

a8=Q

Reweaponization of a Malware Sample

Kārlis Podiņš, CERT.LV

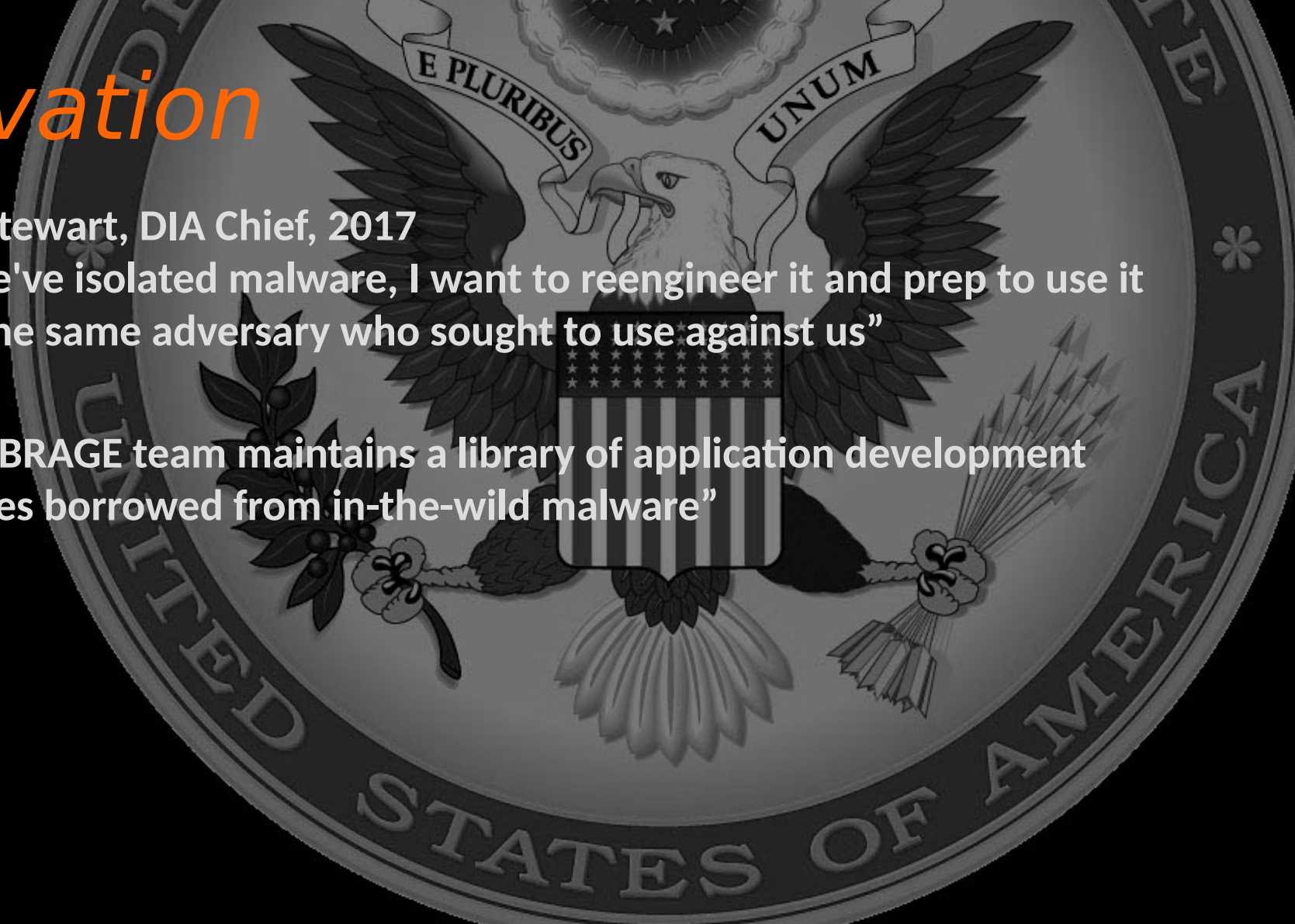
a8=Q





Motivation

- 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”

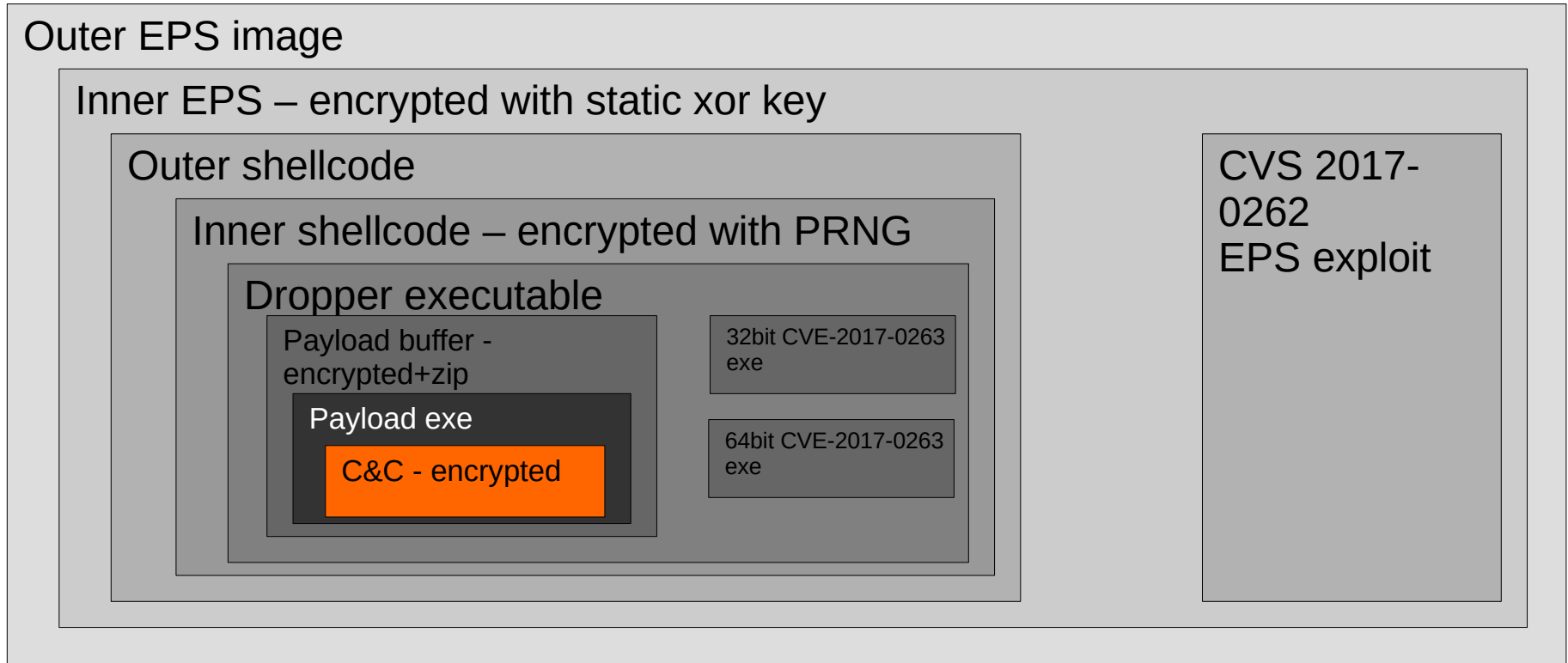


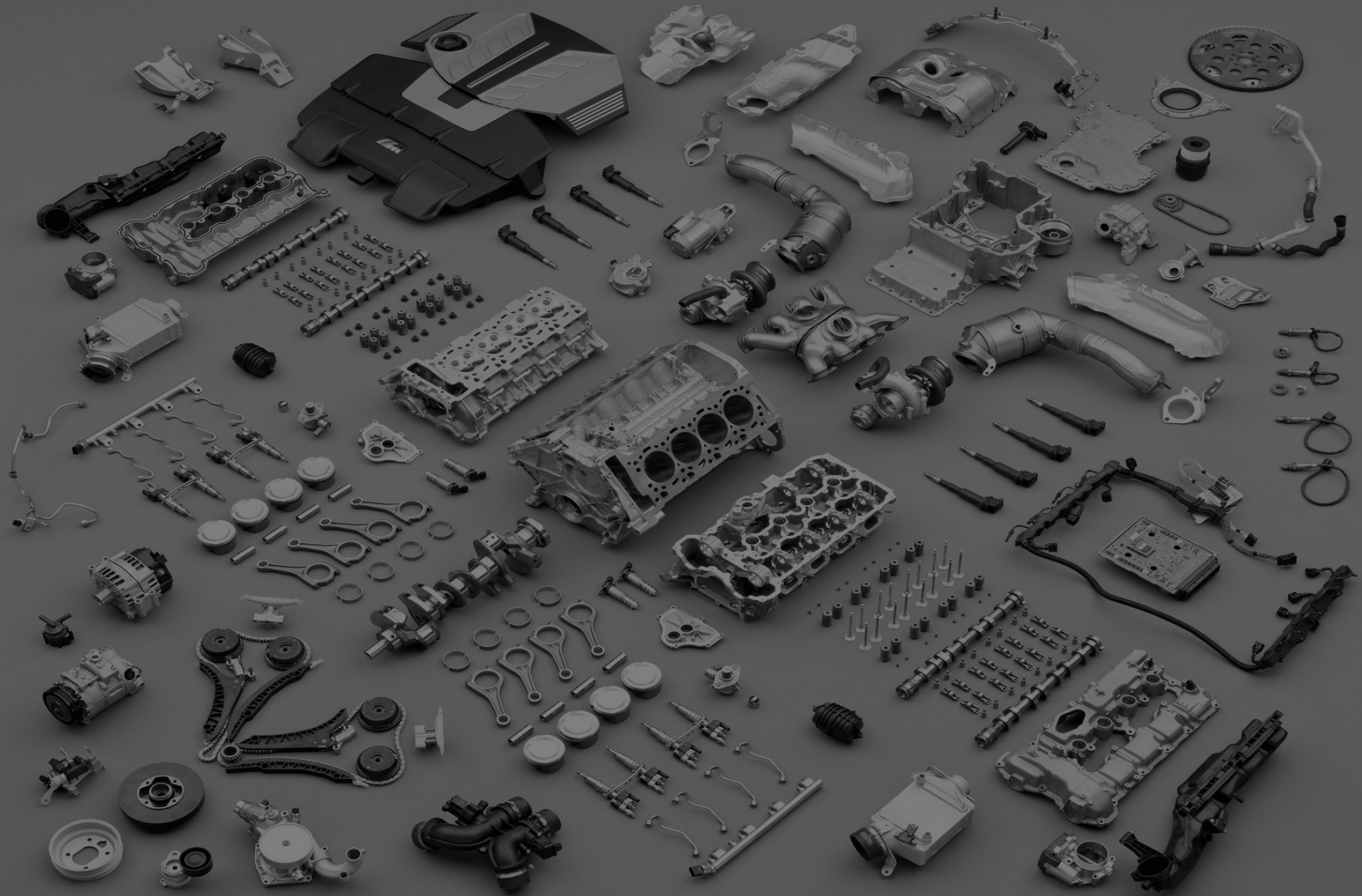
Man vs Machine



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 screenshot shows a Wireshark capture of network traffic on a Local Area Connection 2. The main pane displays a list of DNS packets. The selected packet (No. 683) is a query from 10.0.2.15 to 85.254.193.137 for the domain cycon.org. The packet details pane shows the structure of the DNS query, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). The packet bytes pane shows the raw hex and ASCII data of the query.

No.	Time	Source	Destination	Protocol	Length	Info
6...	24.043...	85.254.193...	10.0.2.15	DNS	222	Standard query response 0xec09 A google.com A 172.217.20.174 N...
6...	24.578...	10.0.2.15	85.254.193...	DNS	85	Standard query 0x9fae A roaming.officeapps.live.com
6...	24.613...	85.254.193...	10.0.2.15	DNS	47	Standard query response 0x9fae A roaming.officeapps.live.com C...
6...	24.931...	10.0.2.15	85.254.193...	DNS	85	Standard query 0xcdb1 A teredo.ipv6.microsoft.com
6...	24.982...	85.254.193...	10.0.2.15	DNS	140	Standard query response 0xcdb1 No such name A teredo.ipv6.micr...
6...	25.498...	10.0.2.15	85.254.193...	DNS	69	Standard query 0x720e A cycon.org
6...	25.795...	85.254.193...	10.0.2.15	DNS	200	Standard query response 0x720e A cycon.org A 104.25.137.98 A 1...
1...	26.014...	10.0.2.15	85.254.193...	DNS	77	Standard query 0x4372 A ocsip.digicert.com
1...	26.015...	85.254.193...	10.0.2.15	DNS	249	Standard query response 0x4372 A ocsip.digicert.com CNAME cs9.w...
1...	26.144...	10.0.2.15	85.254.193...	DNS	75	Standard query 0x97bc A ocsip.msocsp.com
1...	26.244...	10.0.2.15	85.254.193...	DNS	70	Standard query 0x6fb9 A ccdcoe.org

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)

```
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  ....
```

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... Yet





Paldies!