a8=Q

Reweaponization of a Malware Sample

Kārlis Podiņš, CERT.LV


a8=Q

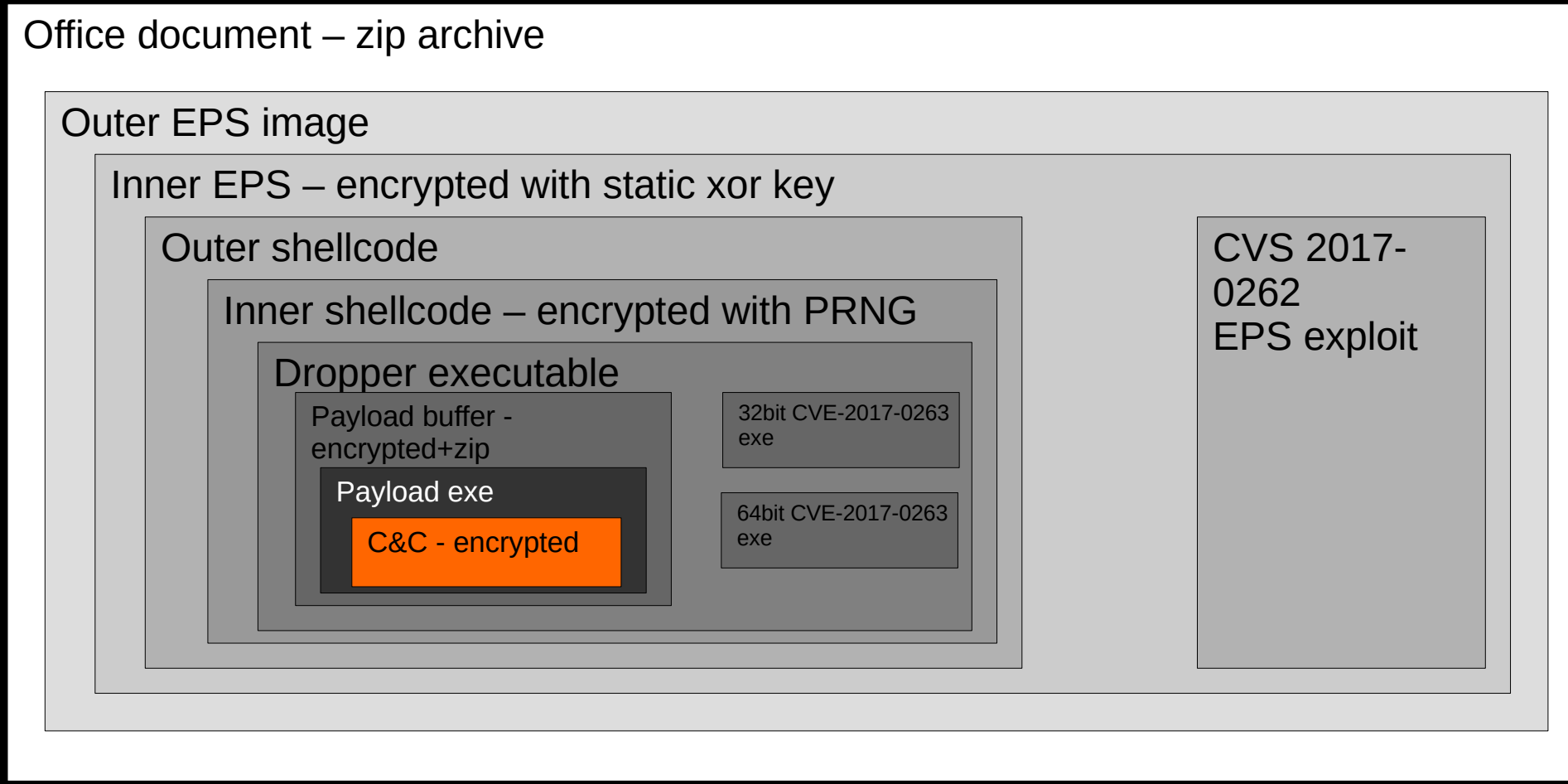

Bishop
Arensburg
Pernau
Fellin
Livonian
Order
Dorpat
Peipus
1242
Republic of No
Pskov
Bishopric of
Dorpat
Gulf of Riga
Bishopric of Courland
Windau
Piltene
Wolmar
Treiden
Riga
Goldingen
Archbishopric of
Riga
Livonian Order
Ascheraden
Durbe
1260
Kokenhusen
Saule

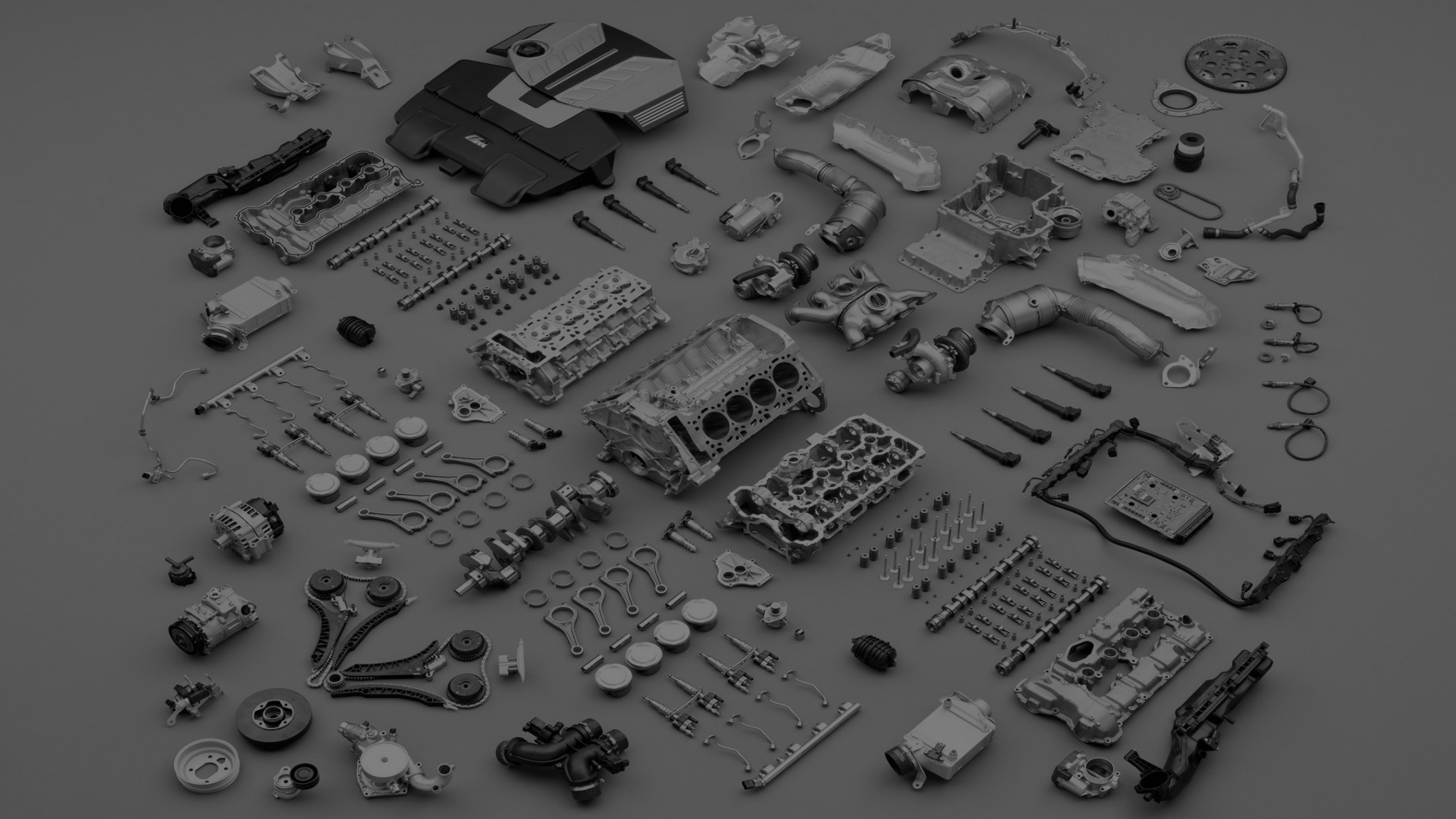
Motivation

- 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

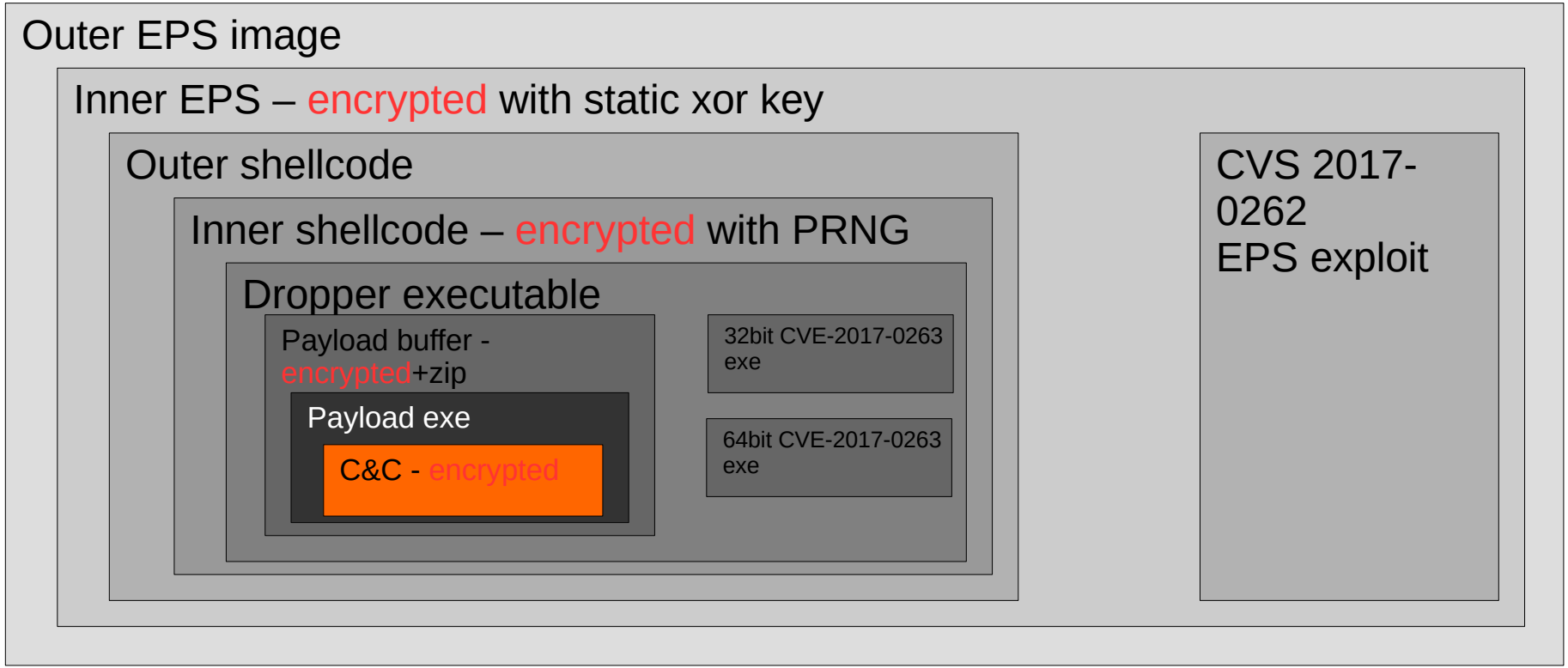
Malware Architecture





Challenges

Office document – zip archive



Reobfuscation

- Perfect symmetry

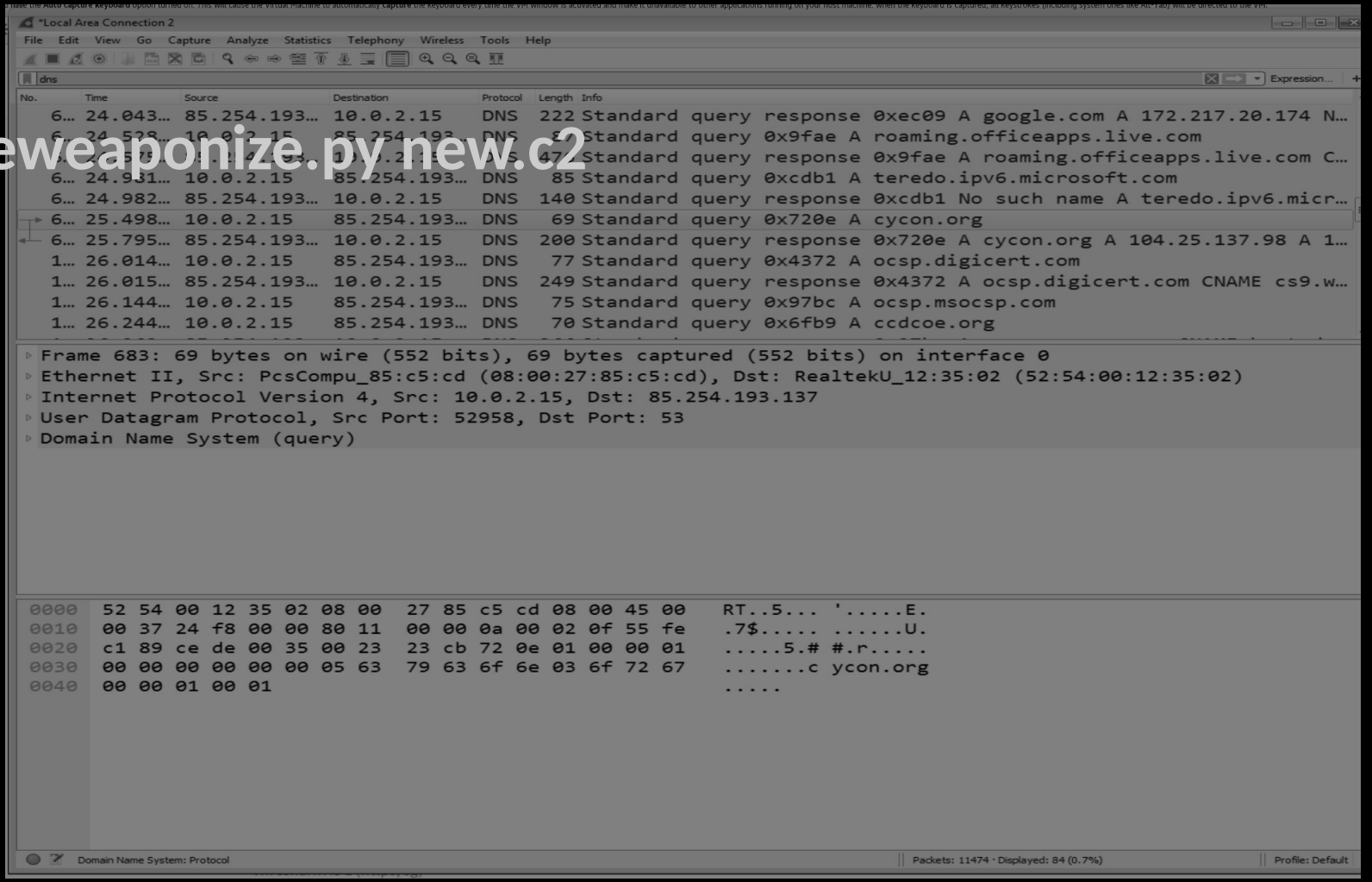
- Known algorithms
- Reimplementation
- One-time pad generation
  - Keystream not affected by input

Lee Barrows, Flickr

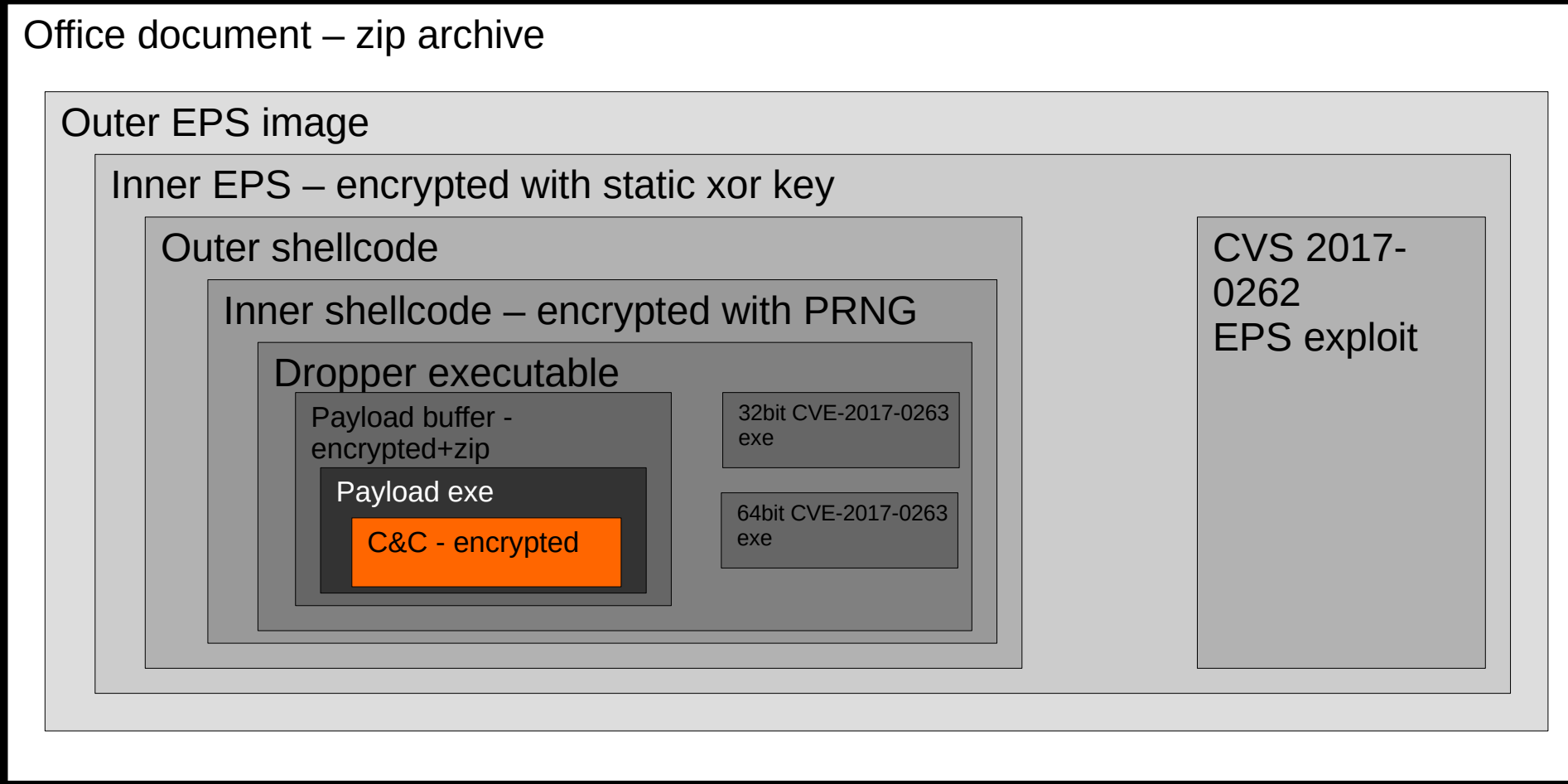
Monique Sherrett (Trottier), Flickr

PoC

- > python reweaponize.py new.c2



Reweaponization Choices



Attribution

By Chris JL, Flickr

Threshold

stipriem.lv


Sky is Not Falling...Yet


Paldies!