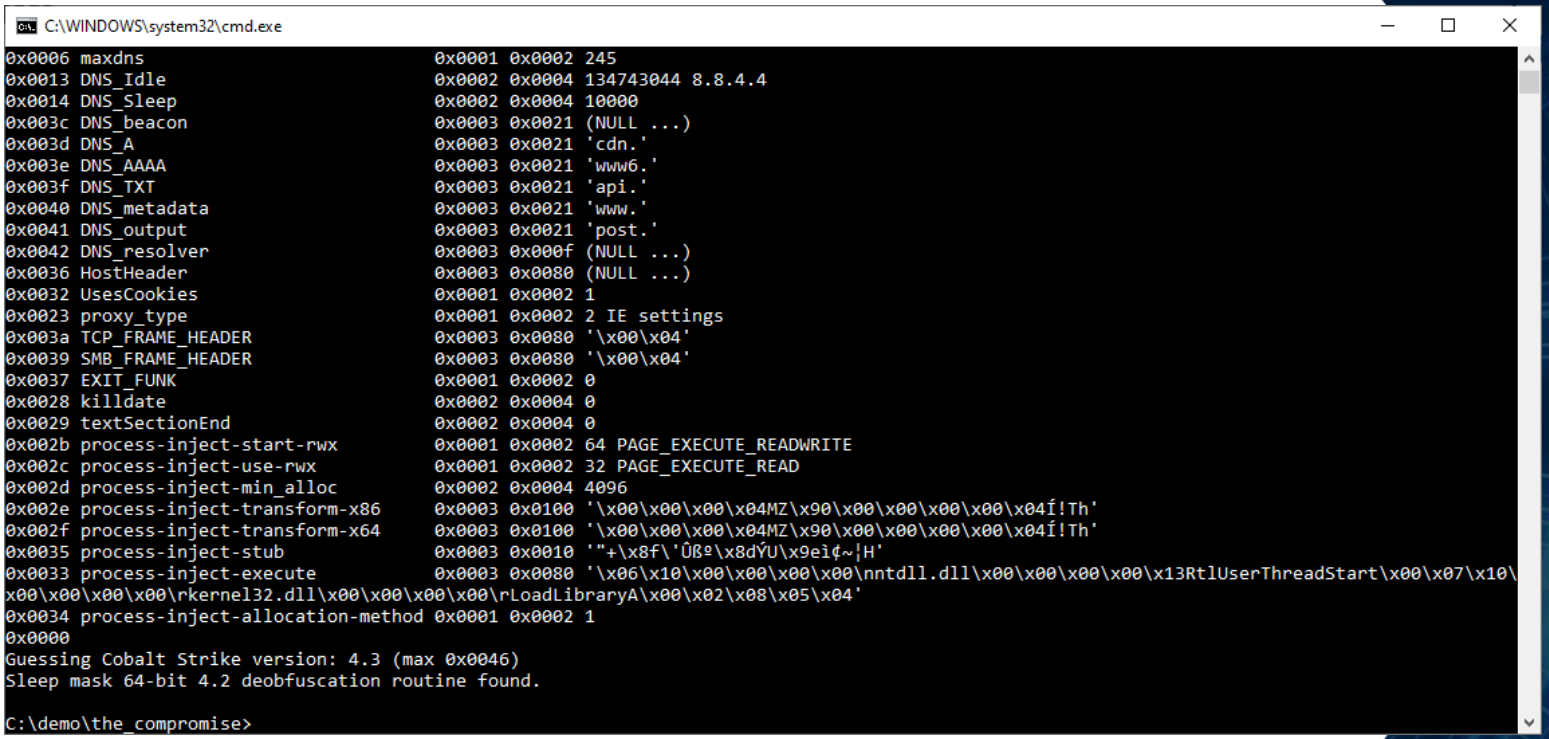
Beacon analysis



Beacon analysis



Beacon analysis



Exercise 01: beacon.exe

Exercise 02:
VBA maldoc with shellcode

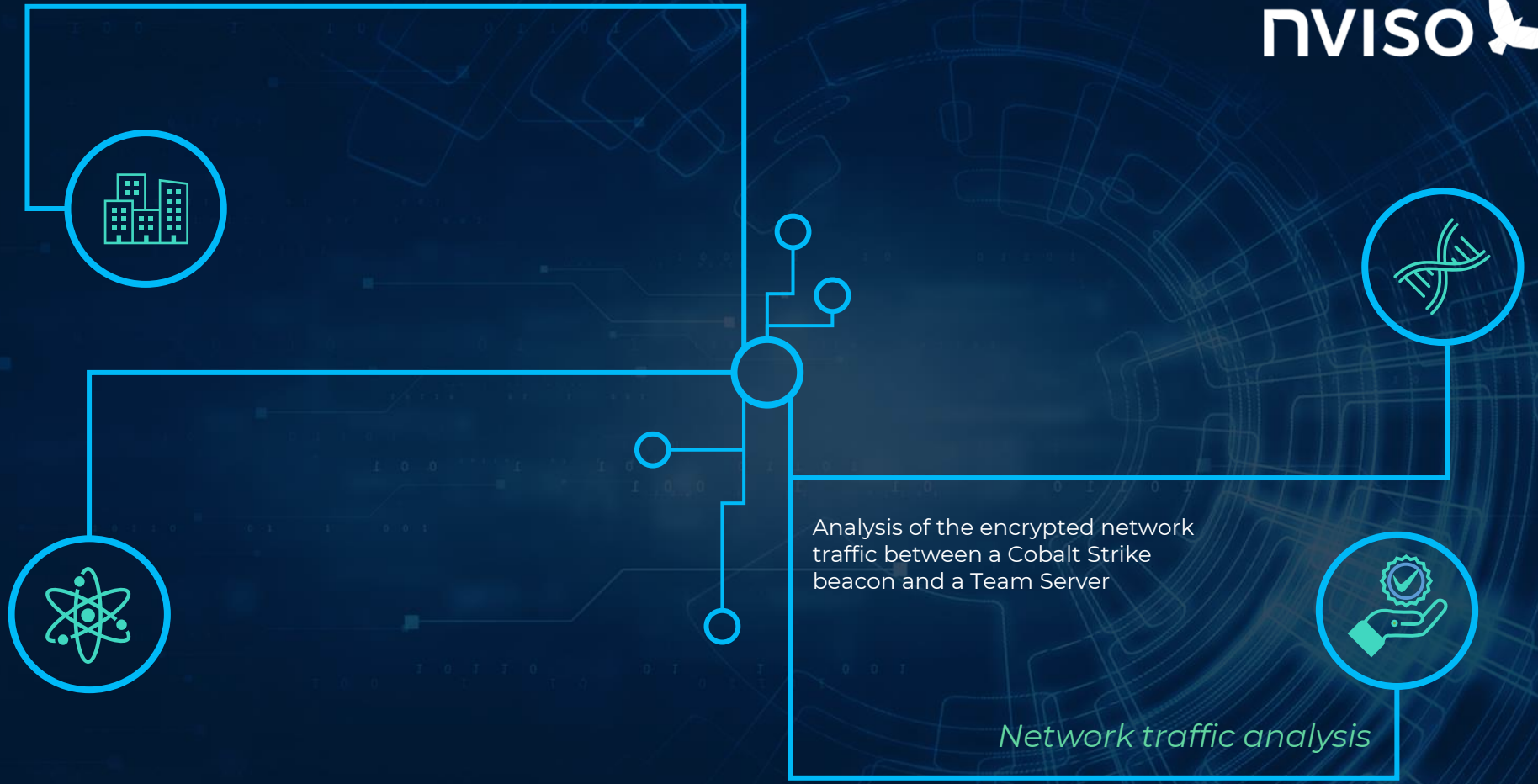
Exercise 03:
Excel 4 macros with shellcode

Exercise 04:
Stager shellcode & beacon

Exercise 05:
PowerShell & Shellcode

Exercise 06:
Process Memory Dump

Exercise 07: Packed/Protected Beacon


Analysis of the encrypted network traffic between a Cobalt Strike beacon and a Team Server
Network traffic analysis

Network traffic analysis

NVISO Labs

Cyber security research, straight from the lab!

Cobalt Strike: Using Known Private Keys To Decrypt Traffic – Part 1

Didier Stevens | cyber threats, Forensics | October 21, 2021 | 2 Minutes

We found 6 private keys for rogue Cobalt Strike software, enabling C2 network traffic decryption.

The communication between a Cobalt Strike beacon (client) and a Cobalt Strike team server (C2) is encrypted with AES (even when it takes place over HTTPS). The AES key is generated by the beacon, and communicated to the C2 using an encrypted metadata blob (a cookie, by default).

https://blog.nviso.eu/2021/11/29/cobalt-strike-decrypting-dns-traffic-part-5/

Wireshark

c:\Python38-32\Scripts\pip.exe install pyshark

c:\Python38-32\Scripts\pip.exe install pycryptodome

c:\Python38-32\Scripts\pip.exe install minidump

metatool.py

Exercise 08: Checksum8 URL

cs-parse-traffic.py

Exercise 09: Unencrypted Traffic

cs-decrypt-metadata.py

Exercise 10:
Leaked Private Key

cs-extract-key.py

Exercise 11:
Process Memory Dump (version 3)

Exercise 12:
Process Memory Dump (version 4)

cs-analyze-processdump.py

Exercise 13:
Sleep Mask Process Memory Dump

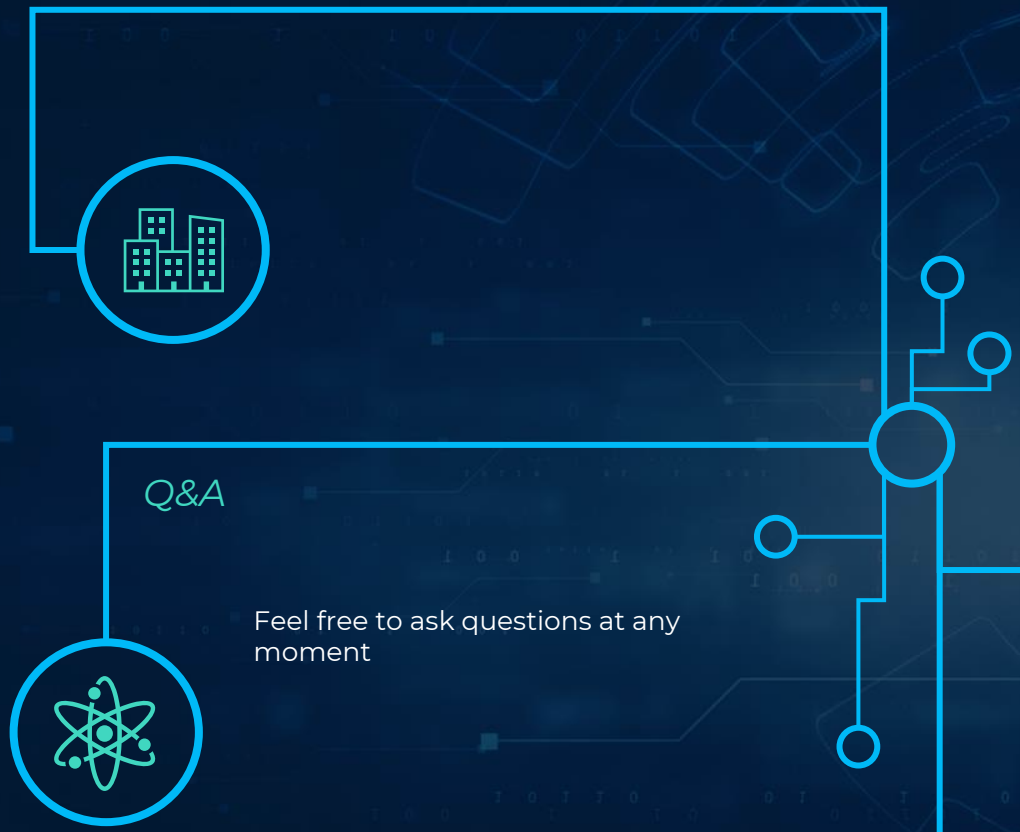
Exercise 14:
Data Transforms

Exercise 15: Unencrypted DNS

Network traffic analysis

A record reply	Last byte	Last nibble	Do checkin	DNS mode	record type
0.0.0.240	0xF0	0000	N	mode dns	A
0.0.0.241	0xF1	0001	Y	mode dns	A
0.0.0.242	0xF2	0010	N	mode dns-txt	TXT
0.0.0.243	0xF3	0011	Y	mode dns-txt	TXT
0.0.0.244	0xF4	0100	N	mode dns6	AAAA
0.0.0.245	0xF5	0101	Y	mode dns6	AAAA

Exercise 16: Encrypted DNS



Q&A

Feel free to ask questions at any moment

nviso

solutions.txt