
ITU

Fragile like a bomb

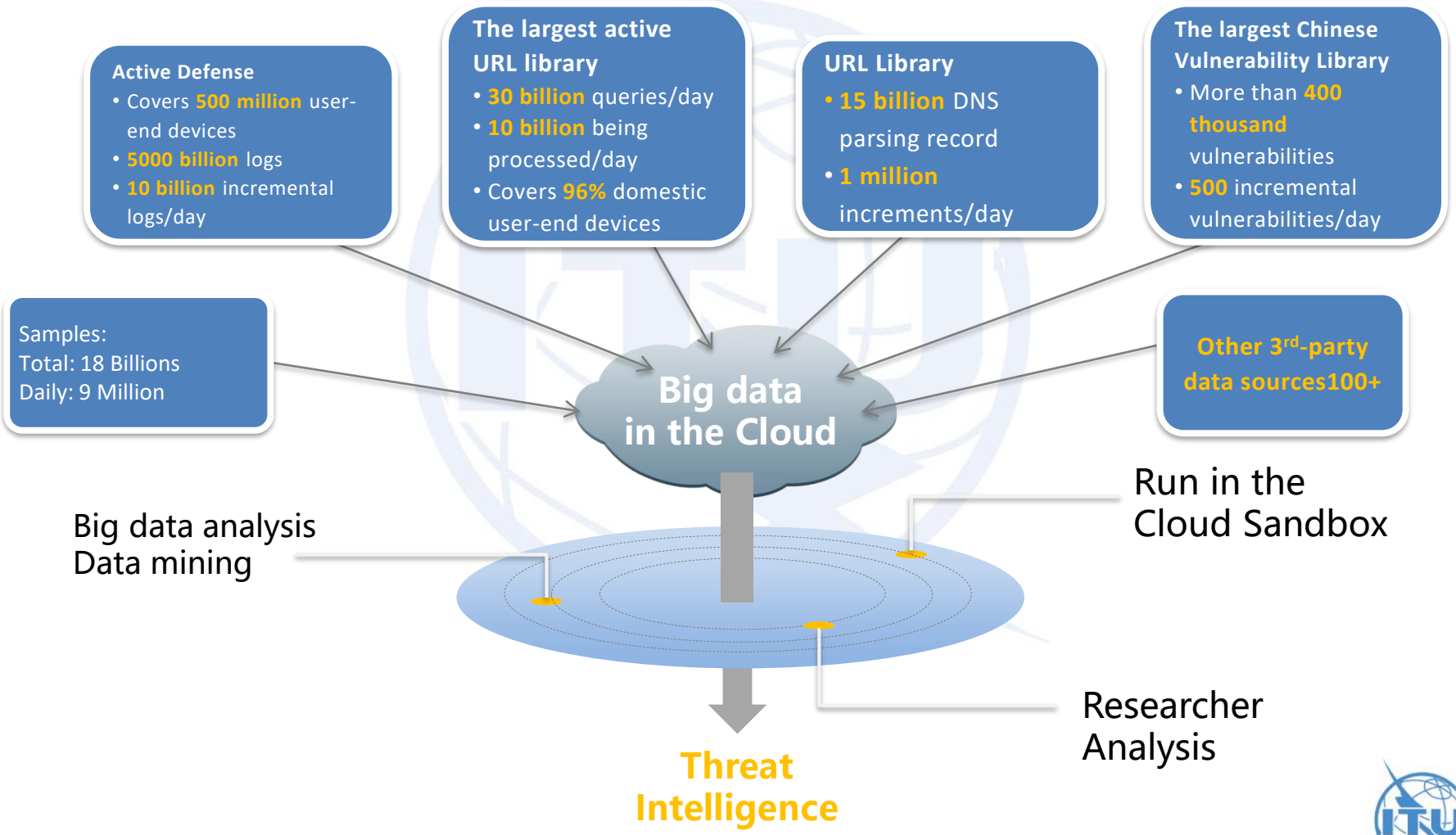
-Zero-day used for targeted attack in the past year

360 Core Security

About Us

- **Founded：** August 2005
- **Employee Base：** 9600+
- **Market Position：** No.1 Internet Security Company in China
- **User Base：**
  - Consumer Market：90% indivial users
  - Enterprise Market：3M enterprise and government clients
- Created the free business model in the security software business

360 Threat Intelligence Center



Vulnerability Acknowledgements

Total: 1275 acknowledgements

- Microsoft: 271
- Google: 497
- Apple: 57
- Adobe: 114
- Qualcomm: 26
- FireFox: 1
- Tesla: 1
- Cisco: 2
- Antivirus Software: 20
- Huawei: 36
- Samsung: 8
- Open Source Projects: 99
- Virtualization Software: 143

Master of Pwn - 2017 Pwn2Own

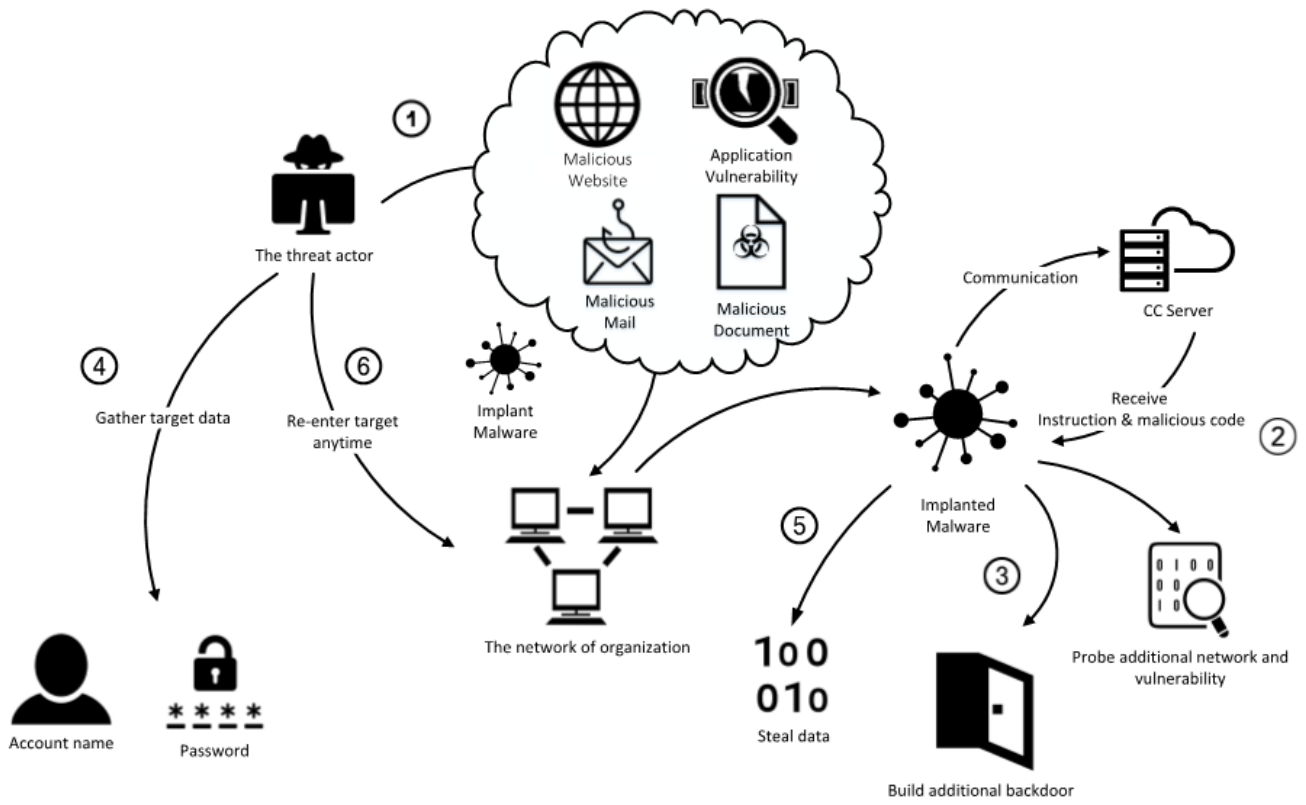
APT Groups and Operations

http://blogs.360.cn/cate/apt-report

Who are the Victims?

- Governmental organizations
- Political parties
- Education institutions and universities
- Telecommunication industry
- Crypto exchange

The Anatomy of an APT attack



Global 0day wild used trend

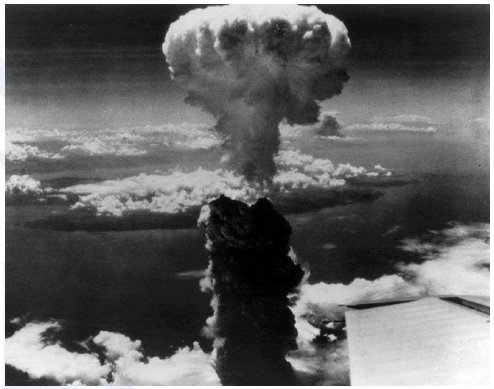
- Apr 2017 CVE-2017-0199（ HTA）
  - In the Wild Attacks Leveraging HTA Handler （FireEye）
- Jun 2017 CVE-2017-026（1/2/3）（Word）
  - EPS Processing Zero-Days Exploited by Multiple Threat Actors （FireEye）
- Jul 2017 CVE-2017-8464 Stuxnet （Shortcut LNK）
  - Third Generation Stuxnet - Isolation Network Advanced Threat Analysis Report (Qihoo 360)
- Sep 2017 CVE-2017-8759 (Word)
  - Zero-Day Used in the Wild to Distribute FINSPY （FireEye）
- Oct 2017 CVE-2017-11826， CVE-2017-11292（Word，Flash）
  - Analysis of CVE-2017-11826 Exploit in the Wild (Qihoo 360)
  - BlackOasis APT and new targeted attacks leveraging zero-day exploit （Kaspersky）
- Dec 2017 CVE-2018-0802（Word）
  - Second Generation Nightmare formula (CVE-2018-0802) (Qihoo 360)
- Feb 2018 CVE-2018-4878（Flash）
  - The first Adobe Flash zero-day vulnerability in the wild in 2018 (Qihoo 360)
- Apr 2018 CVE-2018-8174（Word & IE）
  - Analysis of the World's First "Double-kill" 0day Attack by APT-C-06 (Qihoo 360)
- Jun 2018 CVE-2018-5002 (Flash)
  - Analysis of the Second Wave of Flash Zero-day Exploit in 2018 (Qihoo 360)

Nightmare with “Office”

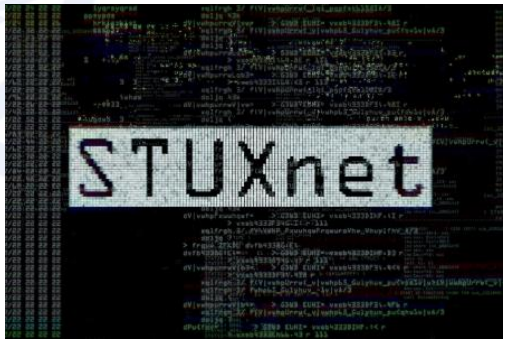
- CVE-2017-11826
  - High-level targeted attack against China
  - Stable + Affecting almost all the office versions
  - Similar to the CVE-2015-1641
- CVE-2018-0802
  - Almost all office versions
  - Similar to the ‘Nightmare Formula’ lurking for 17 years

21st-century cyber weapon

In 1945, Physical Weapon ->
In 2005, Invisible Weapon

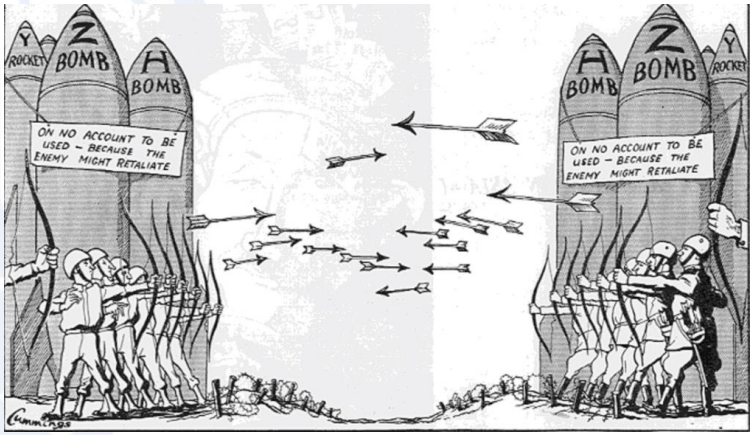


- In June 2010
  - The most complicated cyber weapon
  - Attack nuclear facility
- In May 2012
  - Attacked multiple countries
  - Flame virus
- In June 2016
  - Isolated networks
  - Resembles two previous generations + unknown attack techniques



Regional Conflict

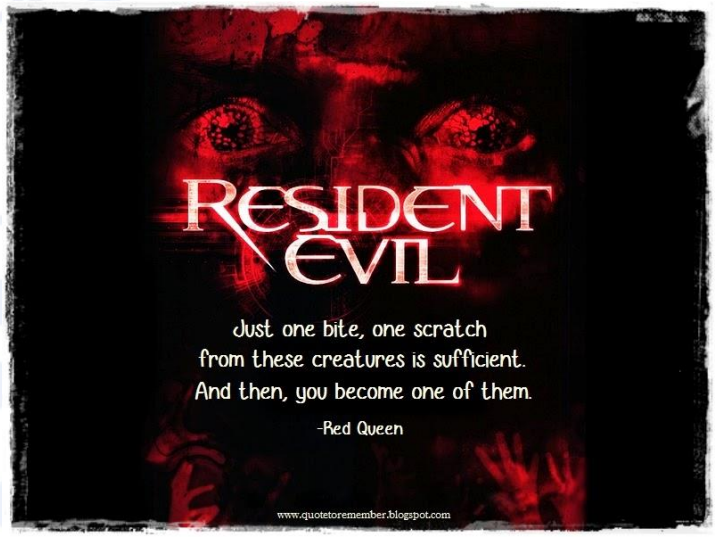
- CVE-2018-4878
  - Check AhnLab, ViRobot APT Shield and 360 Security
  - Different approach to attack
  - China and South Korea are the targets



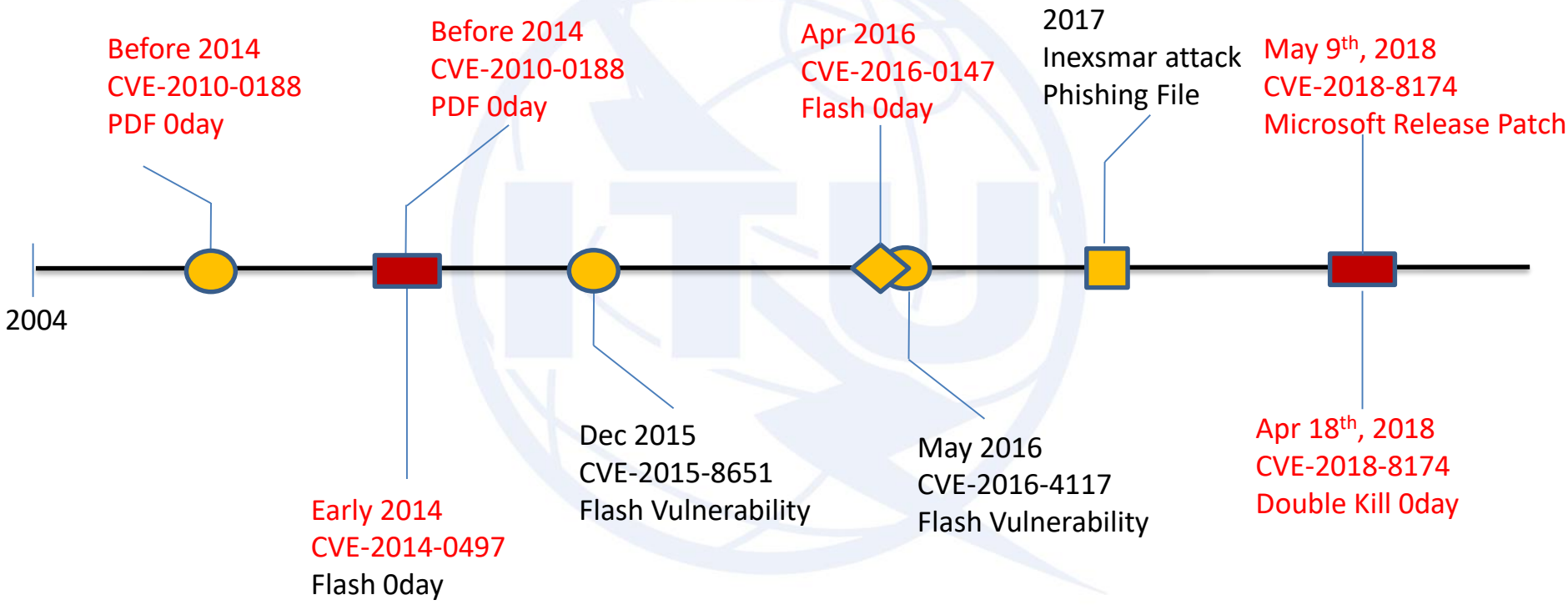
- CVE-2018-5002
  - Wildly Used Flash 0day
  - Remotely load the Flash vulnerability
  - Middle East is the main target

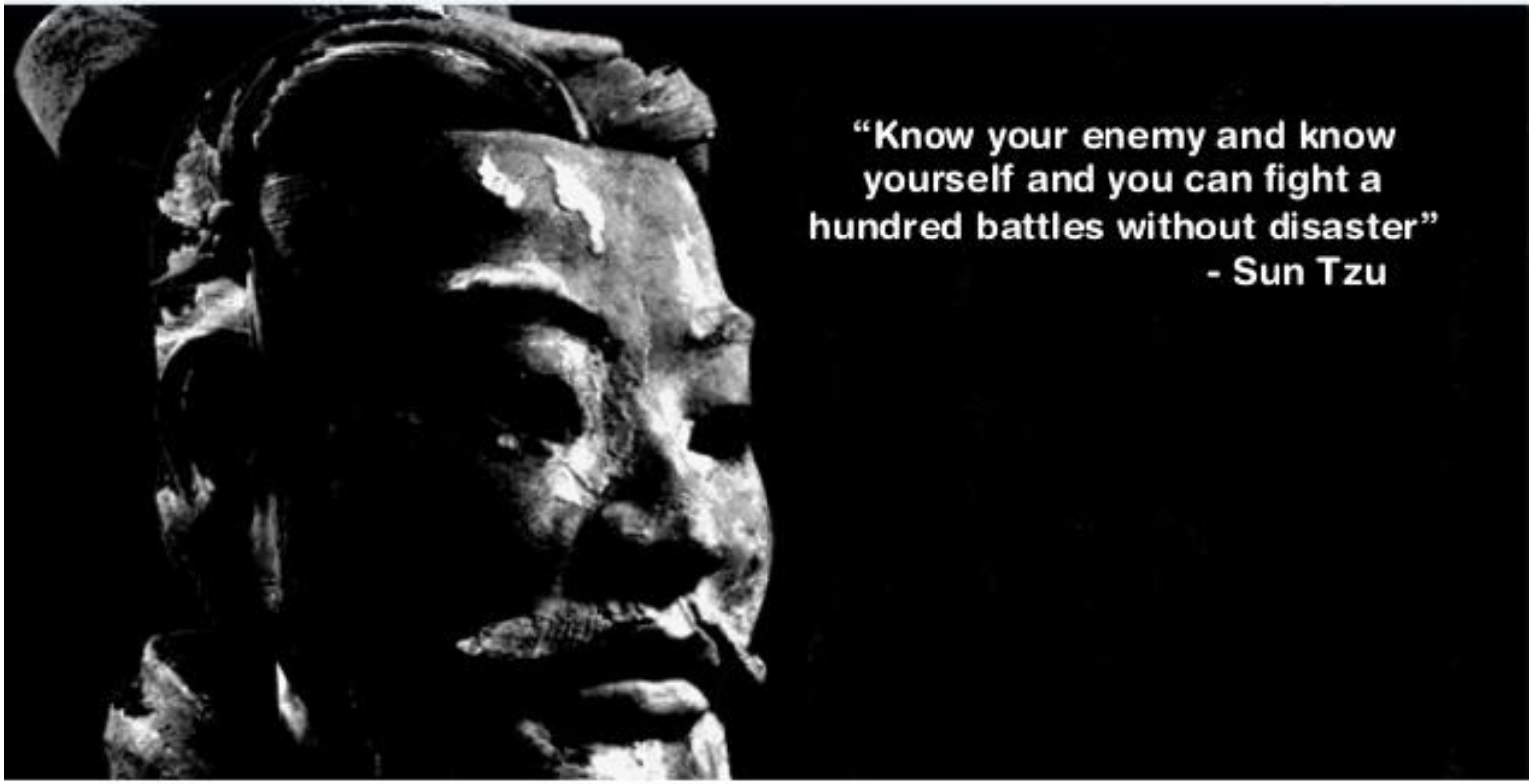
Double Kill – the Revolution

- CVE-2018-8174
  - Potential target: browse the web or open Office doc
  - Latest version of IE and applications that use the IE kernel
- APT-C-06
  - Special compromised machine has a large mount of malware
  - Constant Attack since 2015



Double Kill - Timeline




"Know your enemy and know
yourself and you can fight a
hundred battles without disaster"
- Sun Tzu

THANK YOU