2018 西湖论剑·网络安全大会
West Lake Cybersecurity Conference

OLYMPIC DESTROYER

Deception of Cybersecurity Industry

主讲人：VITALY KAMLUK

KASPERSKY

1

WHO AM I

KASPERSKY lab

2018 西湖论剑 • 网络安全大会
West Lake Cybersecurity Conference

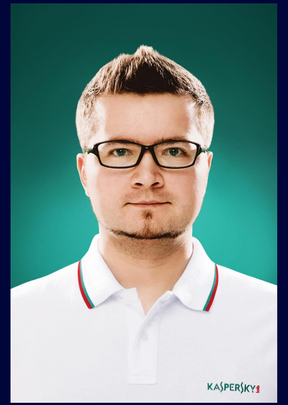
VITALY KAMLUK

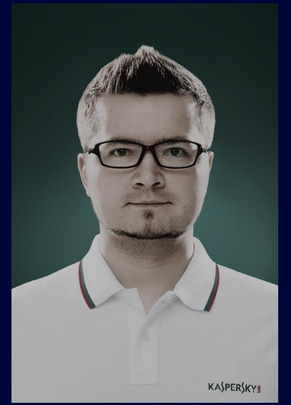
Director of APAC Research Team, KASPERSKY LAB

Experience:

- 13 years with Kaspersky Lab
- 2 years with INTERPOL in Singapore

- Reverse Engineering
- Digital Forensics
- Computer Investigations





KASPERSKY

2018 西湖论剑·网络安全大会
West Lake Cybersecurity Conference

KASPERSKY Global Research & Analysis Team

- APT Discovery
- Investigations
- Threat Intelligence Service

KASPERSKY lab

KASPERSKY lab

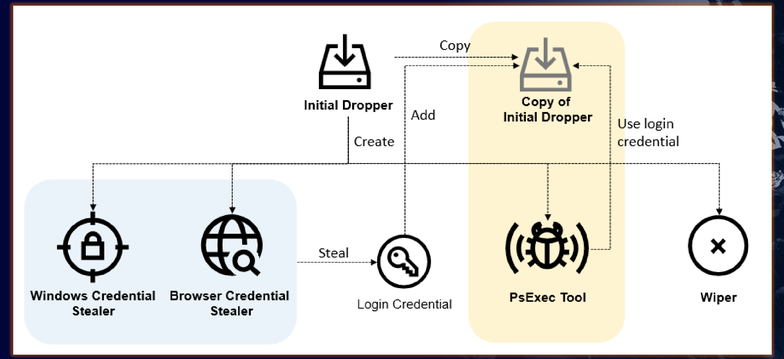
2

OLYMPIC DESTROYER

KASPERSKY lab

What Is Olympic Destroyer

- Self-replicating network worm
- Collects user credentials
- Carries a wiper to destroy data
- Disables local system from boot



Why Is It Special?

- Destructive cyber-sabotage attack
- No motive for cybercriminals => Nation-state?
- Olympic Games infrastructure was a target
- Compromise of supply chains

9th February 2018
Pyeonchang, South Korea

Chain of Events

- 24 Feb — Washigton Post claimed that it was Russia that used NK false flag
- **Crowdstrike** claimed there was no proof it's Sofacy.
- **IntezerLabs** claimed OlympicDestroyer used code of 3 Chinese APT groups
- **Microsoft** claimed they found EternalRomance
- 12 Feb — Samples started circulating in the community. **Cisco Talos** published blog about OlympicDestroyer, connected to NotPetya/Expetr & BadRabbit
- 9 Feb — Official opening ceremony of Winter Olympics suffers from unknown cyberattack
- 7 Jan — McAfee blogs about spear phishing campaign on Olympics

Our Position

- What is the infection vector?
- How large was the operation?
- Why cybersecurity industry was confused?
- What is the true motivation of the attacker?

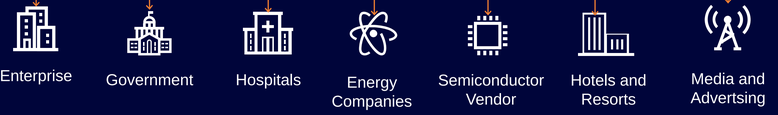
This is just a sample picture. This is not a picture of the attacked resort.

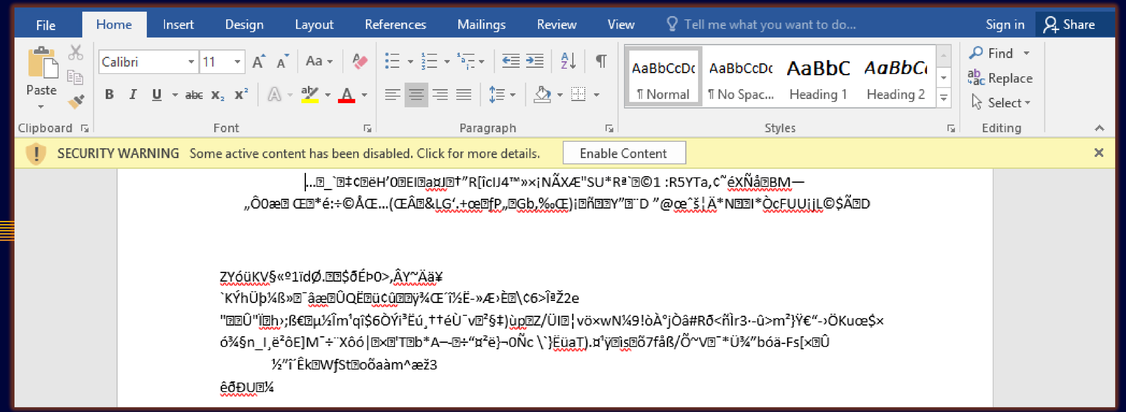
KASPERSKY lab

The Infection Vector

November-December 2017

Email



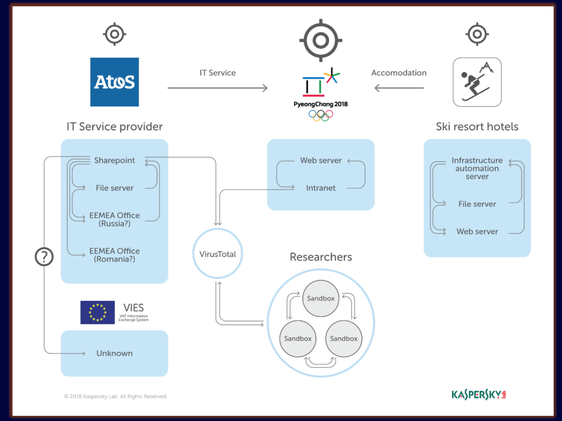


Weaponized Macro Document

KASPERSKY

Tracing The Infection

- The worm collects credentials and hostnames
- Every new generation includes appended new hosts
- It is possible to reconstruct the chain of infection



OlympicDestroyer propagation chart

Attribution Hell

- No financial motivation
- Similarities to different actors
- False signatures to trigger detections

NotPetya?

Eternal Romance?

Chinese Hackers?

Lazarus?

Rich Header Overlap

- Unusual attribute connected OlympicDestroyer to Lazarus
- This attribute, knows as Rich Header has never been used for attribution before

```
   0    9000 ──────────────────────────────── 3c0d740347b0362331c882c2dee96dbf ─
   0  4d 5a 90 00 03 00 00 00  04 00 00 00 ff ff 00 00  MZ..............
  10  b8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  ........@.......
  20  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
  30  00 00 00 00 00 00 00 00  00 00 00 00 e8 00 00 00  ................
  40  0e 1f ba 0e 00 b4 09 cd  21 b8 01 4c cd 21 54 68  ........!..L.!Th
  50  69 73 20 70 72 6f 67 72  61 6d 20 63 61 6e 6e 6f  is program canno
  60  74 20 62 65 20 72 75 6e  20 69 6e 20 44 4f 53 20  t be run in DOS
  70  6d 6f 64 65 2e 0d 0d 0a  24 00 00 00 00 00 00 00  mode....$.......
  80  d3 1e 27 79 97 7f 49 2a  97 7f 49 2a 97 7f 49 2a  ..'y..I*..I*..I*
  90  ec 63 45 2a 96 7f 49 2a  f8 60 43 2a 9c 7f 49 2a  .cE*..I*.`C*..I*
  A0  14 63 47 2a 92 7f 49 2a  f8 60 4d 2a 93 7f 49 2a  .cG*..I*.`M*..I*
  B0  54 70 14 2a 90 7f 49 2a  97 7f 48 2a da 7f 49 2a  Tp.*..I*..H*..I*
  C0  a1 59 42 2a 94 7f 49 2a  52 69 63 68 97 7f 49 2a  .YB*..I*Rich..I*
  D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
  E0  00 00 00 00 00 00 00 00  50 45 00 00 4c 01 05 00  ........PE..L...
```

Olympic Destroyer

```
   0    4000 ──────────────────────────────── 5d0ffbc8389f27b0649696f0ef5b3cfe ─
   0  4d 5a 90 00 03 00 00 00  04 00 00 00 ff ff 00 00  MZ..............
  10  b8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  ........@.......
  20  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
  30  00 00 00 00 00 00 00 00  00 00 00 00 e8 00 00 00  ................
  40  0e 1f ba 0e 00 b4 09 cd  21 b8 01 4c cd 21 54 68  ........!..L.!Th
  50  69 73 20 70 72 6f 67 72  61 6d 20 63 61 6e 6e 6f  is program canno
  60  74 20 62 65 20 72 75 6e  20 69 6e 20 44 4f 53 20  t be run in DOS
  70  6d 6f 64 65 2e 0d 0d 0a  24 00 00 00 00 00 00 00  mode....$.......
  80  d3 1e 27 79 97 7f 49 2a  97 7f 49 2a 97 7f 49 2a  ..'y..I*..I*..I*
  90  ec 63 45 2a 96 7f 49 2a  f8 60 43 2a 9c 7f 49 2a  .cE*..I*.`C*..I*
  A0  14 63 47 2a 92 7f 49 2a  f8 60 4d 2a 93 7f 49 2a  .cG*..I*.`M*..I*
  B0  54 70 14 2a 90 7f 49 2a  97 7f 48 2a da 7f 49 2a  Tp.*..I*..H*..I*
  C0  a1 59 42 2a 94 7f 49 2a  52 69 63 68 97 7f 49 2a  .YB*..I*Rich..I*
  D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
  E0  00 00 00 00 00 00 00 00  50 45 00 00 4c 01 03 00  ........PE..L...
```

Lazarus

Rich Header

- Contains encrypted data
- Includes references and counters to used object files
- May uniquely identify the project and author
- We discovered that it was **FORGED** in OlympicDestroyer samples.

Offset	First value	Second value	Description
00	44 61 6E 53 (“DanS”)	00 00 00 00	Beginning of the header
08	00 00 00 00	00 00 00 00	Empty record
10	Tool id, build version	Number of items	Bill of materials record #1
...			
...	52 69 63 68 “Rich”	Checksum / XOR key	End of the header

```
  Raw data              Type          Count     Produced by
=============================================================
000C 1C7B 00000001   oldnames            1     12 build 7291
000A 1F6F 0000000B   cobj               11     VC 6 (build 8047)
000E 1C83 00000005   masm613             5     MASM 6 (build 7299)
0004 1F6F 00000004   stdlibdll           4     VC 6 (build 8047)
005D 0FC3 00000007   sdk/imp             7     VC 2003 (build 4035)
0001 0000 0000004D   imports            77     imports (build 0)
000B 2636 00000003   c++obj              3     VC 6 (build 9782)
```


KASPERSKY lab

Proof of Rich Header Forgery

Raw data	Type	Count	Produced by
000C 1C7B 00000001	oldnames	1	12 build 7291
000A 1F6F 0000000B	cobj	11	VC 6 (build 8047)
000E 1C83 00000005	masm613	5	MASM 6 (build 7299)
0004 1F6F 00000004	stdlibdll	4	VC 6 (build 8047)
005D 0FC3 00000007	sdk/imp	7	VC 2003 (build 4035)
0001 0000 0000004D	imports	77	imports (build 0)
000B 2636 00000003	c++obj	3	VC 6 (build 9782)

Forged Rich Header in Olympic Destroyer

Raw data	Type	Count	Produced by
009E 9D1B 00000008	masm10	8	VC 2010 (build 40219)
0093 7809 0000000B	sdk/imp	11	VC 2008 (build 30729)
0001 0000 00000063	imports	99	imports (build 0)
00AA 9D1B 0000003A	cobj	58	VC 2010 (build 40219)
00AB 9D1B 0000000E	c++obj	14	VC 2010 (build 40219)
009D 9D1B 00000001	linker	1	157 build 40219

Original Rich Header in Olympic Destroyer

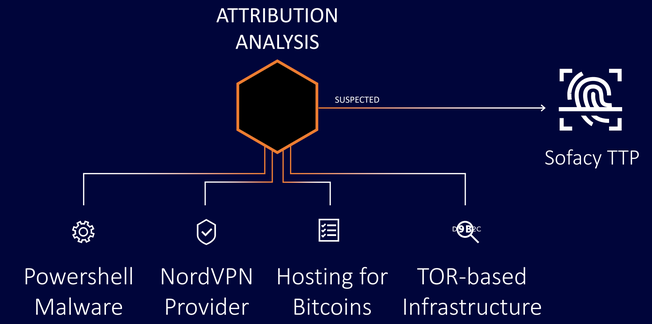
KASPERSKY lab

3

ATTRIBUTION

KASPERSKY lab

Who Might Be Behind It?



National Security

Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say

The PyeongChang 2018 Winter Olympics opened with a dazzling ceremony Feb. 9. (Pawel Kopczynski/Reuters)

By Ellen Nakashima February 24 Email the author

4

CONCLUSIONS

KASPERSKY lab

So What Was Olympic Destroyer?

A. Demonstration of power

B. Controlled-impact cyberweapon checking

C. Attempt to master the art of false-flags

THANKS!
谢谢观看

KASPERSKY