RSA Conference2016

Singapore | 20-22 July | Marina Bay Sands

Connect to Protect

SESSION ID: TTA1-R08

Threat Intelligence Landscape in China

Feng Xue

CEO

ThreatBook

@s0what

#RSAC

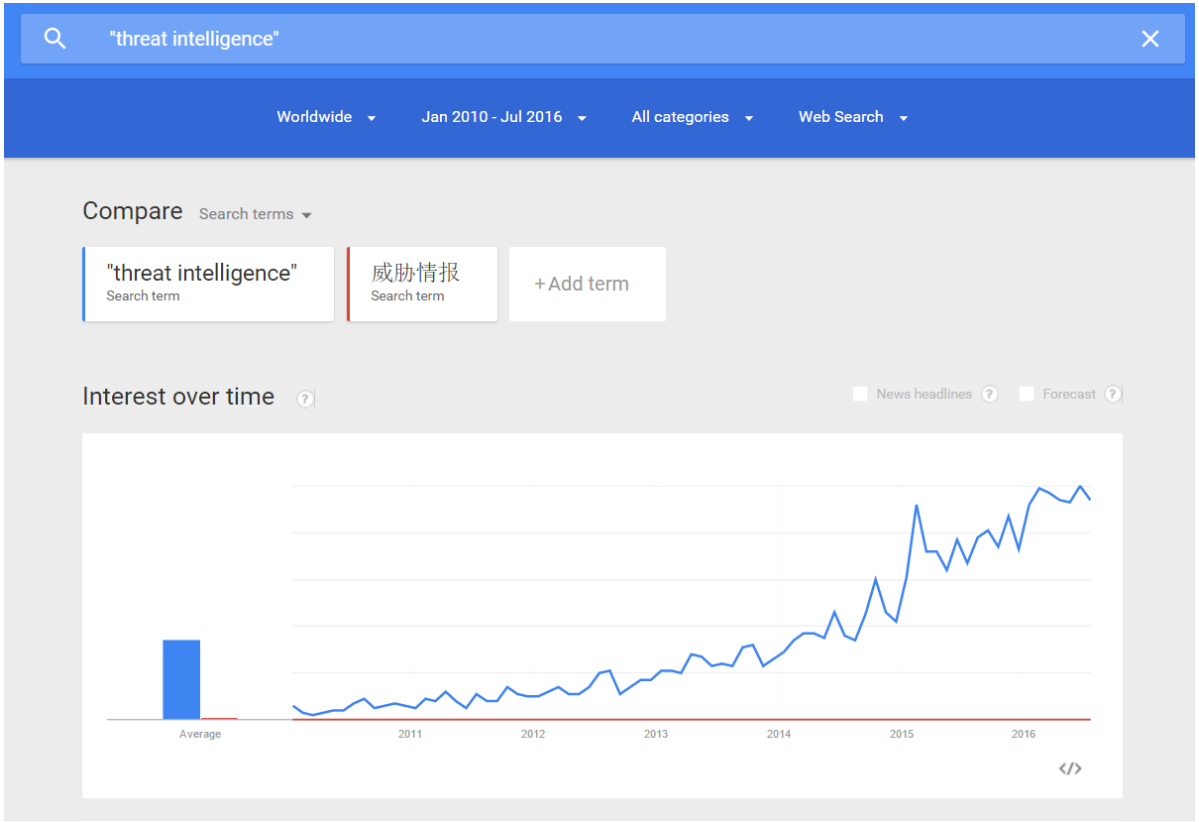
Agenda

- Introduction
- Threat Intelligence
- China’s Threat Intel Ecosystem
- Two real world cases
  - XCodeGhost
  - DarkHotel Operation 8651

Introduction

- Feng Xue, 16 years in cyber security
- Founder and CEO of ThreatBook, China's 1st Threat Intel company
- CISO for Amazon China
- Director of Internet Security for Microsoft in China

Interests about Threat Intelligence



Sun Tzu on the Art of War

“if you know your enemies and know yourself, you will not be imperiled in a hundred battles”

- Sun Tzu

“Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard.”

Threat Intelligence
- Gartner

Threat Intelligence

Data + Analysis

Data – what matters

- Volume
- Diversity
- Historical
- Connections
- Regional
- Analysis

Threat Intelligence in China

- 2015
  - First TI company founded
  - Similar to “Cloud Computing” in 2010
- 2016
  - Dozens of vendors claim that they offer TI services
  - Customers are not ready yet
  - Devices are not ready yet
- 2017?

CrowdSourced TI

- Being very popular among *SRC (security response center)
- Upgraded from “bug bounty program”
- Anything useful – vulnerabilities, phone numbers, emails, incidents, leads

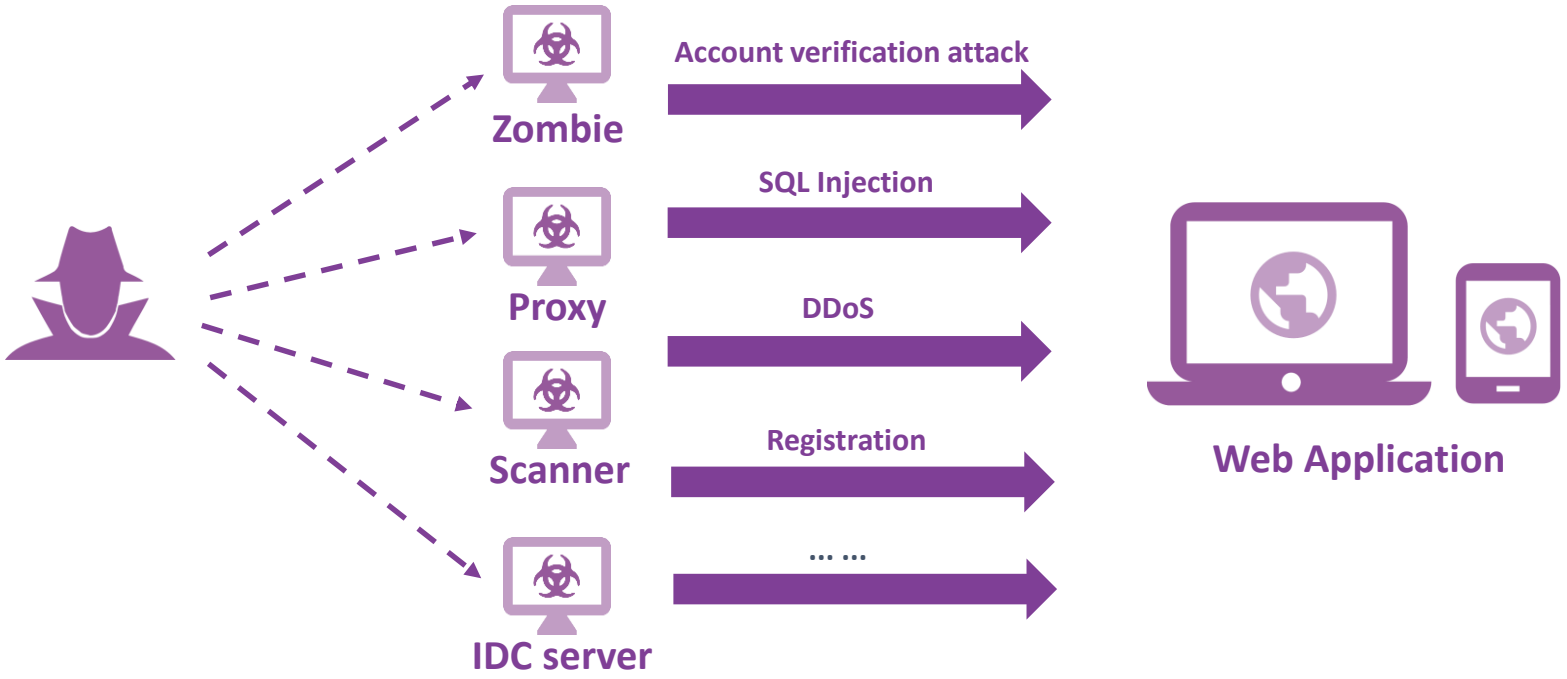
Standard

- STIX, TAXII
- STIX 2.0
- No standard in China yet

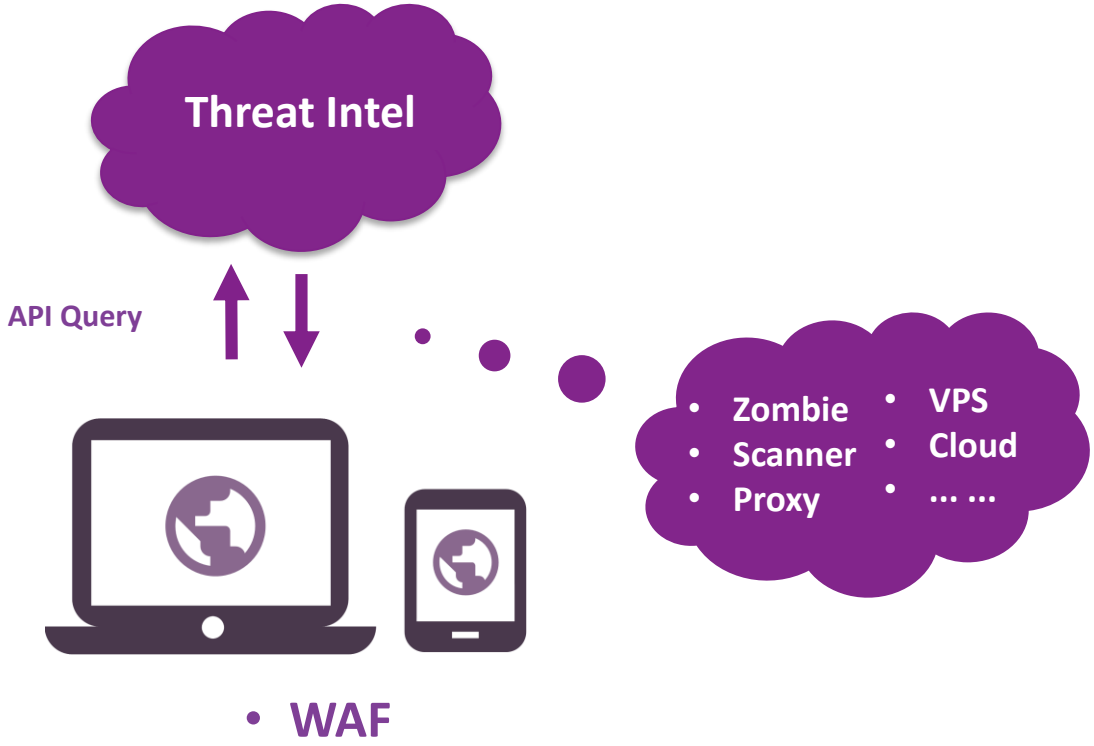
TI+

- Threat Intelligence +
- Intelligence driven solutions, such as:
  - Scanner
  - WAF
  - NGFW
  - SIEM
  - And so on…

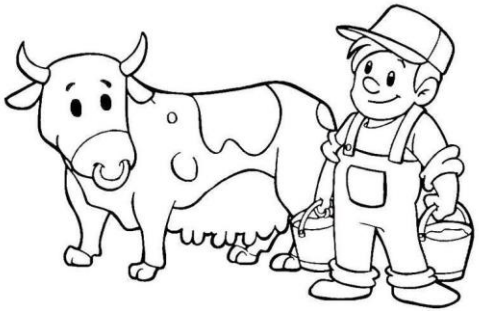
Example: WAF


Zombie
Proxy
Scanner
IDC server
Account verification attack
SQL Injection
DDoS
Registration
... ...
Web Application

Example: WAF

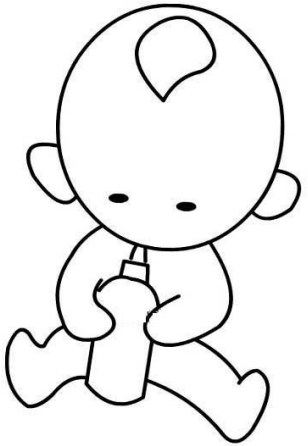


Ecosystem



Producer

Security
Products/Stores

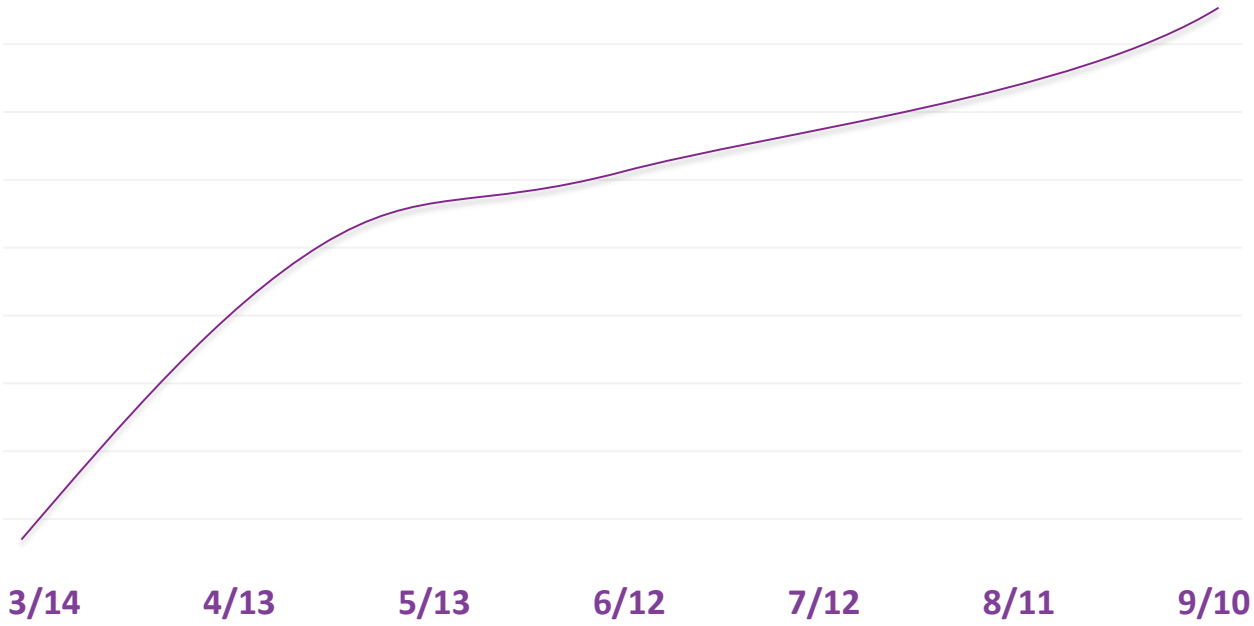


Consumer

XCodeGhost – No.1 iOS security incident

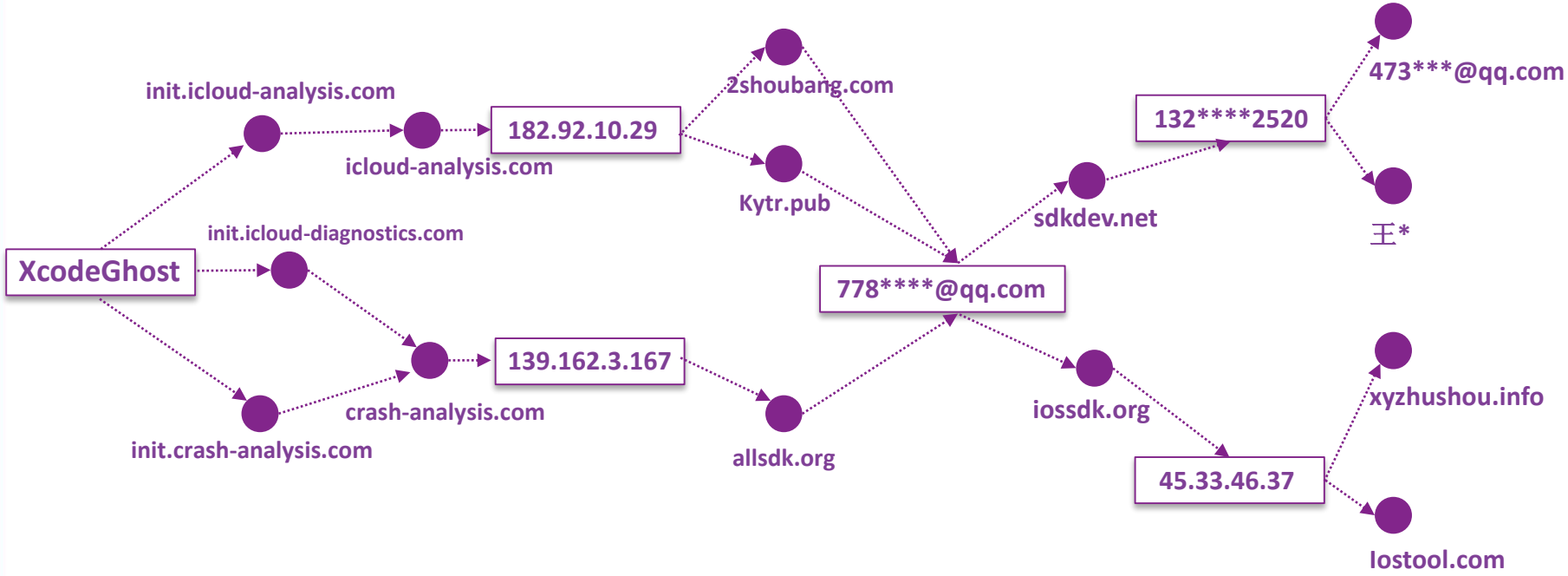
XCodeGhost - When

init.icloud-analysis.com



XCodeGhost - Who

init.icloud-analysis.com



XCodeGhost - Why

- XCodeGhost vs. KeyRaider
- XCodeGhost vs. PC TrojanSpy

DarkHotel Operation 8651

DarkHotel Operation 8651 Analysis

- Starting with a .swf file
- Profiling
- DarkHotel
- Who’s behind it?

Conclusion

- Threat Intelligence is still in early stage in CN
- Customers and devices are not ready yet
- More and more security vendors starting to invest in TI

Apply

- Know yourself, know your enemies
- Diversity and source of data matters
- Analysis matters more