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

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

32bit CVE-2017-0263 exe

64bit CVE-2017-0263 exe

C&C - encrypted

CVS 2017-0262
EPS exploit
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
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

32bit CVE-2017-0263 exe

64bit CVE-2017-0263 exe

C&C - encrypted

CVS 2017-0262
EPS exploit
Attribution

By Chris J., Flickr
Threshold
Sky is Not Falling
Paldies!