

Malware Reweaponization

case study

Kārlis Podiņš, CERT.LV

Executive Summary



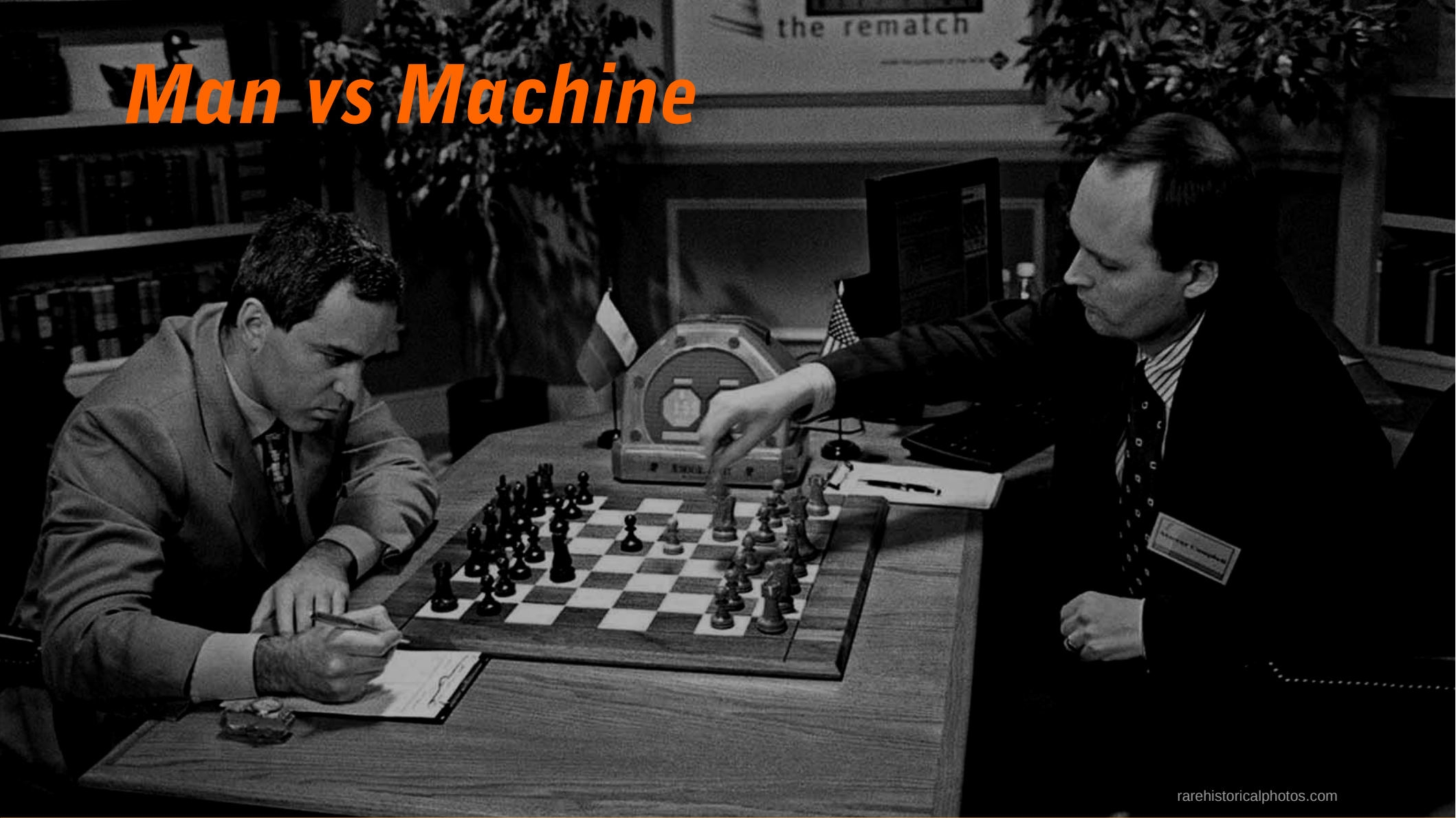


Context

- Vincent R. Stewart, DIA Chief, 2017
 - “Once we've isolated malware, I want to reengineer it and prep to use it against the same adversary who sought to use against us”
- Wikileaks
 - “The UMBRAGE team maintains a library of application development techniques borrowed from in-the-wild malware”

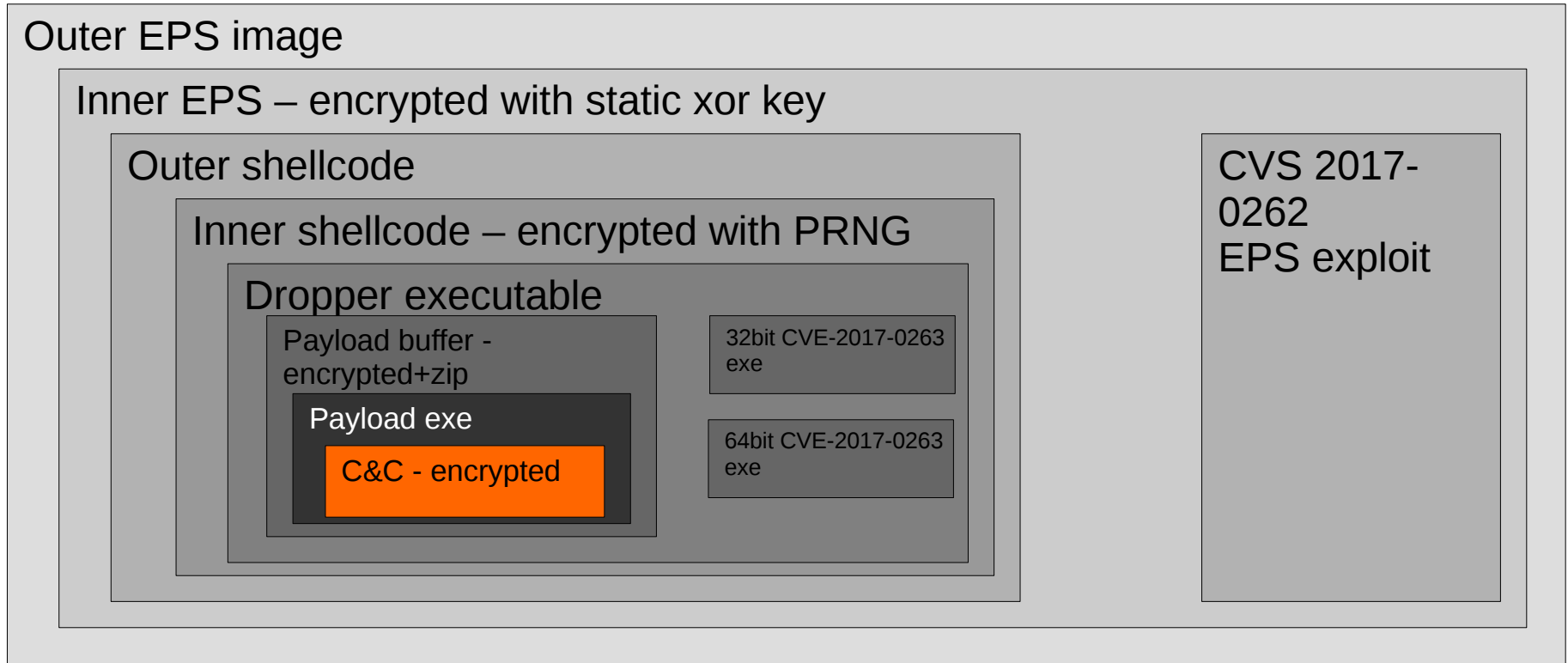


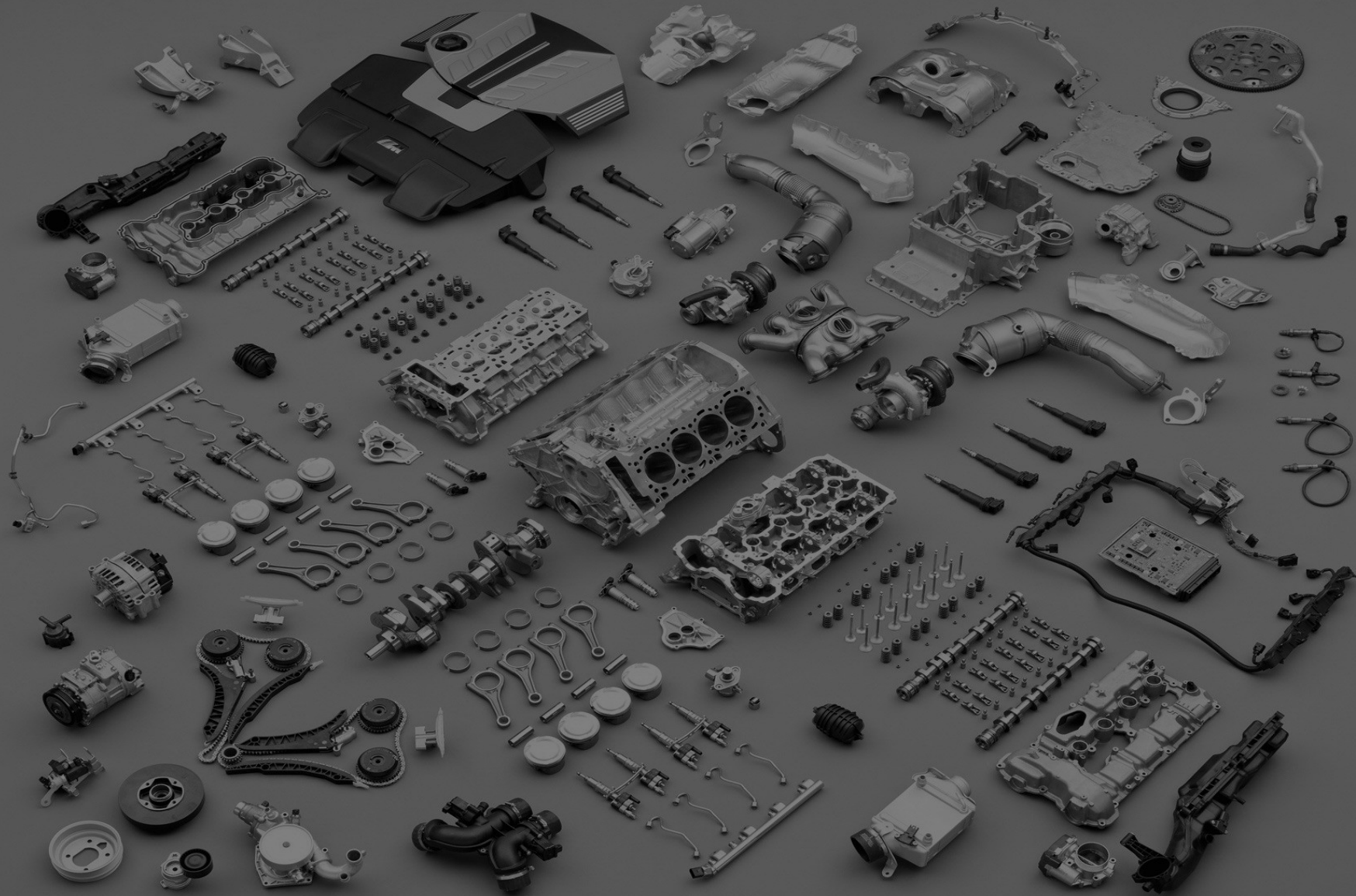
Man vs Machine



Malware Architecture

Office document – zip archive









Challenges

Office document – zip archive

Outer EPS image

Inner EPS – **encrypted** with static xor key

Outer shellcode

Inner shellcode – **encrypted** with PRNG

Dropper executable

Payload buffer -
encrypted+zip

Payload exe

C&C - **encrypted**

32bit CVE-2017-0263
exe

64bit CVE-2017-0263
exe

CVS 2017-
0262
EPS exploit

Reobfuscation

- Perfect symmetry
- Known algorithms
- Reimplementation
- One-time pad generation
 - Keystream not affected by input





PoC

- > python reweaponize.py new.c2

The image shows a Wireshark network traffic capture window titled "Local Area Connection 2". The main pane displays a list of DNS packets. The selected packet (No. 6) is a query from source 10.0.2.15 to destination 85.254.193.137. The packet details pane shows the following structure:

- Frame 683: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface 0
- Ethernet II, Src: PcsCompu_85:c5:cd (08:00:27:85:c5:cd), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 85.254.193.137
- User Datagram Protocol, Src Port: 52958, Dst Port: 53
- Domain Name System (query)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 52 54 00 12 35 02 08 00 27 85 c5 cd 08 00 45 00  RT..5... '.....E.
0010 00 37 24 f8 00 00 80 11 00 00 0a 00 02 0f 55 fe  .7$.....U.
0020 c1 89 ce de 00 35 00 23 23 cb 72 0e 01 00 00 01  .....5.# #.r....
0030 00 00 00 00 00 00 05 63 79 63 6f 6e 03 6f 72 67  .....c ycon.org
0040 00 00 01 00 01  .....
```

The status bar at the bottom indicates "Domain Name System: Protocol" and "Packets: 11474 · Displayed: 84 (0.7%)".

Reweaponization Choices

Office document – zip archive

Outer EPS image

Inner EPS – encrypted with static xor key

Outer shellcode

Inner shellcode – encrypted with PRNG

Dropper executable

Payload buffer -
encrypted+zip

Payload exe

C&C - encrypted

32bit CVE-2017-0263
exe

64bit CVE-2017-0263
exe

CVS 2017-
0262
EPS exploit

Attribution



Threshold



Sky is Not Falling





Paldies!