



Analyzing Cobalt Strike Beacons, Servers and Traffic

Didier Stevens



Didier Stevens

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

Next to his professional 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.



dstevens@nviso.be



[didierstevens](#)

Intro

Introduction to Cobalt Strike for Blue Teamers



Analysis of Cobalt Strike beacons



Beacon Analysis

Q&A

Feel free to ask questions at any moment



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



Network traffic analysis

Intro

Introduction to Cobalt Strike for Blue Teamers



cobaltstrike
by HelpSystems

BUY NOW

FEATURES

SCREENSHOTS

TRAINING

Download Community Kit Contact Us

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



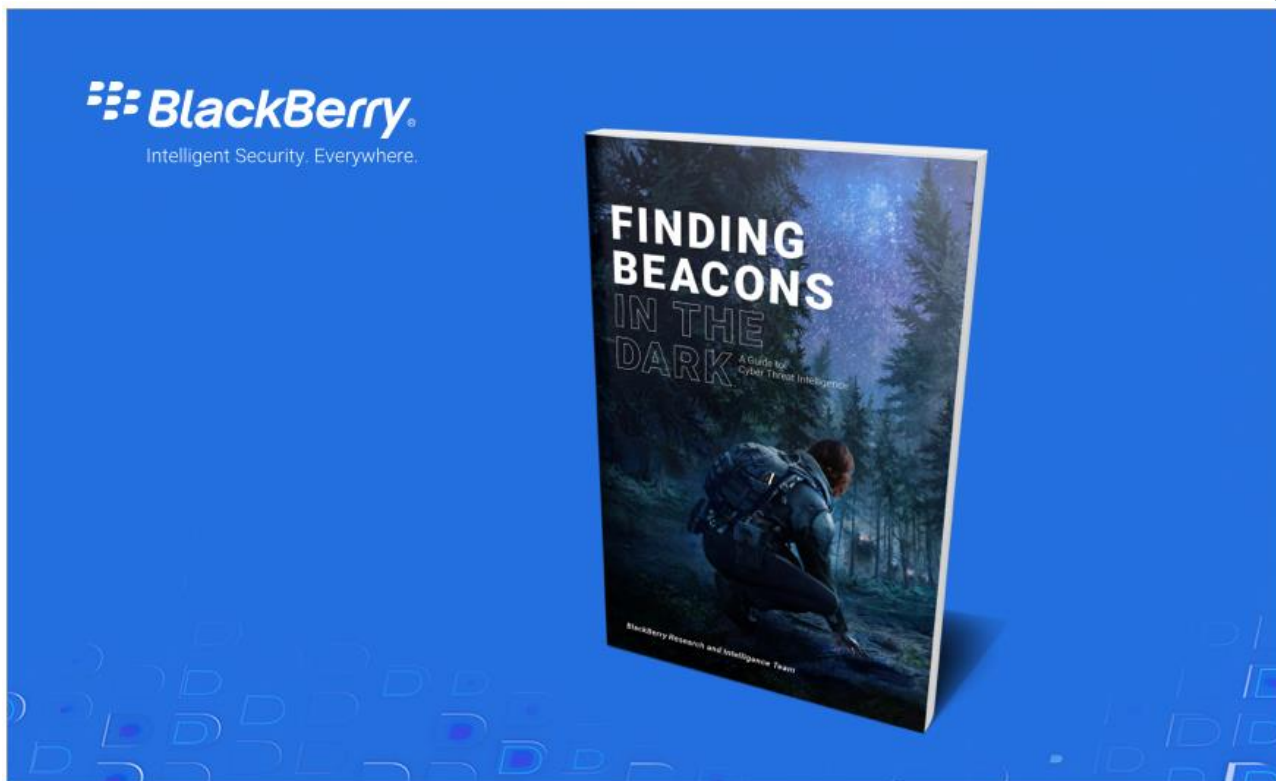
The screenshot shows a blog post on a website. At the top left is a red 'M' logo. In the top right corner, there is a navigation menu with 'INCIDENT RESPONSE' highlighted in white and a red circle with a white exclamation mark next to it. Below the logo, the word 'BLOG' is written in a small, grey font. The main title of the blog post is 'Defining Cobalt Strike Components So You Can BEA-CONFIDENT in Your Analysis' in a large, bold, black font. Below the title, the author's name 'ALYSSA RAHMAN' is displayed in a smaller, grey font, followed by the date and reading time 'OCT 12, 2021 | 23 MINS READ'. At the bottom of the header section, there are two hashtags: '#MALWARE' and '#THREAT RESEARCH'. The main body of the blog post is visible at the bottom of the screenshot, starting with a paragraph about Cobalt Strike.

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>



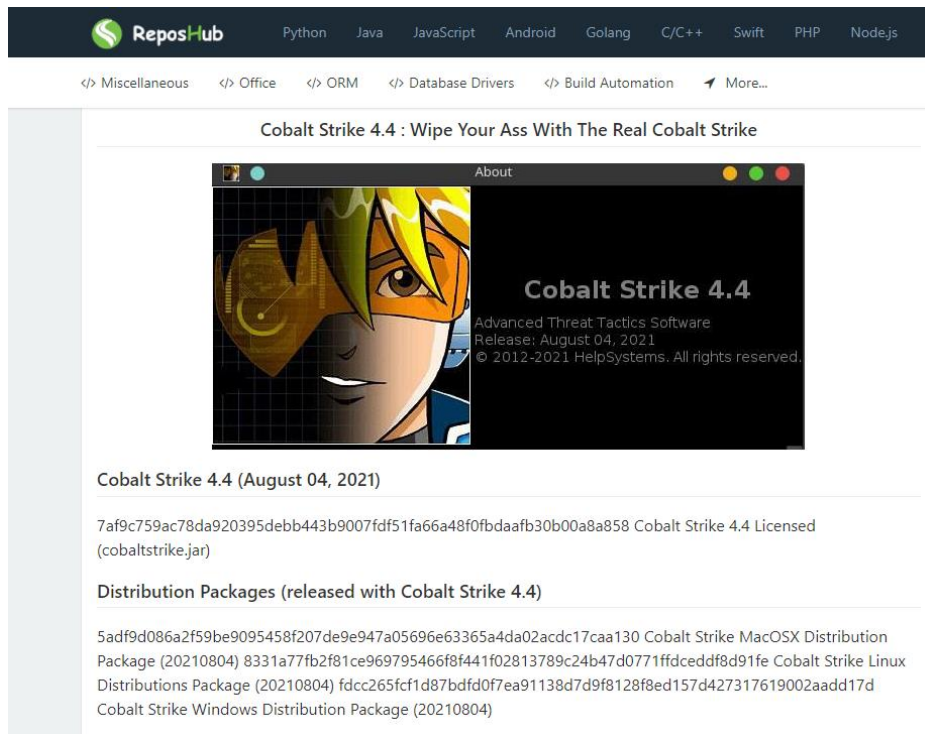





Cobalt Strike 4.4

Advanced Threat Tactics Software
Release: August 04, 2021

© 2012-2021 HelpSystems. All rights reserved.



Cobalt Strike 4.4 : Wipe Your Ass With The Real Cobalt Strike

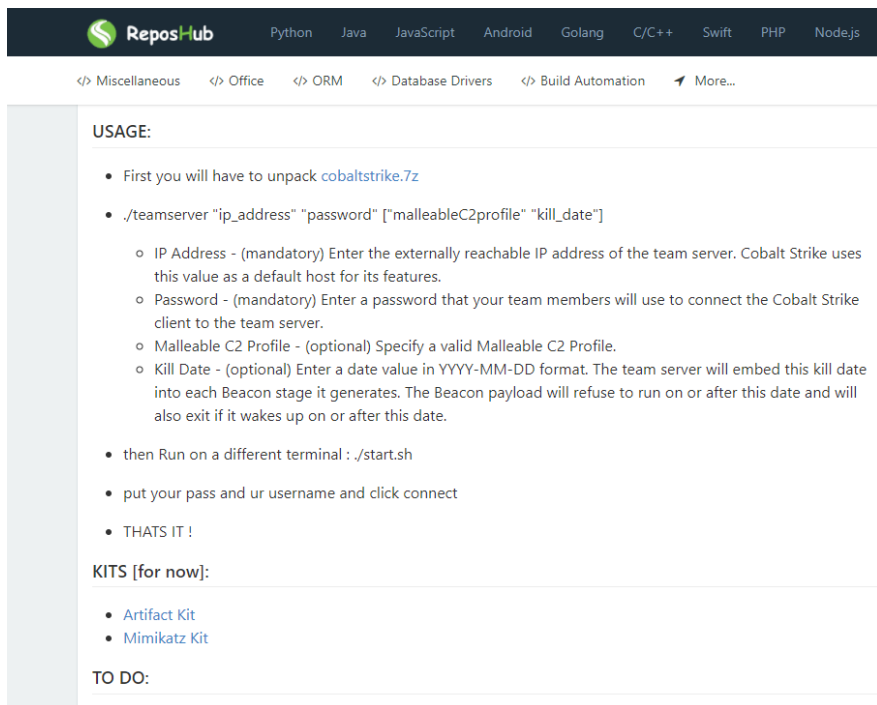


Cobalt Strike 4.4 (August 04, 2021)

7af9c759ac78da920395debb443b9007fd51fa66a48f0bdaafb30b00a8a858 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)



The screenshot shows a GitHub repository page for 'ReposHub'. The navigation bar includes links for Python, Java, JavaScript, Android, Golang, C/C++, Swift, PHP, and Node.js. Below the navigation bar, there are links for Miscellaneous, Office, ORM, Database Drivers, Build Automation, and More... The main content area is titled 'USAGE:' and contains a list of instructions for using Cobalt Strike. The instructions include unpacking 'cobaltstrike.7z', running a command to start the team server with various options (IP Address, Password, Malleable C2 Profile, Kill Date), and then running './start.sh' and clicking connect. Below the usage instructions, there is a section titled 'KITS [for now:]' with links for 'Artifact Kit' and 'Mimikatz Kit'. At the bottom, there is a section titled 'TO DO:'.

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:



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)

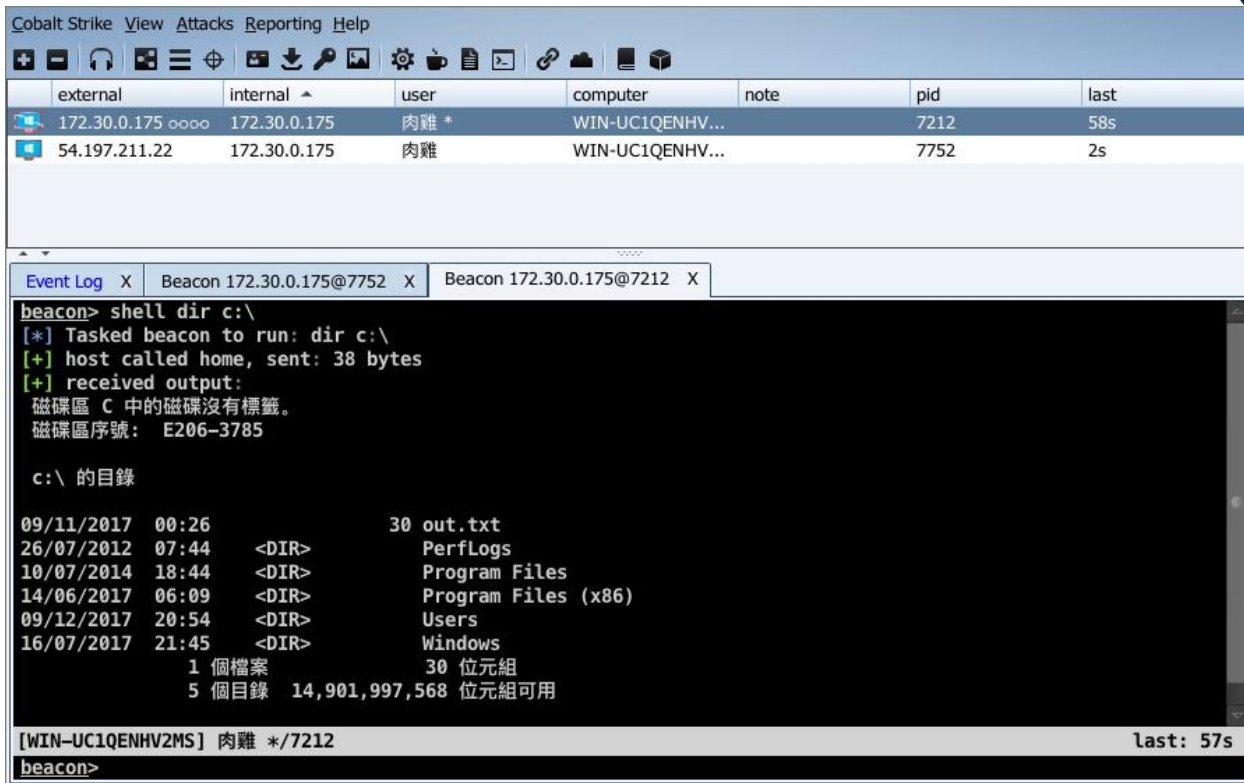
1.5 . 1 . **shell nltest / dclist:** <===== domain controllers



Team Server = C2 Server
Beacon = Bot

Team Server = Management Server
Beacon = Agent





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

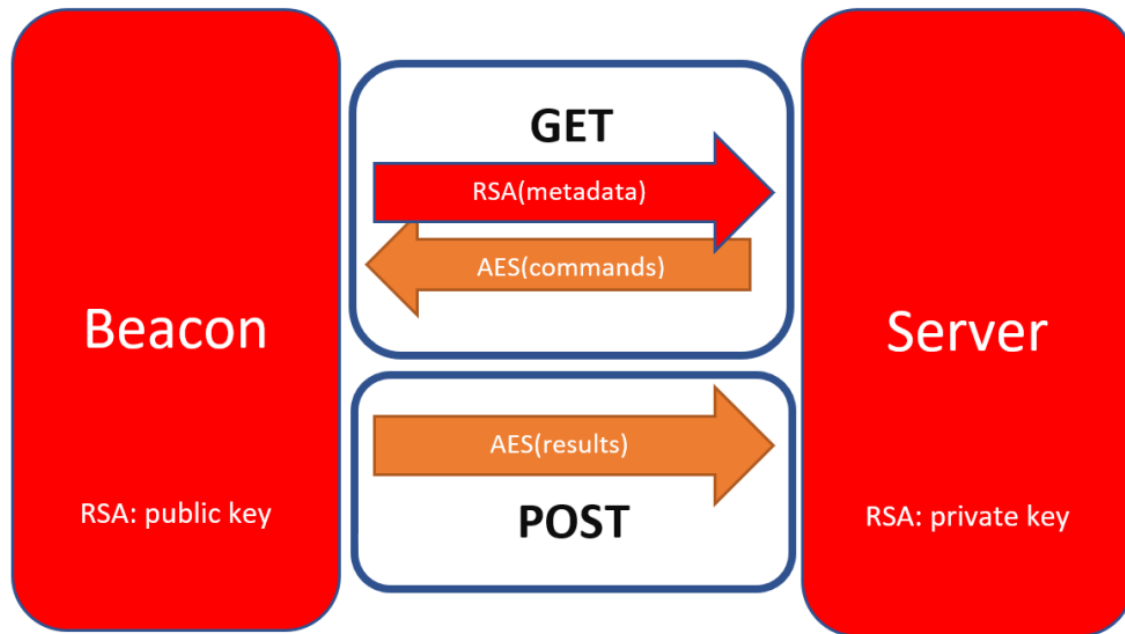
Event Log X Beacon 172.30.0.175@7752 X Beacon 172.30.0.175@7212 X

```
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>
```





NVISO Labs

Cyber security research, straight from the lab! 🐛



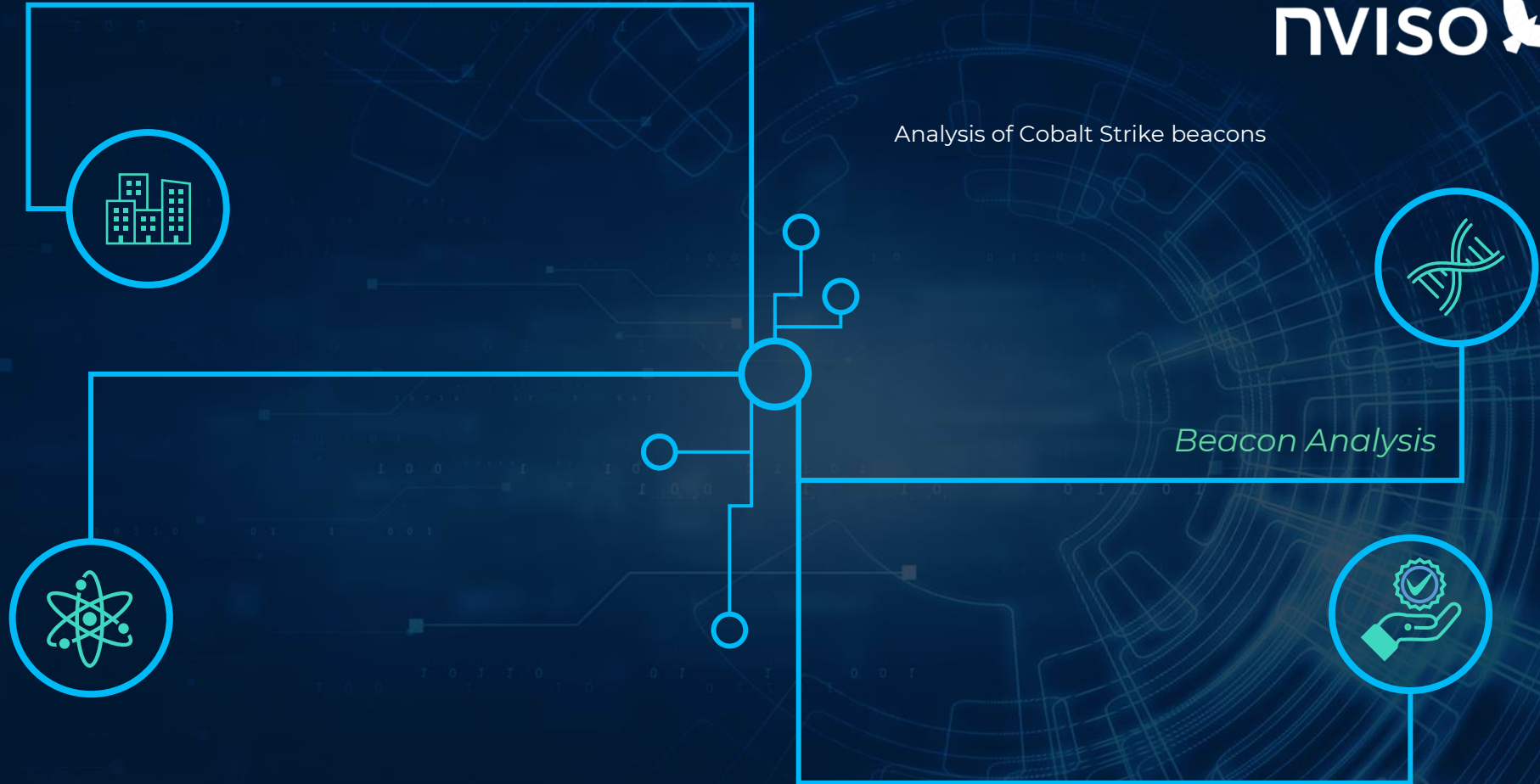
Cobalt Strike: Using Known Private Keys To Decrypt Traffic – Part 1

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

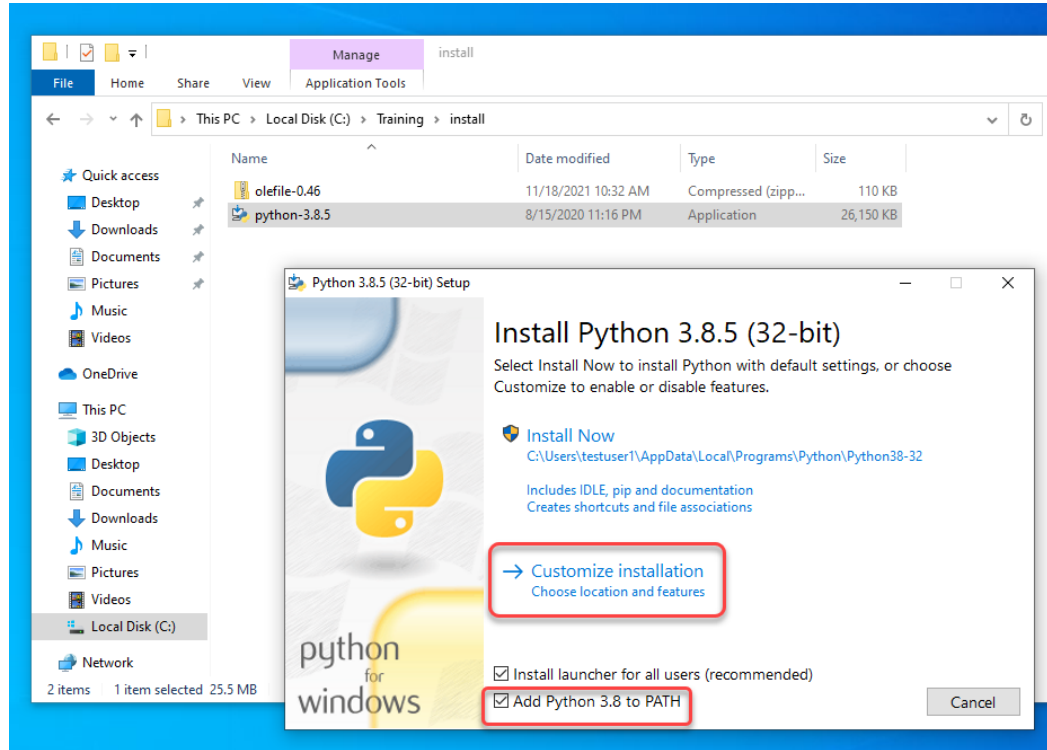
We found 6 private keys for rogue Cobalt Strike software, enabling C2 network traffic decryption.

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).

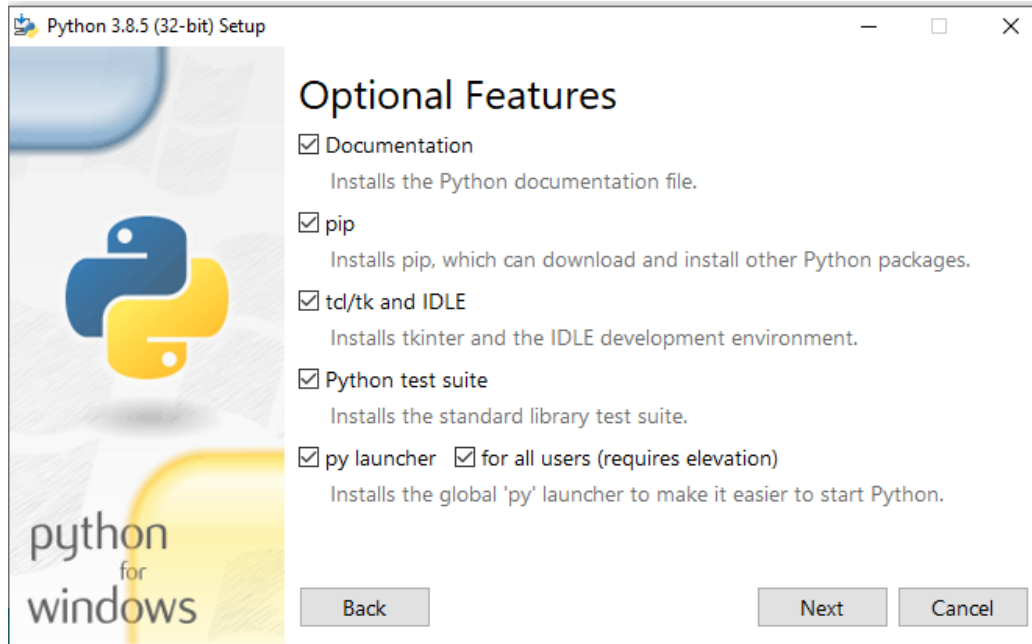
Analysis of Cobalt Strike beacons



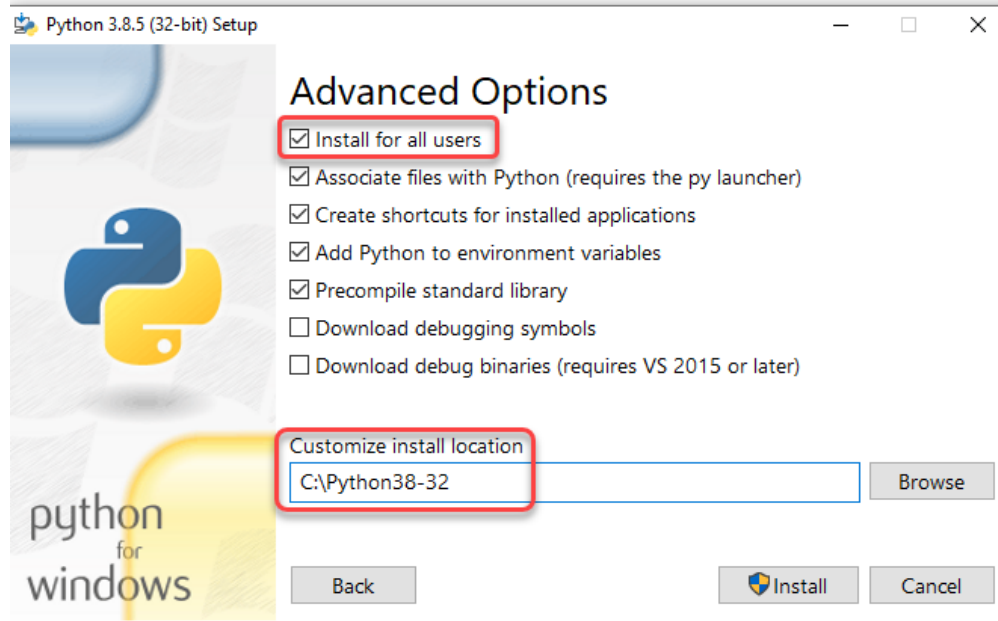
Beacon analysis



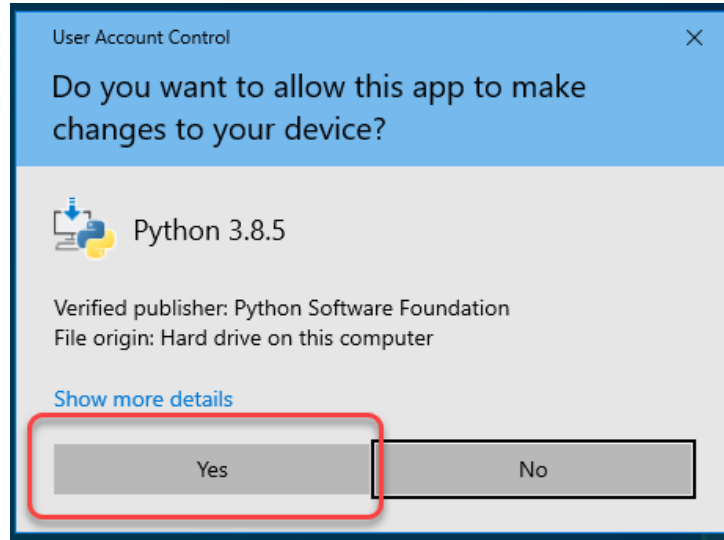
Beacon analysis



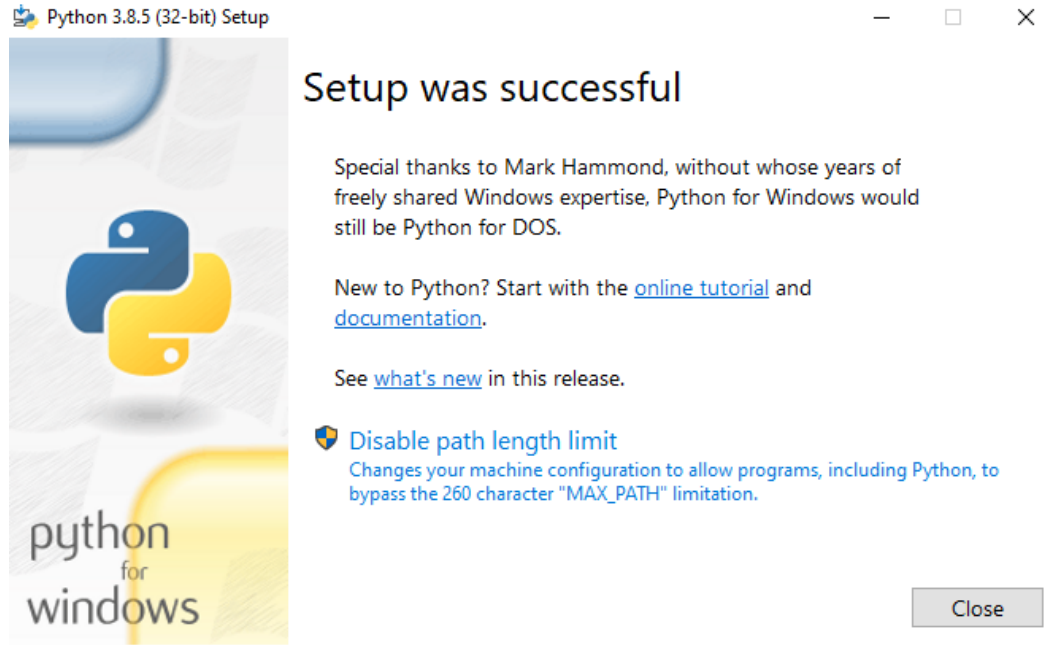
Beacon analysis



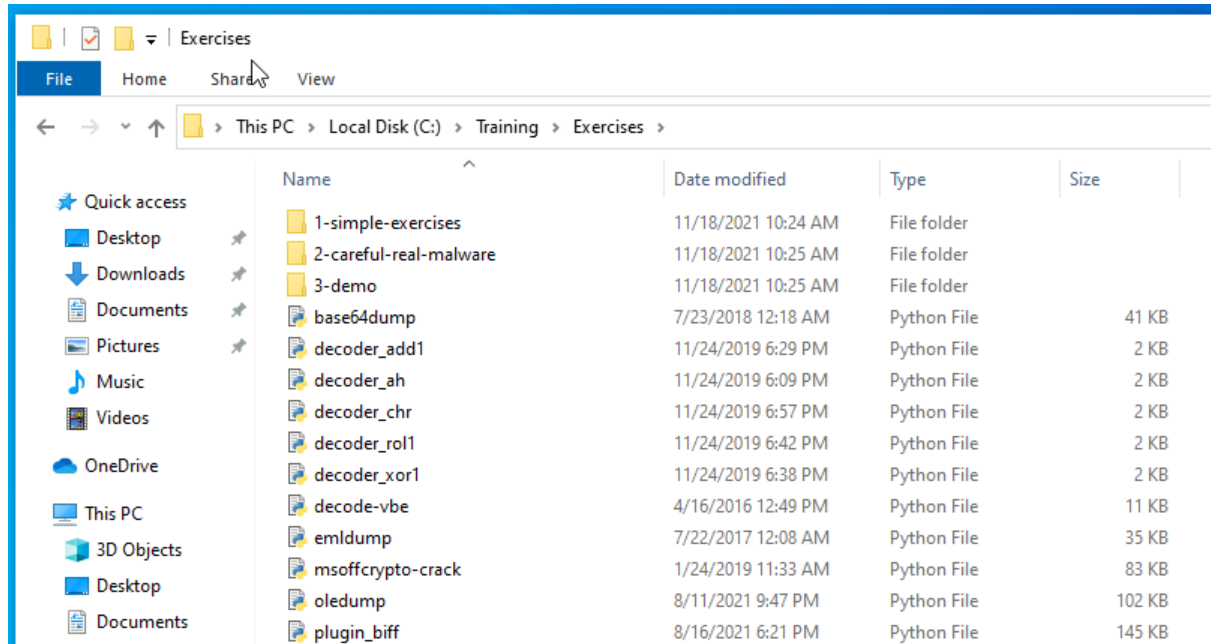
Beacon analysis



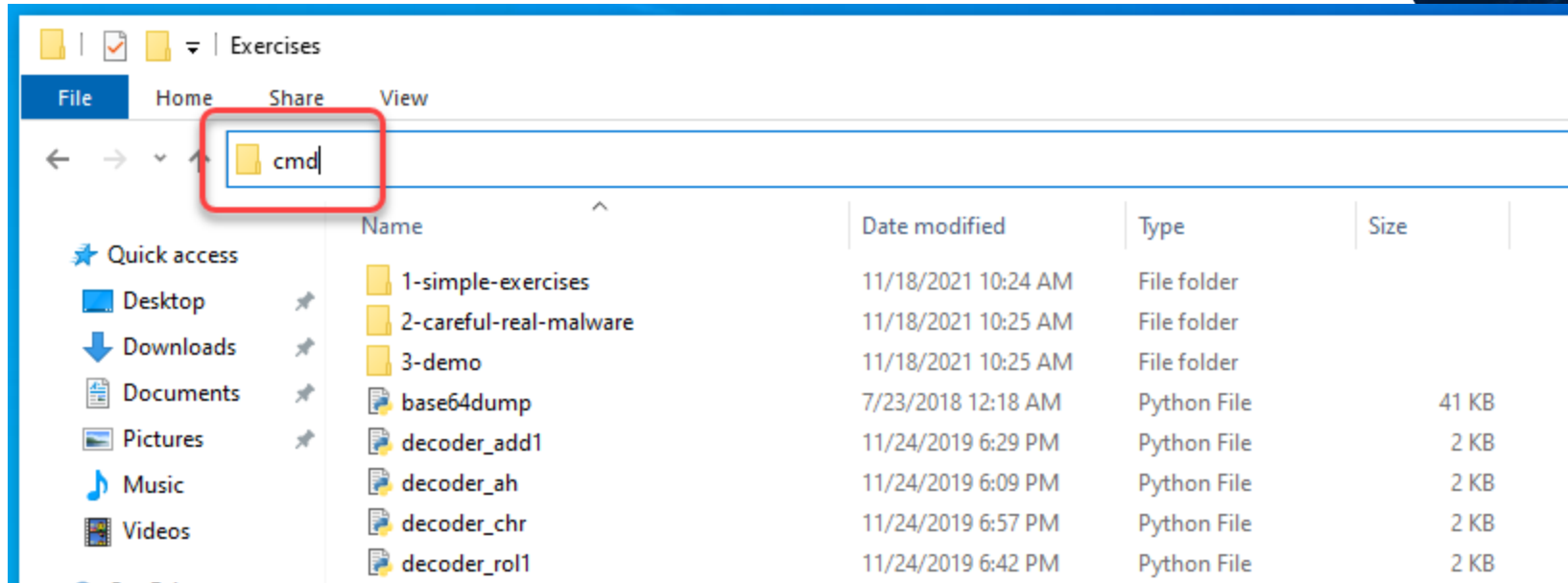
Beacon analysis



Beacon analysis



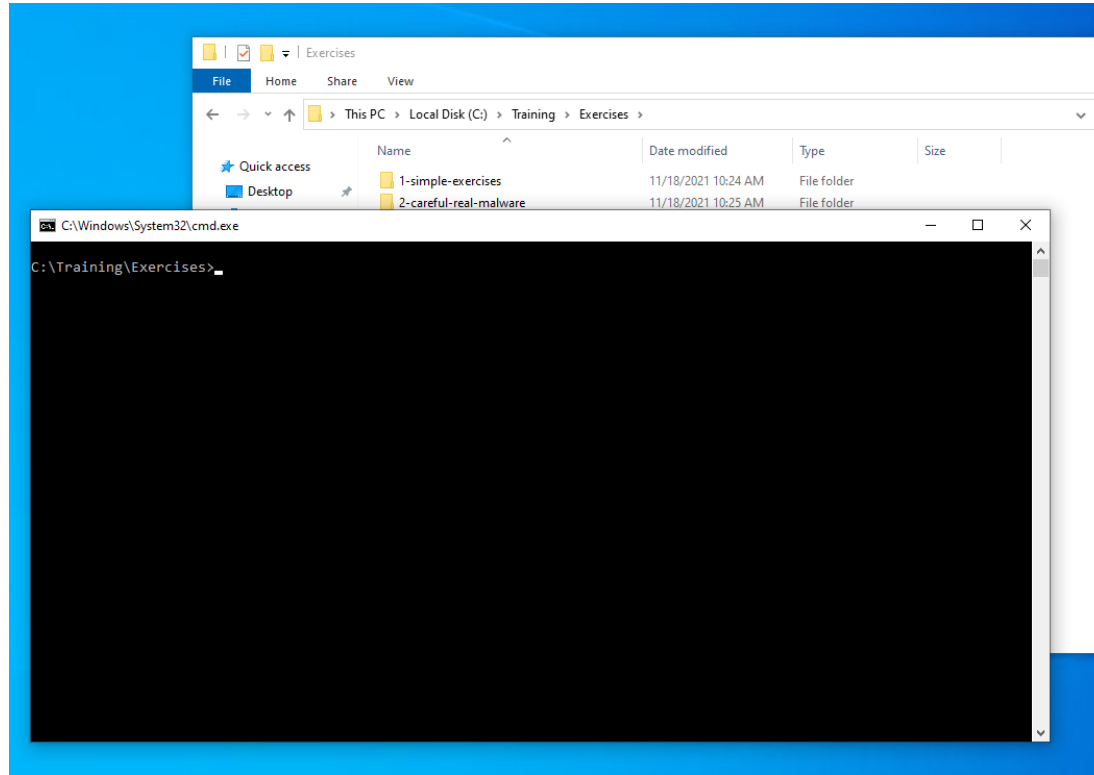
Beacon analysis



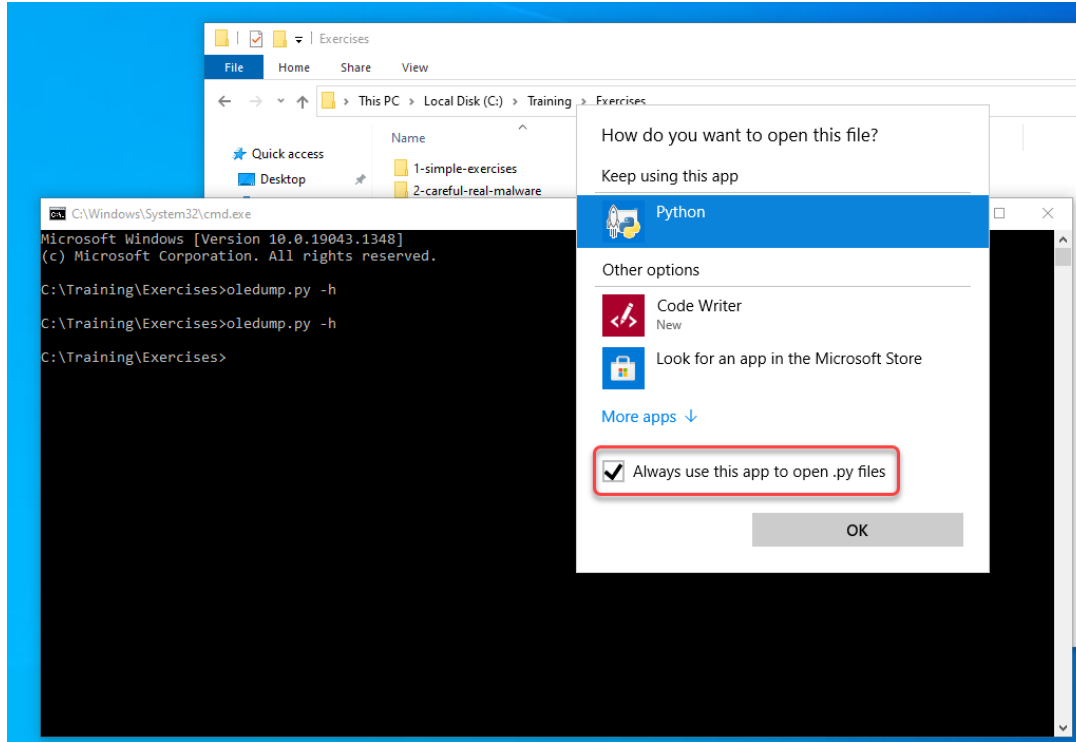
The screenshot shows a Windows File Explorer window titled 'Exercises'. The address bar contains the path 'cmd', which is highlighted with a red rectangular box. The main pane displays a list of files and folders:

Name	Date modified	Type	Size
1-simple-exercises	11/18/2021 10:24 AM	File folder	
2-careful-real-malware	11/18/2021 10:25 AM	File folder	
3-demo	11/18/2021 10:25 AM	File folder	
base64dump	7/23/2018 12:18 AM	Python File	41 KB
decoder_add1	11/24/2019 6:29 PM	Python File	2 KB
decoder_ah	11/24/2019 6:09 PM	Python File	2 KB
decoder_chr	11/24/2019 6:57 PM	Python File	2 KB
decoder_rol1	11/24/2019 6:42 PM	Python File	2 KB

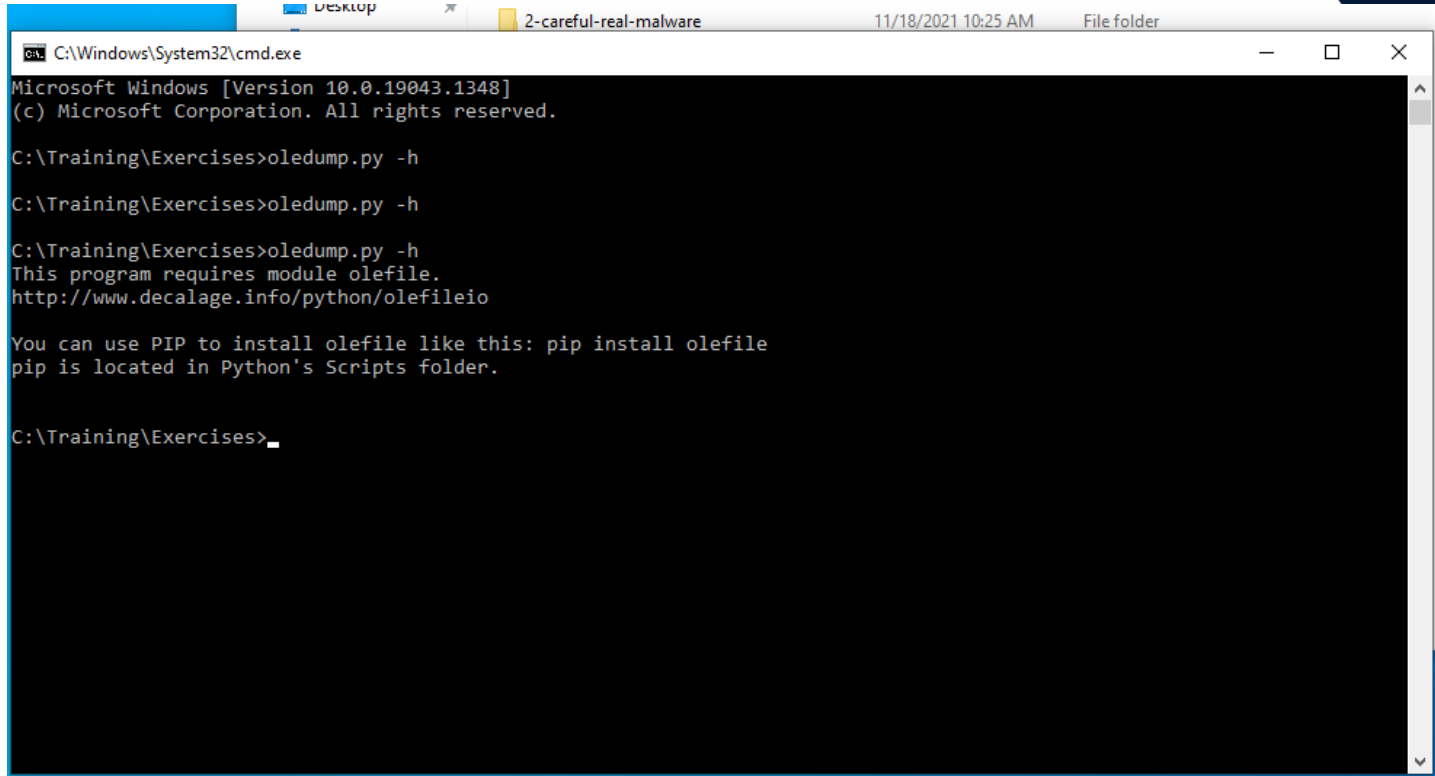
Beacon analysis



Beacon analysis



Beacon analysis



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19043.1348]
(c) Microsoft Corporation. All rights reserved.

C:\Training\Exercises>oledump.py -h

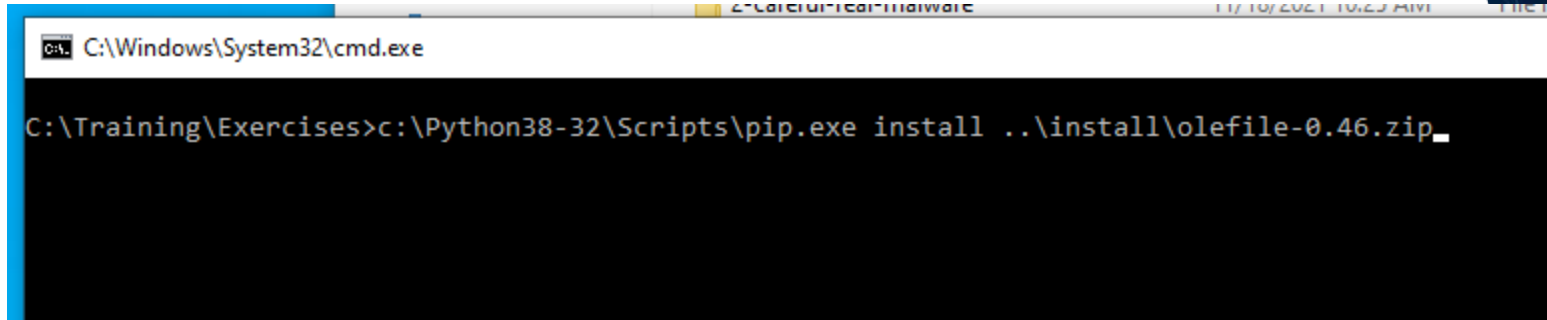
C:\Training\Exercises>oledump.py -h

C:\Training\Exercises>oledump.py -h
This program requires module olefile.
http://www.decalage.info/python/olefileio

You can use PIP to install olefile like this: pip install olefile
pip is located in Python's Scripts folder.

C:\Training\Exercises>_
```


Beacon analysis



```
C:\Windows\System32\cmd.exe  
C:\Training\Exercises>c:\Python38-32\Scripts\pip.exe install ..\install\olefile-0.46.zip_
```

Beacon analysis

```
C:\Windows\System32\cmd.exe

C:\Training\Exercises>c:\Python38-32\Scripts\pip.exe install ..\install\olefile-0.46.zip
Processing c:\training\install\olefile-0.46.zip
Using legacy setup.py install for olefile, since package 'wheel' is not installed.
Installing collected packages: olefile
  Running setup.py install for olefile ... done
Successfully installed olefile-0.46

C:\Training\Exercises>
```

Beacon analysis

```
C:\Windows\System32\cmd.exe

C:\Training\Exercises>c:\Python38-32\Scripts\pip.exe install ..\install\olefile-0.46.zip
Processing c:\training\install\olefile-0.46.zip
Using legacy setup.py install for olefile, since package 'wheel' is not installed.
Installing collected packages: olefile
  Running setup.py install for olefile ... done
Successfully installed olefile-0.46

C:\Training\Exercises>
```

Practical & Hands-on

1768.Py

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

Beacon analysis

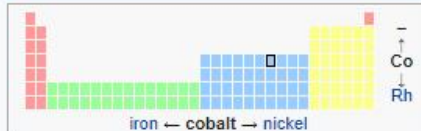
Cobalt, $_{27}\text{Co}$



Cobalt

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

Cobalt in the periodic table



iron ← cobalt → nickel

↑ Co
Rh

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

13:E7D0h:	00 00 00 00	00 00 00 00	00 01 00 00	00 00 00 00	00 00 00 00	00 00 00 00
13:E7E0h:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00y...Ou.
13:E7F0h:	00 00 00 00	00 01 00 00	00 FF 00 00	00 FF 00 00	00 30 75 00y...Ou.
13:E800h:	00 00 00 00	00 FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FFyyyyyyyyyy
13:E810h:	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF 00 00 00	yyyyyyyyyyyyyy
13:E820h:	00 00 00 00	00 2E 2F 2E	2F 2E 2C 2E	2F 2E 2C 2E	2F 2E 2C 2E	2F 2E 2C 2E/.../...
13:E830h:	2F 2E 2C 2E	1B 2E 2D 2E	2C 2E 2A 2E	2E 2E 5B 1E 2E-...É...[..
13:E840h:	2A 2E 2C 2E	2A 2E 0E 2B	CA 2E 2B 2E	2F 2E 2C 2E	*...*...É...+.../...
13:E850h:	33 2E 29 2E	2D 2F 2E 1E	AF B1 1E 23	28 27 04 8A	3...)/...±.#('...-
13:E860h:	66 A8 D9 23	2F 2F 2F 2B	3F 2D AF A3	2E 1E AF A7	f_U#///+...F..._§
13:E870h:	2C AF AF 2E	A7 E4 A7 4A	C3 7A 62 D5	D2 A7 48 F2\$§\$!zB00\$Hò
13:E880h:	07 26 0F 0A	A5 02 E6 DD	FA 4A 13 0E	13 98 00 AD8...Y...@YÚJ...X...
13:E890h:	50 C5 AF 60	46 39 AC B7	5A EA 0C 7F	6B FB 2A EF	PA^F9~+Zè...k0*i
13:E8A0h:	D9 72 25 7D	4D 5C 82 7C	5E 8D 77 3D	52 2D D1 A5	Ur%}WV... ^..w=R-Nÿ
13:E8B0h:	D3 42 E6 D5	F3 44 BA D1	63 05 F2 24	82 50 3F E9	OBa00D°Nc.ò\$ P?e
13:E8C0h:	E0 C7 A3 A5	48 05 5D 7E	28 F2 E1 F5	7F 97 FD 2E	àçE¥H.]- (0a0...-ý.
13:E8D0h:	4F B7 E6 2D	AA 61 F9 C0	7D ED C7 09	49 1F E6 CA	0·æ-^auA}iÇ.I.æÉ
13:E8E0h:	10 38 FB 7D	2B 2E D1 E8	50 17 AC 1F	3A 3F 32 6F8D)+.ÑèP...i?2o
13:E8F0h:	E6 5F 5E EF	2C 2D 2F 2E	2F 2E 2E 2E	2E 2E 2E 2E	æ^i,-/.../...
13:E900h:	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E
13:E910h:	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E
13:E920h:	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E
13:E930h:	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E
13:E940h:	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E
13:E950h:	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2D 2F	2E 59 4F 428...-/..YOB
13:E960h:	42 4B 5A 00	5A 46 4B 4A	4F 5C 45 4B	5D 5A 5D 47	BKZ.ZFKJ0AEK]Z]G
13:E970h:	4A 4B 00 41	5C 49 02 01	5D 4B 4F 5C	4D 46 01 2E	JK.A.I...]K0\MF...
13:E980h:	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E
13:E990h:	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E
13:E9A0h:	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E
13:E9B0h:	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E
13:E9C0h:	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E
13:E9D0h:	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E
13:E9E0h:	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E
13:E9F0h:	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E
13:EA00h:	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E
13:EA10h:	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E
13:EA20h:	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E
13:EA30h:	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E
13:EA40h:	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E
13:EA50h:	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2E	2E 2E 2E 2Em.
13:EA60h:	2F 2E 2C 2E	2E 2E 6A 2E	2C 2E 2A D1	D1 D1 D1 2Ej...*ÑNNN
13:EA70h:	6B 2E 2C 2E	2A D1 D1 D1	D1 2E 68 2E	2C 2E 2A D1	k...*NNNN.h...*Ñ
13:EA80h:	D1 D1 D1 2E	2D 2E 2D 2E	3E CD 7A 82	96 32 20 BC	NNN...->Iz,-2 ¼
13:EA90h:	46 8E 2B BF	1E EF 4A 3D	DD 2E 33 2E	2D 2E 6E 0B	FZ+z_i=¥.3...n.

Beacon analysis

```
13:E7D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
13:E7E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....y.....
13:E7F0h: 00 00 00 00 00 01 00 00 00 FF 00 00 00 30 75 00 .....y...ou.
13:E800h: 00 00 00 00 00 FF FF FF FF FF FF FF FF FF FF FF FF .....yyyyyyyyyy
13:E810h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF .....yyyyyyy.....
13:E820h: 00 00 00 00 00 00 01 00 01 00 02 00 01 00 02 00 .....5.....u0.
13:E830h: 01 00 02 00 25 00 03 00 02 00 04 00 00 75 30 00 .....ä.....
13:E840h: 04 00 02 00 04 00 20 05 F4 00 05 00 01 00 02 00 .....0.Y0...*t
13:E850h: 1D 00 07 00 03 01 00 30 81 9F 30 0D 06 09 2A 86 HI+.....0.%
13:E860h: 48 86 F7 0D 01 01 01 05 00 03 81 8D 00 30 81 89 .....%&diTLöü&fÜ
13:E870h: 02 81 81 00 89 CA 89 64 ED 54 4C FB FC 89 66 DC .....$.Eo0d= =v5f
13:E880h: 99 08 91 24 8B 2C C8 F3 D4 64 3D 20 3D 76 A7 83 ~è.Nh.,*tA"QEO.A
13:E890h: 7E EB 81 4E 68 17 82 99 74 C4 22 51 45 D5 04 C1 =\,Scr~RpEY.|.y+
13:E8A0h: F7 5C 0B 53 63 72 AC 52 70 A3 59 13 7C 03 FF 8B y1E0Yj"yM+U.~.ç
13:E8B0h: FD 6C C8 FB DD 6A 94 FF 4D 2B DC 0A AC 7E 11 C7 Ié.(f+sP.UIU0'0.
13:E8C0h: CE E9 8D 8B 66 2B 73 50 06 DC CF DB 51 B9 D3 00 a"ME...0xISAé'g1Ea
13:E8D0h: 61 99 C8 03 84 4F D7 EE 53 C3 E9 27 67 31 C8 E4 >.0S...y&-9,1...A
13:E8E0h: 3E 16 D5 53 05 00 FF C6 7E 39 82 31 14 11 1C 41 EqpÁ.....
13:E8F0h: C8 71 70 C1 02 03 01 00 01 00 00 00 00 00 00 00 .....
13:E900h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
13:E910h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
13:E920h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
13:E930h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
13:E940h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
13:E950h: 00 00 00 00 00 00 00 00 08 00 03 01 00 77 61 6C .....wal
13:E960h: 6C 65 74 2E 74 68 65 64 61 72 6B 65 73 74 73 69 let.thedarkestsI
13:E970h: 64 65 2E 6F 72 67 2C 2F 73 65 61 72 63 68 2F 00 de.org./search/.
13:E980h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
13:E990h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
13:EA00h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
13:EA10h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
13:EA20h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
13:EA30h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
13:EA40h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
13:EA50h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 43 00 .....C.
13:EA60h: 01 00 02 00 00 00 44 00 02 00 04 FF FF FF FF 00 .....D...yyyy.
13:EA70h: 45 00 02 00 04 FF FF FF FF FF 00 46 00 02 00 04 FF E....yyyy.F....y
13:EA80h: FF FF FF 00 0E 00 03 00 10 E3 54 AC B8 1C 0E 92 yyy.....âT...
13:EA90h: 68 A0 05 91 30 C1 8A 13 F3 00 1D 00 03 00 40 25 h.'0AS.6.....@%
```


Beacon analysis

```
C:\WINDOWS\system32\cmd.exe
0x0006 maxdns 0x0001 0x0002 245
0x0013 DNS_Idle 0x0002 0x0004 134743044 8.8.4.4
0x0014 DNS_Sleep 0x0002 0x0004 10000
0x003c DNS_beacon 0x0003 0x0021 (NULL ...)
0x003d DNS_A 0x0003 0x0021 'cdn.'
0x003e DNS_AAAA 0x0003 0x0021 'www6.'
0x003f DNS_TXT 0x0003 0x0021 'api.'
0x0040 DNS_metadata 0x0003 0x0021 'www.'
0x0041 DNS_output 0x0003 0x0021 'post.'
0x0042 DNS_resolver 0x0003 0x000f (NULL ...)
0x0036 HostHeader 0x0003 0x0080 (NULL ...)
0x0032 UsesCookies 0x0001 0x0002 1
0x0023 proxy_type 0x0001 0x0002 2 IE settings
0x003a TCP_FRAME_HEADER 0x0003 0x0080 '\x00\x04'
0x0039 SMB_FRAME_HEADER 0x0003 0x0080 '\x00\x04'
0x0037 EXIT_FUNK 0x0001 0x0002 0
0x0028 killdate 0x0002 0x0004 0
0x0029 textSectionEnd 0x0002 0x0004 0
0x002b process-inject-start-rwx 0x0001 0x0002 64 PAGE_EXECUTE_READWRITE
0x002c process-inject-use-rwx 0x0001 0x0002 32 PAGE_EXECUTE_READ
0x002d process-inject-min_alloc 0x0002 0x0004 4096
0x002e process-inject-transform-x86 0x0003 0x0100 '\x00\x00\x00\x04MZ\x90\x00\x00\x00\x04f!Th'
0x002f process-inject-transform-x64 0x0003 0x0100 '\x00\x00\x00\x04MZ\x90\x00\x00\x00\x04f!Th'
0x0035 process-inject-stub 0x0003 0x0010 '"+\x8f'\0B\x8dYU\x9ei4~!H'
0x0033 process-inject-execute 0x0003 0x0080 '\x06\x10\x00\x00\x00\x00\nntd11.dll\x00\x00\x00\x00\x13RtlUserThreadStart\x00\x07\x10\x00\x00\x00\x00\rkernel32.dll\x00\x00\x00\x00\rLoadLibraryA\x00\x02\x08\x05\x04'
0x0034 process-inject-allocation-method 0x0001 0x0002 1
0x0000
Guessing Cobalt Strike version: 4.3 (max 0x0046)
Sleep mask 64-bit 4.2 deobfuscation routine found.
C:\demo\the_compromise>
```

Exercise 01: beacon.exe

Exercise 02: VBA maldoc with shellcode

Exercise 03:

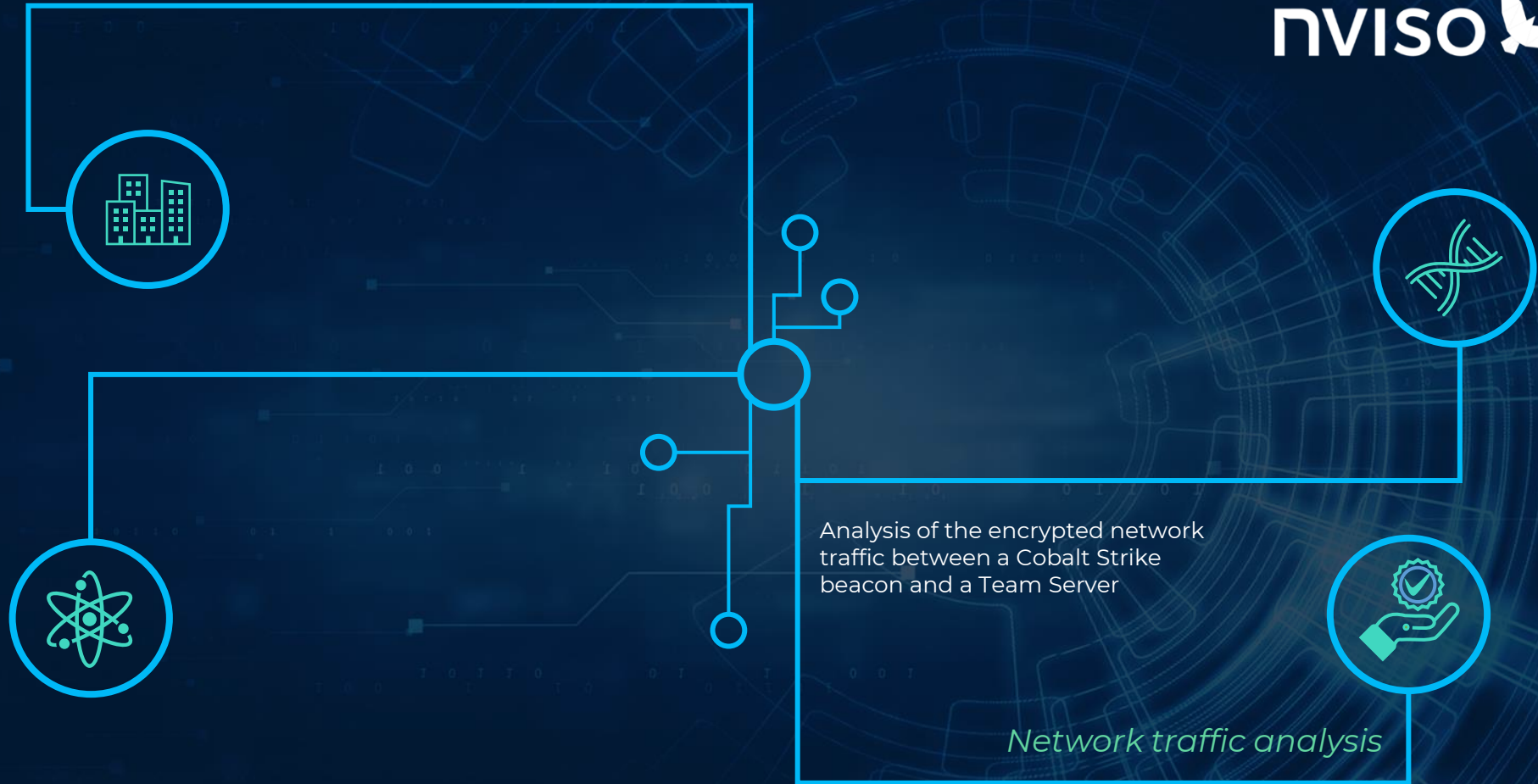
Excel 4 macros with shellcode

Exercise 04: Stager shellcode & beacon

Exercise 05: PowerShell & Shellcode

Exercise 06: Process Memory Dump

Exercise 07: Packed/Protected Beacon





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).

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

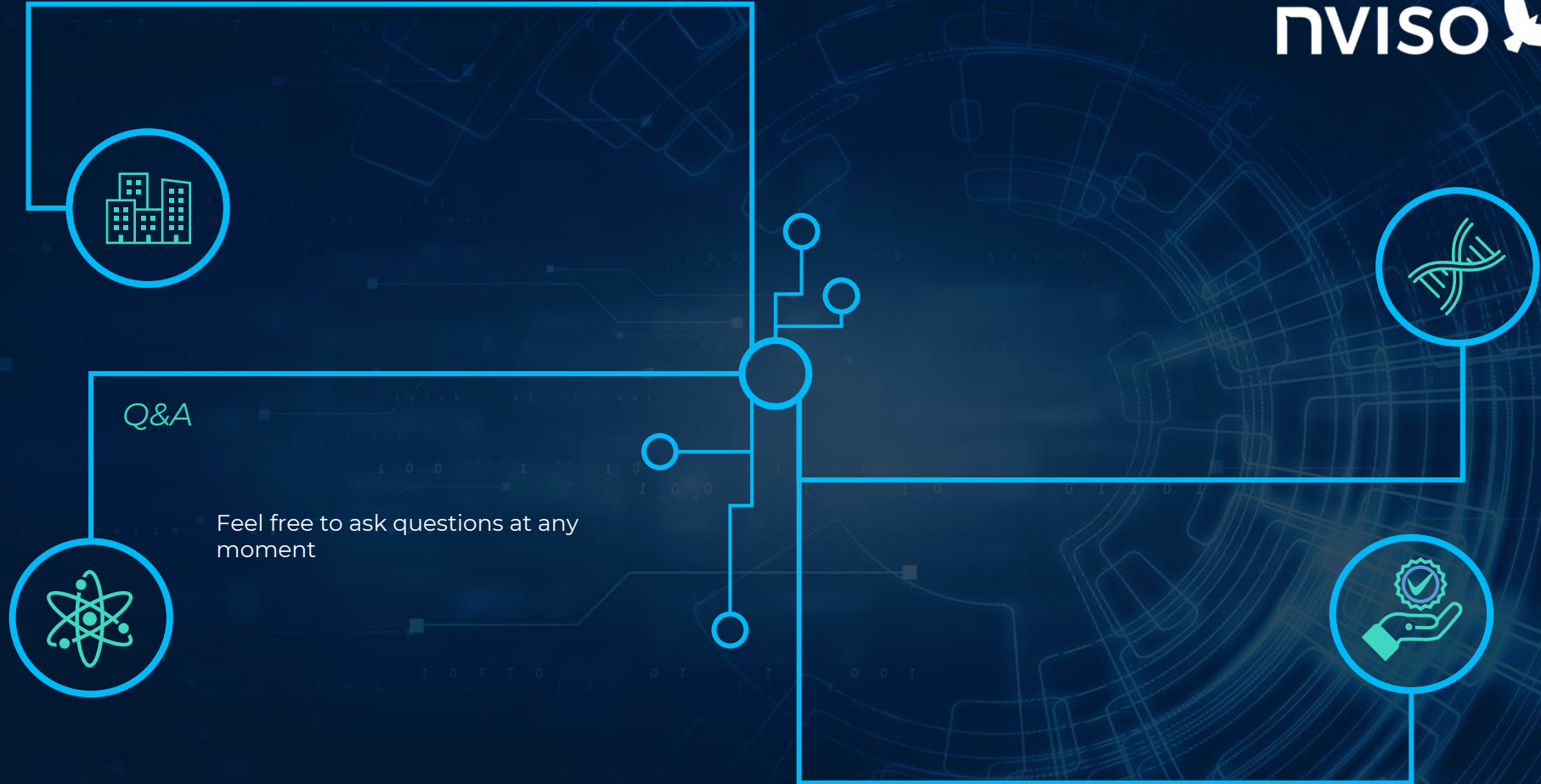
Exercise 14: Data Transforms

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

solutions.txt