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

Kenneth Geers  
Senior Research Scientist, 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”
WhoAmI: CERT-Latvia
Russia

FancyBear
CozyBear
WhiteBear
VenomousBear
YouNameItBear
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
$ 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

Outer shellcode

Inner shellcode – encrypted with PRNG

Custom crypto reimplemented

One-time pad generation

Xor cipher with static key

Dropper - exe
Payload buffer - encrypted
Payload buffer – ZIP compressed
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
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

 CVE-2017-0261
EPS exploit

32bit
CVE-2017-0262
EOP

64 bit
CVE-2017-0263
EOP
Python replaceCnC.py cycon\org [epsOutputFile]
Re-weaponization Choices

False Flag

![Graph showing False Flag and Complexity]

- Shellcode
- Payload
- C&C
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