Mo’ Money
Mo’ Problems

Making A LOT more money on the Web the black hat way

Jeremiah Grossman
Founder & Chief Technology Officer

Trey Ford
Director, Solutions Architecture

BlackHat USA 2009
07.30.2009
A study conducted by the Verizon Business RISK Team

2009 Data Breach Investigations Report

The embodiment of converged IT and physical security.

- InformationWeek
Director of Solutions Architecture

6 years as an information security consultant for Fortune 500s

PCI-DSS
Curmudgeon

???
TechCrunch Layoff Tracker

Plan B
Hacker Stimulus Package

http://www.techcrunch.com/layoffs/

Last update: July 3, 2009
Total Layoffs Since August 27, 2008: 479
Total Employees Laidoff: 340,066
Get Rich or Die Trying, 2008...

Four figures: Solving CAPTCHAs
Five figures: Manipulating payment systems
High five figures: Hacking Banks
Six figures: Scamming eCommerce
High Six figures: Defraud Affiliate Networks
Seven figures: Gaming the stock market

All still work just fine. :)

http://www.youtube.com/watch?v=SIMF8bp5-qq
Im in ur webz
crosing ur scripzz!
SHOW ME THE MONEY!
The target won’t know

How the breach was detected:
• 3rd party detection due to FRAUD (55%)
• 3rd party detection NOT due to fraud (15%)
• Employee Discovery (13%)
• Unusual System Performance (11%)

2009 Data Breach Investigations Report

© 2009 WhiteHat, Inc. | Page 10
Don’t be that guy

David Kernell, 20 year-old student University of Tennessee student, allegedly hacked into former VP candidate Sarah Palin’s Yahoo Mail.

Stephen Watt, TJX hack participant which the feds call “the largest identity theft in our Nation’s history.” AKA (Operation Get Rich or Die Tryin)

Gary McKinnon, described as the 'UFO Hacker,' allegedly broke into United States military and NASA computers to find evidence of government-suppressed information.
Attacker Targeting

Random Opportunistic
- Fully automated scripts
- Unauthenticated scans
- Targets chosen indiscriminately

Directed Opportunistic
- Commercial and Open Source Tools
- Authentication scans
- Multi-step processes (forms)

Fully Targeted
- Customize their own tools
- Focused on business logic
- Clever and profit driven ($$$)

The Super Hacker?
Holiday Grinch-bots

eBay’s "Holiday Doorbusters" promotion, administered by Strobe Promotions, was giving away 1,000 items -- **2009 corvette, plasma TVs, jet skis, diamond ring**, etc -- to the first person to find and buy **specially-marked $1 items**.

Some "contestants" used scripts, skipping to 'buy', without even viewing the goods. **Almost 100%** of the prizes were 'won' this way as evidenced by the **visitor counters showing "0000."**

Many were not happy and complaining in the forums. Disappointed with eBay’s response, some took matters into their own hands **listing "other" items for $1.**

"**This is picture I took of my cat** with my Cannon Powershot Camera after she overheard that people were using scripting to purchase HOLIDAY DOORBUSTERS items on eBay. **Not responsible for poor scripting techniques.**"
Recover someone else’s password - it’s a feature!
“Appropriate” access to Email

Start with just an email address

Answer these questions to validate your identity
We need to verify a few questions and we’ll be done.

Birthday
- Select Month -

Day

Year

Country of Residence
- Select One -

Postal Code

Next
Doing a little research

3. In case you forget your ID or password...

Alternate Email

Security Question
Where did you meet your spouse?
- Select One -

Just a couple more details...

Type the code shown

Type the code shown

© 2009 WhiteHat, Inc. | Page 16
or ‘lots’ of research

Sarah Palin — Date of Birth: February 11, 1964

Account information used by the anonymous ‘hacktivists’:

Sarah Palin account info:
gov.palin@yahoo.com
DOB 2/11/64
ZIP 99687

Todd Palin:
fek9wnr@yahoo.com
DOB: 9/6/64
ZIP 99654
... and you’ve got MAIL

Re: Looks like it's my turn in Dan's crosshairs

From: "gov.palin@yahoo.com" <gov.palin@yahoo.com>
To: "Sean personal2" <spanmail@alaska.com>

Arghhh! He is so inconsistent and purposely misleading! I am sorry, Sean. He can keep trying, but you are the right one for the Congressional position and he KNOWS it (that's the inconsistency). Remember how he said it all only really matters on measures like LIFE, honesty, ability, etc... all those things you are (as opposed to attributes of your opponents)? He knows you fill all of his, and conservatives', and Alaskans' criteria. His fighting you reveals some evil stuff going on with him. Does he want someone OPPOSED to the life issue in Congress? NOT capable of working with both parties? NOT experienced and capable and standing strong on all the right issues?

I am so sorry he does this.

-----Original Message-----
From: Sean personal2
Sender: Sean personal2
To: Sarah's Personal Email
Sent: Jul 23, 2008 6:49 PM
Subject: Re: Looks like it's my turn in Dan's crosshairs

Yesterday, as I sat the record straight on my support for you and my ads, Pagan asked if I supported ACES. I told him I did, gave my reasons why and now he's replaying it over and over next to my ad where I tell people I'm for lower taxes (which was my legislative history, voted against a state income tax, fought Tony's long range financial plan that included five new taxes, didn't raise taxes when oil was at $5 a barrel, cut spending instead.)

It got ugly and will be.
“The most secure email accounts on the planet”

To get into a StrongWebmail account, the account owner must receive a verification call on their phone. This means that even if your password is stolen, the thief can’t access your email because they don’t have access to your telephone.

http://www.strongwebmail.com/
Break into my email: get $10,000. Here is my username and password.

May 21, 2009

Break into my email: get $10,000. Here is my username and password.
Username: CEO@StrongWebmail.com
Password: Mustang85

StrongWebmail.com is offering $10,000 to the first person that breaks into our CEO’s StrongWebmail email account. And to make things easier, Strong Webmail is giving the username and password away!

Lance James

Aviv Raff

Mike Bailey

http://www.asscert.com/

http://twitpwn.com/

http://www.asscert.com/
The easiest route

1) Registered an account and identified multiple XSS issues in a matter of minutes (Rackspace WebMail software).

2) Sent ceo@strongwebmail.com an email laced with specially crafted JavaScript malware

3) Emailed support@strongwebmail.com stating they won the contest and sent details to the CEO encouraging them to check the account.

4) Within minutes the email were opened, which initiated several Ajax requests to the server, pilfering the inbox, and sending the data to a remote logging script.

http://skeptikal.org/2009/06/strongwebmail-contest-won.html
The easiest route

http://skeptikal.org/2009/06/strongwebmail-contest-won.html
StrongWebmail said it was "not deterred" by the contest's quick conclusion and would be launching a new competition once this bug was fixed. "We won't rest until we have created the most secure e-mail in the world," the company said.
Twitter Hacker

**Hacker Croll** initiates a password recovery for a Twitter employee’s Gmail account. Reset email to secondary account: ******@h******.com.

Guesses secondary Hotmail account, deactivated, but is able to re-register the account. Resends the reset email and bingo.

Pilfers inbox for passwords to other Web services, sets the Gmail password to the original so employee would not notice.

Used the same password to compromise employee's email on Google Apps, steal hundreds of internal documents, and access Twitter's domains at GoDaddy. **Sent to TechCrunch.**

Personal AT&T, MobileMe, Amazon, iTunes and other accounts accessed using username/passwords and password recovery systems.

"I’m sorry" - **Hacker Croll**

Promo codes for cheapskates

- X% and $X off sales
- Free Shipping
- 2 for 1 Specials
- Add-Ons & Upgrades
MacWorld Hacker VIP

Client-Side Hacking
Back to Back Free MacWorld Platinum Pass
($1,695)

http://grutztopia.jingojango.net/2008/01/another-free-macworld-platinum-pass-yes.html
http://grutztopia.jingojango.net/2008/02/your-client-side-security-sucks.html
Free Pizza Tastes Better

March 31, 2009...

1. Go to the Domino's Pizza site.
2. Order a medium one-topping pizza.
3. Enter coupon code “BAILOUT” FREE!

Still have to go pick it up!

11,000 \times $7.00 = $77,000 (per pizza)

“Spoke to a Domino's rep, who told me the free-pizza code was created internally for a promotion that was never actually green-lit.”
Scams that Scale

They make money, a little or a lot.

Generally not considered hacking.

Can do them over and over again.
Instead of using affiliate links the “traditional” way:

```html
<a href="http://AffiliateNetwork/p?
program=50&affiliate_id=100/">really cool product!</a>
```

Force affiliate requests with “Cookie Stuffing”:

```html
<iframe src="http://AffiliateNetwork/p?
program=50&affiliate_id=100/
width="0" height="0"></iframe>
```

Remove pesky referer by placing code on SSL pages:

“Clients SHOULD NOT include a Referer header field in a (non-secure) HTTP request if the referring page was transferred with a secure protocol.” - RFC 2616

Affiliate networks will get suspicious of all these requests with no referers
Referer Manipulation

High traffic site, owned by the SEO and unknown by Affiliate network. IFRAME the site with “clean” referer.

```html
<iframe src="http://niceseo/" width="0" height="0"></iframe>
```

Clean site, also owned by SEO, serves up cookie-stuffing code only to requests with referer of the black-hat website.

```html
<iframe src="http://AffiliateNetwork/p?program=50&affiliate_id=100/" width="0" height="0"></iframe>
```

To the affiliate Affiliate network everything looks 100% legit when investigating. They will never see cookie-stuffing code. Mind the impression ratio!
Manufacturing Links

Identify websites with a high PR or traffic, with **site:** search features, whose link results do not have “nofollow”, URLs block by robots.txt, and do not redirect.

“Powered by Google”, but others may work as well. Use a link farm to link to search results pages so they get indexed.

```html
<a href="http://www.weather.com/search/websearch?Keywords=site:mysite.com+keyword&start=0&num=10&twx=on&type=web">keyword pair</a>
```
Remote Firefox Vulnerabilities ha.ckers.org web application ...
I actually sat in a hacker con and watched the Errata Security guys sniff everyone’s traffic ... It’s super super easy if you know what you are looking for ...
ha.ckers.org/blog/20070530/remote-firefox-vulnerabilities/ - 20k - Cached - Similar pages

ha.ckers.org web application security lab
... double hashed because people think they’re being super clever, etc... <
DIV STYLE="background-image: url(http://router/path/to/hack)">blah</DIV> ...
ha.ckers.org/ - 45k - Cached - Similar pages

Token Authentication Gone Phishing ha.ckers.org web application ...
Hacker proof? No. Yes, time based makes it harder, and I think it’s ... You may have a super-duper algorithm or communication protocol that ...
ha.ckers.org/blog/20060817/token-authentication-gone-phishing/ - 21k - Cached - Similar pages

SES SEO News ha.ckers.org web application security lab
... there that might point the hacker to a more useful location to attack. ...
It just happens that both super good guys and super bad guys ...
ha.ckers.org/blog/20060809/ses-seo-news/ - 8k - Cached - Similar pages

Looking glasses - hacking layers 2-3 via web applications ha.ckers ...
So each super-massive-ISP sets up a script called a "looking glass" that is ...
In this way you can hack the 2-3 OSI layers via the web ...
ha.ckers.org/blog/20060620/looking-glasses-hacking-layers-2-3-via-web-applications/ - 9k - Cached - Similar pages

XSS Book ha.ckers.org web application security lab
But if I’m not super quick on the posts and answering email, .... The Javascript then pointed to PHP script on the hacker’s server. ...
ha.ckers.org/blog/20070128/xss-book/ - 25k - Cached - Similar pages
Google Maps vs. Spammers

http://thehollytree.blogspot.com/2008/02/scam-alert-phony-israeli-owned.html
Google Maps vs. Spammers

Google Local Business Center

New! Now offering a reporting dashboard. Learn how people find your business.

Write a review
1448 Willard St
San Francisco, CA 94117-3721
(415) 375-7680

Get directions: To here - From here
Add or edit your business

Help customers find you on Google, it's free.

Free listing
Local customers already search Google for the products and services you offer. Create a business listing to be sure they find you.

Free updates
Keep your address, phone number, hours of operation, and more up-to-date. Even create coupons and display photos and videos, all for free.

http://thehollytree.blogspot.com/2008/02/scam-alert-phony-israeli-owned.html
Roofer Tom Berge used the aerial photographs of towns across the world to pinpoint museums, churches and schools across south London with lead roof tiles (darker colour).

Berge and his accomplices used ladders and abseiling ropes to strip the roofs and took the lead ($164,980) in a stolen vehicle to be sold for scrap.

Sentenced to eight months in prison – suspended for two years – after confessing to over 30 offenses.

http://www.independent.co.uk/news/uk/crime/thief-googled-163100000-lead-roofs-1645734.html
Returning other people’s iPods

Nicholas Arthur Woodhams, 23 from Kalamazoo, Michigan set up shop online to repair iPods.

Abused Apple’s Advance Replacement Program by guessing iPod serial numbers backed with Visa-branded gift cards ($1 pre-auth).

Repeated the process 9,075 times, resold the “replacements” at heavily discounted prices ($49), and denied any Apple credit charges.

Charged with trademark infringement, fraud, and money-laundering.

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9130136&intsrc=news_ts_head
http://www.appleinsider.com/articles/08/06/26/apple_makes_example_of_ipod_repairman_in_lawsuit.html
http://launderingmoney.blogspot.com/2009/03/money-laundering-charges-for-kalamazoo.html
“Federal prosecutors have asked U.S. District Court Judge Robert Bell to let them seize real estate and personal property -- including a 2004 Audi and a 2006 drag racer -- as well as more than $571,000 in cash belonging to Woodhams, all alleged to be proceeds from his scam.”
A group of U.K.-based DJs provided 19 songs, to distributor Tunecore, who put them for sale on iTunes and Amazon.

Once online, the DJs opened accounts with 1,500 stolen or cloned US and British credit cards to buy $825,000 worth of their albums $10 at a time over a couple month.

Apple and Amazon paid roughly $300,000 in royalties, which boosted their chart rankings, resulting in even more sales and increased royalties for the DJs.

Apple received 'stop payment' orders from credit card companies, which led to the DJs’ arrest on suspicion of conspiracy to commit fraud and money laundering.

http://www.metro.co.uk/news/article.html?DJs_arrested_in_%A3200,000_iTunes_scam&in_article_id=682928&in_page_id=34
Mythical Super Hacker

Anyone can do this stuff!

Skill does not affect return on investment.

Competitors got caught because they didn’t try not to.
Will Hack for $, £, ¥, €, R$, ₨
Online Permit Management

In 2006, the Brazilian environment ministry did away with paper dockets and implemented an online program to issue permits documenting how much land a company could legally log and tracking the timber leaving the Amazon state of Para.

“We’ve pointed out before that this method of controlling the transport of timber was subject to fraud.”

André Muggiati
Campaigner Amazon office in Manaus
Greenpeace International
Allegedly 107 logging companies hired hackers to compromise the system, falsifying online records to increase the timber transport allocations. Police arrested 30 ring leaders. 202 people are facing prosecution.

As a result, an estimated 1.7 million cubic meters of illegal timber have been smuggled out of the Amazon, enough to fill 780 Olympic-sized swimming pools.

$833,000,000,000

Same computer system is used in two other Brazilian states.

Hiring the Good Guys

KPMG audited 70 FAA Web applications and identified 763 high-risk vulnerabilities

“By exploiting these vulnerabilities, the public could gain unauthorized access to information stored on Web application computers. Further, through these vulnerabilities, internal FAA users (employees, contractors, industry partners, etc.) could gain unauthorized access to ATC systems because the Web applications often act as front-end interfaces (providing front-door access) to ATC systems.”

Memorandum

U.S. Department of Transportation
Office of the Secretary of Transportation
Office of Inspector General


From: Rebecca C. Lang
Assistant Inspector General for Financial and Information Technology Audits

To: Acting Federal Aviation Administrator

This report presents the results of our audit of Web applications security and intrusion detection in air traffic control (ATC) systems. This audit was requested by the Ranking Minority members of the House Committee on Transportation and Infrastructure and its Aviation Subcommittee.

http://news.cnet.com/8301-1009_3-10236028-83.html
http://www.darkreading.com/security/government/showArticle.jhtml
Measure Website Security, some say...

Focus on the most important assets, test comprehensively, and get to the rest later. Defend against the **Fully Targeted** (Super Hacker). While others...

Recommend a minimum baseline for all assets, then test more thoroughly when resources allow. Defend against the **Random Opportunists** (Bots and Worms).

Success requires **FLEXIBILITY** to perform both comprehensive and scaled out testing in accordance with the organizations tolerance for risk.
Attack Classification Misnomer

Dial is a measurement of target focus, NOT skill.

No shortage of weak websites.

Forgetting to ‘not get caught’?

Learning ‘super hacker’ skillz?

Plenty of money still to be made.
‘Plan B’ Problems

$900 million
Questions?

Jeremiah Grossman
Blog: http://jeremiahgrossman.blogspot.com/
Twitter: http://twitter.com/jeremiahg
Email: jeremiah@whitehatsec.com

Trey Ford
Blog: http://treyford.wordpress.com/
Twitter: http://twitter.com/treyford
trey.ford@whitehatsec.com

WhiteHat Security
http://www.whitehatsec.com/

Link to slides also available