DISSECTING EXPLOIT KITS

DANIEL FRANK
WHO AM I

- Security Researcher
- Developer
- Speaker (Microsoft DCC 2016, ROOTCON 11)

- daniel.frank@rsa.com
- @dani3lfrank
AGENDA

- Exploit Kits flow and top vulnerabilities
- Market and geolocation related stats
- Magnitude Exploit Kit with live demos
- Sundown Exploit Kit with live demos
- Conclusions
demo time!
Demo time?

Already?
LIVE DEMO
EXPLOIT KITS FLOW AND TOP VULNERABILITIES
WHAT IS AN EXPLOIT KIT

- A toolkit
- Redirects victim to a landing page
- Identifies and exploits client side vulnerabilities
- Delivers malicious payload
TOP VULNERABILITIES

- In 2016, Adobe Flash provided 6 out of top 10 vulnerabilities used by Exploit Kits
- Rest of the top 10 are IE and Silverlight vulnerabilities
- CVE-2016-0189 is linked the most to Exploit Kits, especially to Sundown
- CVE-2015-7645 was used by 7 Exploit Kits
EXPLOIT KITS MARKET
MARKET – 2015

Exploit Kits Types

- Angler: 60%
- Nuclear: 14%
- Magnitude: 12%
- Sundown: 0%
- Others: 14%
MARKET – 2015

- According to TrendMicro:
  - Angler 60%
  - Nuclear 14%
  - Magnitude 12%
  - Sundown 0.33%
  - Others 13.67%

- Angler has the biggest share

- Magnitude has some share of the market

- Sundown still has less than 1%
MARKET – 2015

Source: http://chartsbin.com/view/33051
BROWSER MARKET SHARE 2015

JAPAN 2015

SOUTH KOREA 2015

Source: http://gs.statcounter.com/browser-market-share/
MARKET – 2016

Countries Most Affected

- Japan: 47%
- US: 33%
- Taiwan: 12.6%
- Others: 8%

MARKET – 2016

- Countries most affected:
  - Japan 47%
  - US 12.7%
  - Taiwan 8%
  - Others 33%

- Japan with almost 50% of the market share

- Taiwan is also with a relatively high share

- US is going strong as well
BROWSER MARKET SHARE 2016

JAPAN 2016

SOUTH KOREA 2016

Source: http://gs.statcounter.com/browser-market-share/
MARKET – EARLY - MID 2017

- According to ThreatPost:
  - RIG who was big in 2016, almost disappeared
    - Still delivering ransomware in Southeast Asia
    - The most common
  - Sundown is still here
    - Changing variants
    - Adapting to changes
  - Magnitude
    - Low volumes
    - Affects Southeast Asia
MAGNITUDE EXPLOIT KIT
MAGNITUDE EXPLOIT KIT

- Started to headline in 2013
- Malware As a Service
- 31% of the market in 2014
- Functional admin panel
- Targeted victims
demo time!
SUNDOWN EXPLOIT KIT
SUNDOWN EXPLOIT KIT

- Still active
- Adjustable to changes
- Copy-paste code
demo
time!
CONCLUSIONS
CONCLUSIONS

- The EK market is slowly dying
- Easy to overcome by keeping software up to date
- Difficult to get exploits to work on victim’s machine
- Less usage of IE
- Less usage of Flash