ATTACK TRENDS 2014

adric.net

March 2014

Attack Trends: Who, What, Huh?

- **Attacker and attack typing**
- **Attack history**
  - RSA, Stuxnet, TJX …
- **Recent attacks in the news**
  - CC breaches
  - More DDoS

- **Example Scenarios:**
  - BHEK2 crimeware
  - Shanghai (APT1)
- **Data Sources**
  - SANS ISC, US CERT
  - Collected breach reports
  - Case studies
  - Researcher blogs
  - Journalists

Attacker typing

- Amateurs
- Script Kiddies
- Hacktivists
- Industrial crime
- Insiders
- Government agents

- Motivation and Sophistication vary
- Anonymous ?
- Combos …
- and False Flag

Attack typing: attacks & exploitation

Attack: Deny, Degrade

- Worms
  - Melissa, ILY
- Network attacks
  - Smurf
  - Flood DoS
- Server side
  - CodeRed, Slammers
  - Web apps: SQLi dumps

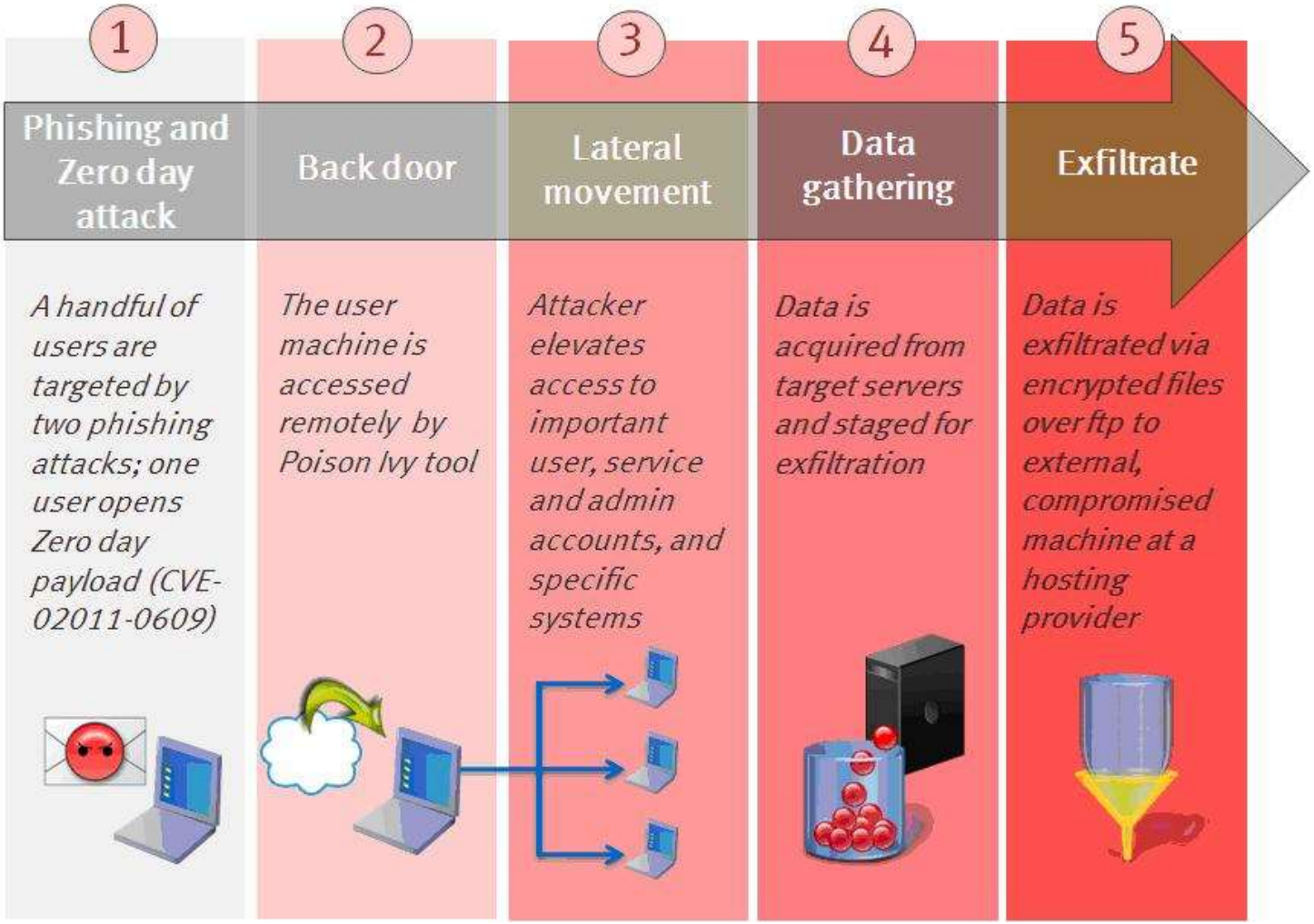
Exploitation: Control

- Trojan -> Botnet zombie
  - Zeus
  - BHEK
- Added a user to your CMS
  - With XSS, SQLi
  - And your netsec console
- Crack in, set up shop
  - Sabotage?
  - Exfil?
  - Profit ?!

ATTACK HISTORY

Some “highlights” of famous attacks

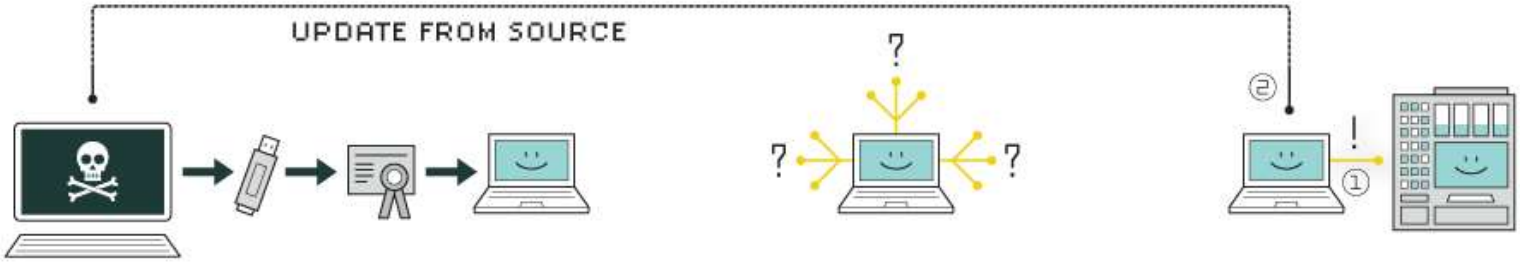
RSA SecureID



RSA SecureID: secret seeds taken

- Multiple phish sent: Eventually a user opened an Excel file
  - Email and attachment said it was about their compensation
  - Embedded Flash file in XLSX with exploit
- Up and down:
  - Attackers sniffed credentials and then moved laterally
  - To their objective on protected network
  - With the required stolen credentials to get there
- Relayed the secret data back out to the network perimeter
  - FTP’d it out to a drop site on public Internet
- Allegedly same attacker then used seed data in attacks
  - on defense contractors the following month
  - Neutralizing their 2F

HOW STUXNET WORKED



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Stuxnet: Stuxnet and friends

- Bypassed air gap
  - With USB sticks
- Multiple zero days
- Valid signatures
- Selective execution
- Sabotaged centrifuges

Kaspersky Labs says:

- *Stuxnet*
- *Flame*
- *Gauss*
- *Magic*
- Infostealer?

are all related

- OLYMPIC GAMES
  - Alleged: US/Israeli op
  - unconfirmed

TJX

Stupid Technology Tricks of 2007

TJX Data Breach

In January, TJX announced that its systems had been hacked. According to TJX, more than 100 million debit and credit cards had been exposed to potential fraud—possibly during the course of several years. The profoundly disturbing fact that TJX stores were using easily cracked WEP to protect their wireless networks was almost beyond belief. With all of the personally identifiable information that was potentially exposed, it will likely be years before the full impact of this breach is known.

—Cameron Sturdevant

TJX

- Weak Wifi used in thousands of stores
- Backend VPN with no network separation
- Plaintext protocols, password reuse
- No sensors, no alerts ... Went on for years
- Millions of plaintext credit cards
  - copied from internal servers and exfil'd
  - Sold on open black market

CURRENT EVENTS

More recently reported…

Holiday 2013 Retailer Breaches

- Target
  - Fireye alerted.
  - In via HVAC contractor?
- Neiman Marcus
- Sally Beauty

- Millions of cards implicated, reissued

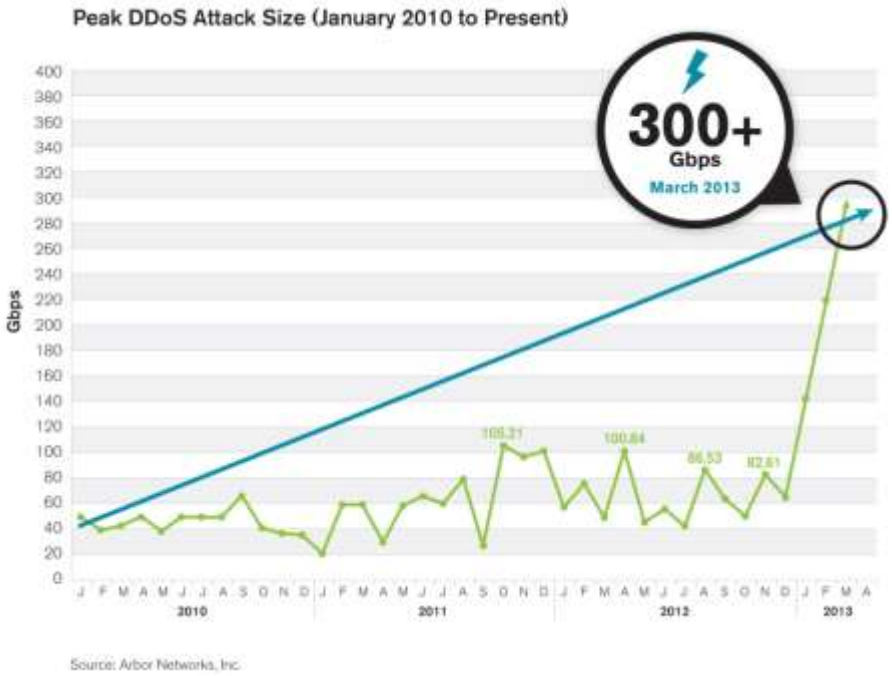
- POS system resident
  - RAM scraping malware
- Like Dexter (hit B&N)

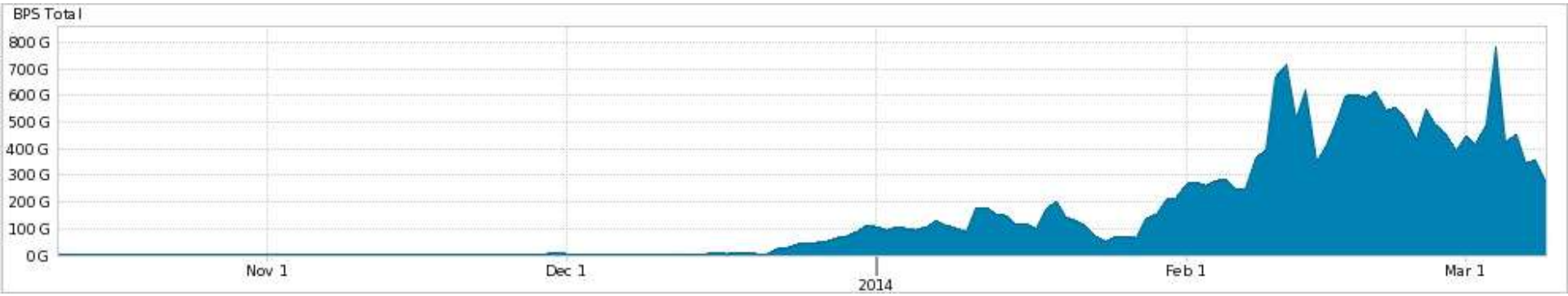
- PCI Compliant?

- Target and Trustwave sued.

DDoS Extortion enhancements

- 20 Gbps → 100 Gbps → ??
- NTP latest
  - DNS still popular
- Amplification X Reflection
- = huge floods
- **Arbor** WSIR 2014:
- "Welcome to the hockey stick age"





EXAMPLE SCENARIOS

Non-fiction, unfortunately

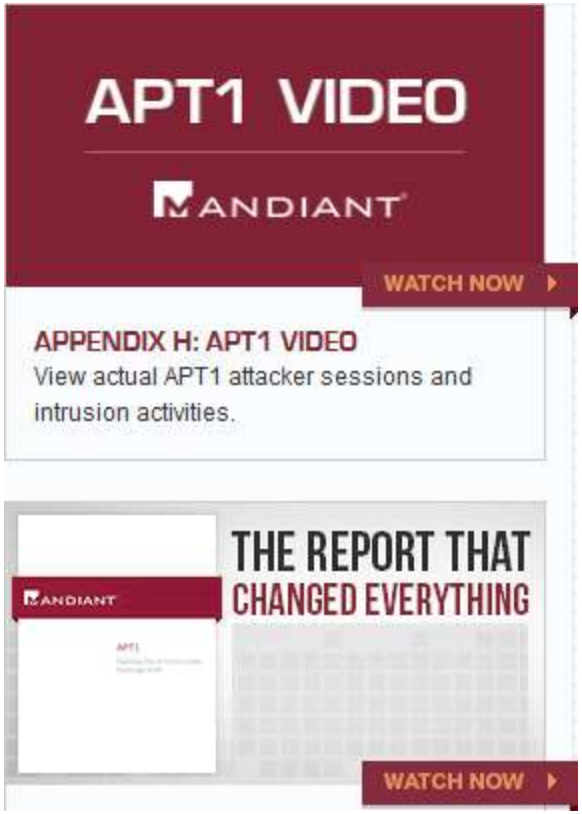
Crimeware example: BHEK

- Web hosted
  - Crime aaS ? Yep
  - Links in spam/phish mail
- Multiple client side attacks
  - Evaluates clients with JS
  - Creates a PDF/Flash file
- Sophisticated
  - Obfuscation
  - Anti-forensics
  - Payload generation

Partial decode from Malware Must Die blog Sept 2012

APT1: Mandiant's report & fallout

- Phish, sploit, exfil
  - Works on hundred of companies
  - Gmail phishing poles (in the video)
- M released 1000s of IoC format indicators
  - Many other researchers were tracking this group.
  - Attackers immediately updated TTP
  - Most APT1 indicators useless within months of report publication



APT1: Attribution Controversy

- Jeffrey Carr (Feb 2013) “Mandiant APT1 Report Has Critical Analytic Flaws”
- Argument recently broke out again Mar 2014 on **DailyDave** list, quickly got personal … ouch
- Mandiant says USGOV sources confirm their attribution.
- Data they publically released … doesn’t. ☹

DATA SOURCES

Data Sources

- SANS ISC, US CERT
- Collective breach reports
  - Verizon DBIR
  - Ponemon
- Case studies
  - RSA
  - Fireye
- Researcher blogs
  - Contagio
  - Malware Must Die
  - Kafeine
- Journalists
  - Krebs
- Corp blogs & WP:
  - Sophos
  - Arbor

AND: Buy or build an Threat intelligence (TI) capability!

Questions?

Ask away now or later:

adric@adric.net
@adricnet

My site:

http://adric.net