UBM Tech
darkreading.com

Next

SECURITY dark READING

MARCH 2013

Protect The Business Enable Access

10 WEB THREATS

That Could Harm Your Business

By Robert Lemos >>

PLUS 6 facts about recent zero-day attacks >>

What We Know About Recent Zero-Day Attacks

MATHEW J. SCHWARTZ
@mathewjschwartz

Last month, Apple, Facebook and Microsoft disclosed that attackers exploited zero-day vulnerabilities in Java browser plug-ins that their employees used, although the bad guys apparently failed to steal any customer or user data from the companies. Earlier in the month, Twitter warned that attackers compromised some 250,000 user accounts. At the time, it didn't say how the systems had been hacked, but it strongly urged users to disable Java.

Even before the companies provided details on the attacks, security experts were seeing signs that something was amiss with Java. "Apple was blocking Java, ... and the U.S. Department of Homeland Security was advising against [using] Java in the browser," says Sean Sullivan, security adviser at F-Secure. "I had a very strong feeling that something was going on."

Here are six facts we now know about the attacks:

1. Compromised iPhone developer site: All four companies apparently were compromised after their mobile developers visited a popular website devoted to iOS development called iPhoneDevSDK. The site's administrator confirms that it apparently had been hacked, and while no data appeared to have been stolen, all users' passwords have been reset as a precautionary measure. "We were alerted that our site was part of an elaborate and sophisticated attack whose victims included large Internet companies," Ian Sefferman, the site's administrator, says in a forum post.

The attackers obtained or guessed a password tied to one of the site's admin accounts. "It appears a single administrator account was compromised," Sefferman says. "The hackers used this account to modify our theme and inject JavaScript into our site. That JavaScript appears to have used a sophisticated, previously unknown exploit to hack into certain users' computers."

It's not yet clear when the drive-by-infection campaign started, but it appears to have ended on Jan. 30.

2. Malware infected Mac OS X systems: Apple has identified malware that infected a limited number of Mac systems through a vulnerability in the Java plug-in for browsers, according to a statement released by Apple. Apple has since released an update that inoculates Java 6 (for any OS X systems running it) against the exploit.

Apple says it identified a small number of systems in the company that were infected and isolated them from its network. There's no evidence that any data left Apple, the company says, and it's working closely with law enforcement to find the source of the malware.

But according to Reuters, which first reported the news of the Apple breach, it's still not clear how much data may have been stolen, or if all infected systems at the company have been identified.

3. Watering-hole technique: The four companies apparently were all exploited via a watering-hole attack in which attackers altered a legitimate website to serve mal-

INTEROP

Worried About Data?

Check out Interop Las Vegas's Risk Management and Information Security track. The IT conference and expo happens May 6-10. Use Priority Code MPIWK by March 22 to save up to $200 off the price of Conference Passes.

Register

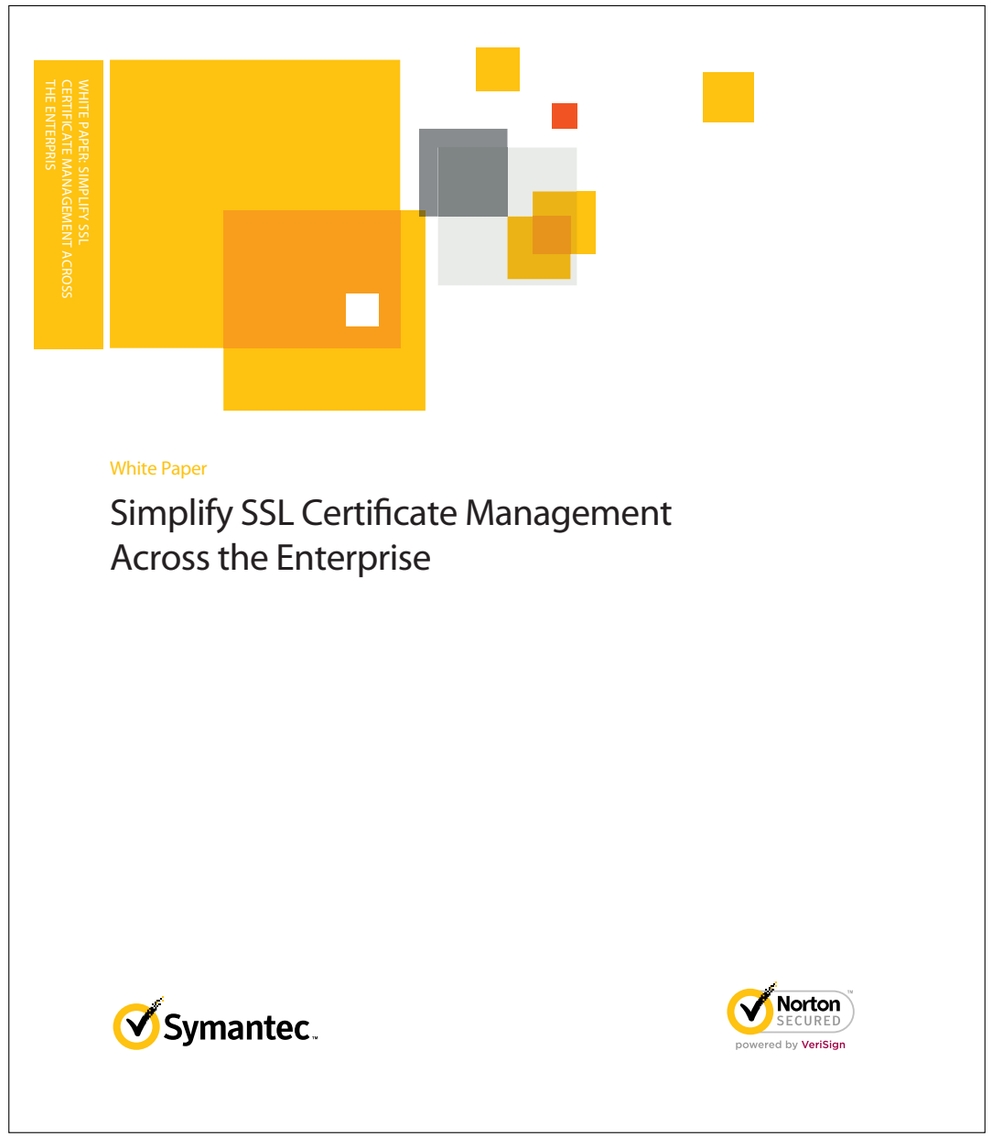
ware in advance of their targets visiting it.

In this case, attackers targeted mobile developers and succeeded in exploiting them, despite their systems being fully up to date and running antivirus software with the latest signature updates, according to a blog post from Facebook's security team. "As soon as we discovered the presence of the malware, we remediated all infected machines, informed law enforcement and began a significant investigation," says Facebook.

4. Suspicious network behavior: While antivirus software didn't spot the attacks, other defenses helped Facebook's security team spot signs of an infection. "We flagged a suspicious domain in our corporate DNS logs and tracked it back to an employee laptop," the Facebook blog post says. "Upon conducting a forensic examination of that laptop, we identified a malicious file, and then searched company-wide and flagged several other compromised employee laptops."

The attack was a previously unseen zero-day exploit that bypassed the Java sandbox to install the malware, Facebook says. "We immediately reported the exploit to Oracle, and they confirmed our findings and provided a patch on February 1, 2013, that addresses this vulnerability."

Similarly, Twitter's information security personnel detected unusual access patterns that led to it identifying unauthorized access attempts to user data, according to



Click here to download this free white paper.

For more information on Symantec SSL certificates visit www.symantec.com
Or call 1-866-893-6565 or 1-650-426-5112.

a blog post by Bob Lord, Twitter's director of information security. The attackers accessed user names, email addresses, session tokens and encrypted/salted versions of passwords, Lord says.

5. Circle the wagons: Being attacked wasn't unusual for Apple, Facebook, Microsoft and Twitter, but according to Facebook, having such an attack succeed was rare.

Facebook says it immediately shared threat intelligence with other affected businesses, though it didn't name them. "Facebook was not alone in this attack," it said. "It is clear that others were attacked and infiltrated recently as well. As one of the first companies to discover this malware, we immediately took steps to start sharing details about the infiltration with the other companies and entities that were affected."

Facebook, working with a third party, also sinkholed the command-and-control server employed by attackers, reports Ars Technica.

6. Others likely exploited: Who else might have been compromised as part of this attack campaign? Because the attackers used sites that target mobile app developers, all mobile app developers — whether using Mac OS X or Windows — should assume they've been targeted, says F-Secure's Sullivan.

What were attackers looking for? If the hackers behind the exploits are criminals, then they're likely pursuing any avenue that could lead to remuneration.

What were attackers looking for? That's not yet clear, but if the hackers behind the exploits are criminals, then they're likely pursuing any avenue that could lead to remuneration. Unfortunately for mobile code developers, that might include efforts to sneak back doors into their mobile apps.

Given that, any developers who have Java enabled in their browsers, have visited mobile developer websites in the last couple of months and find evidence their computers are compromised probably should use their source code versioning system to check recent commits, Sullivan says. "And if you don't use a source code version system (such as SVN or Git), have fun rereading your entire code base."

Mathew J. Schwartz covers information security for InformationWeek. Write to him at mat@penandcamera.com. You can find more stories by him at informationweek.com/mathewschwartz.

10 WEB THREATS That Could Harm Your Business

Easily overlooked vulnerabilities can put your data and business at risk.

By Robert Lemos

SQL injections accounted for about 7% of Web attacks in 2011 and looked to be petering out, according to security services vendor Trustwave. Then last year those exploits jumped to 26% of Web attacks, hitting companies that could have easily protected themselves.

The Trustwave data proves what hackers have known for years: Even though application vulnerabilities are well known and can be fixed or blocked, many companies don't implement secure coding practices and regularly test their applications to find them. Companies that overlook such basic Web security practices have no chance against more advanced attacks, says Chris Pogue, Trustwave's director of incident response and forensics.

Input validation, where user input — such as a search query — is limited to simple strings, is an easy way to protect against SQL injection, but developers frequently fail to do that, Pogue says. "It's one of the things that's

taught in college, and if it has made it into the university system, then it's not bleeding-edge technology," he says.

The Web presents a variety of security threats for unwary businesses, from well-known SQL injection and cross-site scripting attacks to more esoteric threats posed by Web scraping and HTML5's many features. What follows are 10 Web threats we think are particularly worrisome, either because they're becoming more popular with attackers or because security pros and developers tend to overlook them.

1. Bigger, Subtler DDoS Attacks

When IT specialists think about distributed denial-of-service attacks, they envision the most basic kind: floods of packets overwhelming a victim's network so that valid requests can't get through. But improvements in defenses have forced attackers to change the way they attack.

Packet floods have become larger, maxing out at 100 Gbps. In a six-month campaign against U.S. banks, for which a group of alleged Muslim hacktivists claimed credit, the volume of attack traffic has regularly surpassed 30 Gbps — throughput rarely seen five years ago.

Attackers also have targeted other parts of the infrastructure. Corporate domain name service servers are a favorite target, according to domain registrar VeriSign. When attackers take DNS servers down, customers can no longer access a company's service. "It doesn't matter how much data center capacity a company has, the requests will never reach their data centers," says Sean Leach, VP of technology for VeriSign's network intelligence and availability group.

Massive DDoS attacks often mask "low-and-slow" attacks, which use specially crafted requests to cause Web applications or appliances handling specific services, such as Secure Sockets Layer communications, to quickly consume processing and memory resources. These application-layer attacks now account for about a quarter of all attacks.

"If the mega-DDoS attacks are the cavemen getting bigger clubs, [low-and-slow] attacks are like the caveman evolving, getting smarter," says Matthew Prince, CEO of Internet security company CloudFlare.

Attackers look for URLs on a target site and then make calls to the back-end database that powers the site. Frequent calls to those Web pages quickly consume a modest site's resources, says John Summers, VP of security products at Akamai Technologies. "The targeting is much better this year than in 2011," Summers says. Attackers "are doing their homework, doing reconnaissance."

It's no longer enough for companies to use an appliance to block bad traffic as it enters their networks because the router will still be overwhelmed in a low-and-slow attack. These attacks can also get through a cloud DDoS mitigation service. Instead, companies should go with a hybrid approach, using Web application firewalls, network security appliances and content distribution networks to create a layered defense that screens out unwanted traffic at the earliest possible point.

2. Old Browsers, Vulnerable Plug-Ins

Cyber attacks that account for millions of dollars a year in bank account fraud are fueled by browser vulnerabilities and, more frequently, the browser plug-ins that handle Or-

JAVA, FLASH, READER — OH MY!

3% of users are vulnerable because Java plug-ins aren't updated regularly

19% of users are vulnerable because Adobe Reader plug-ins aren't updated

10% of users are vulnerable because Flash plug-ins aren't updated

Data: Zscaler's State Of The Web report, 4Q 2012

SECURITY dark READING

Don't Be Vulnerable

Dark Reading's Vulnerability Management Tech Center is your portal to news, best practices and other data related to detecting and remediating security vulnerabilities.

Click Here

acle's Java and Adobe's Flash and Reader. Exploit kits bring together a dozen or so attacks on various vulnerable components and can quickly compromise a company's systems if the patches aren't up to date.

A recent version of the popular Blackhole exploit kit, for example, contained attacks for 16 vulnerabilities, including seven targeting the Java browser plug-in, five targeting the Adobe PDF Reader plug-in and two targeting Flash, according to anti-malware firm Sophos. The Sweet Orange exploit kit contains Java, PDF, Internet Explorer and Firefox exploits, according to the creator's statements that security firm Webroot discovered. "These exploit kits are really good at identifying which vulnerabilities are unpatched in the browsers that people are running," says Grayson Milbourne, Webroot's senior threat researcher.

Companies should pay attention to Oracle's Java plug-in in particular. Cybercriminals are focusing on Java because it's widely deployed but poorly patched, says Michael Sutton, VP of research at Zscaler, a security-as-a-service provider.

Only 4% of systems at companies using Zscaler's security service have the Java plug-in installed, but almost 80% of those Java plug-ins are out of date, according to the provider's data for the last quarter of 2012. Adobe's Flash and Reader plug-ins are more ubiquitous but better patched, Sutton says. "Companies haven't grasped the problem of how Java plug-ins have been abused," he says.

Patching is the most obvious way to protect against this vulnerability. A number of patch management products, such as Qualys for large companies and Secunia for small and midsize businesses, are available. Companies that want to protect against zero-day attacks (for which a patch hasn't been released) should use anti-malware software such as ValidEdge (recently acquired by McAfee) and Invincea, which runs downloaded files in a sandbox.

3. Good Sites Hosting Bad Content

Attackers are targeting well-known, legitimate websites to take advantage of users' trust in those sites. For example, in the VOHO watering hole attack last year, attackers infected legitimate financial and tech industry websites in Massachusetts and Washington, D.C., commonly accessed by their intended victims, says security vendor RSA.

Such tactics are difficult to explain to employees, and technical defenses aren't always enough, says Dan Ingevaldson, CTO at Easy Solutions, a fraud protection company. "You can't stop it by asking users to browse well-known websites, because the fact that the site is legitimate doesn't matter," he says.

A more insidious attack, malvertising, is the insertion of malicious content into an ad network. The malicious ad may crop up only occasionally in the network's rotation, making the attack difficult to detect.

It's a serious issue, says Robert Hoblit, senior

director of product management for Symantec. "When you're serving malvertising to your end users, you're going to get blacklisted and you'll lose revenue," he says.

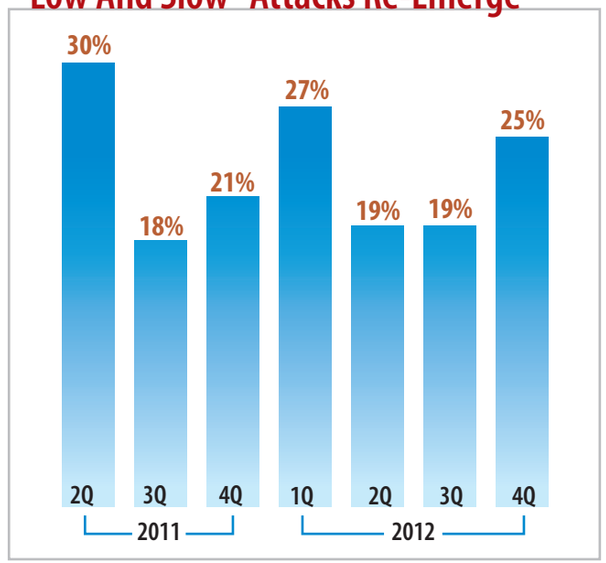
Again, a layered defense will help stop both watering hole and malvertising attacks. Security proxies that clean Web traffic and attempt to catch malicious executables work well, but they should be paired with anti-malware protection on employees' computers to catch the execution of known threats.

4. Mobile Apps And The Unsecured Web

The bring-your-own-device movement has led to a surge in consumer-owned devices inside corporate firewalls. But mobile apps are notoriously poorly programmed, putting business data at risk, says Zscaler's Sutton. There's been a lot of talk about the increasing amount of mobile malware published online, but few security experts are issuing warnings about how programming mistakes turn legitimate mobile apps into dangerous threats.

Nearly 60% of mobile apps Zscaler has studied are grabbing unique hardware information from devices and passing it over Web interfaces, Sutton says. Worse, about 10% of the applications aren't transmitting users' credentials securely, he says.

"Low And Slow" Attacks Re-Emerge



Data: Prolexic's Quarterly Denial-Of-Service Attack reports, 2Q 2011 to 4Q 2012

Part of the problem is that Google's and Apple's app stores aren't as secure as they should be. Mobile app security should be better than in the PC world because these app stores act as gatekeepers, "but they're clearly not catching these issues," Sutton says.

Furthermore, the Web services that power many mobile apps are poorly programmed. Because users don't like to type passwords to use services from their mobile devices, mobile apps often use session tokens that don't expire. Attackers can sniff traffic at Wi-Fi hotspots and pick out these tokens, letting them access their victims' accounts.

"The guy who sniffed that traffic … can be you for a year," says Dan Kuykendall, CTO at NT Objectives, a Web application security provider. Sound security programming is the best way to defeat these sorts of man-in-the-middle attacks, but it's not being applied to mobile apps, Kuykendall says. "We're seeing a lot of Web security 1999 problems — wide open stuff," he says. A new generation of developers isn't putting the necessary defenses in place to stop malicious hacking, and "we know that's a very bad assumption to make," he says.

Companies do find it difficult to limit the applications loaded onto an employee-owned phone. But they can limit the data that workers put on their devices or in the cloud and limit the devices to a corporate DMZ.

5. Failing To Clean Up Bad Input

Since 2010, SQL injection has held the top spot on the Open Web Application Security Project's list of top 10 security vulnerabilities. Dynamic websites that pass search queries or other application inputs to a back-end database server are vulnerable to SQL injection. But the simple fix, as mentioned earlier, is to check all user-provided input to make sure it's valid.

Companies often focus on their main web-

site when fixing SQL flaws and forget to lock down other connected sites, such as remote collaboration systems and contractor time-tracking systems. Attackers can use those other sites to infect employees' systems and gain access to the internal network without the need to circumvent security measures on the victim company's main site, says Jeremiah Grossman, CTO at Web application security firm WhiteHat.

To minimize SQL injection flaws, pick a software development framework and commit to it, Grossman says. As long as the developers stick to programming in that framework and keep its patches up to date, they'll create secure code, Grossman says.

6. The Hazards Of Certificates

Two years ago, a series of hacks against certificate authorities — the companies that determine who's trusted online — gave attackers the tools they needed to issue fraudulent SSL certificates that could disguise a malicious website as a legitimate, well-known company's site. The attacks, against Comodo, DigiNotar and other certificate authorities, underscored the danger of relying too much on a single security technology.

These attacks also highlighted the blind trust that companies were putting in certificates. In addition to letting attackers create authentic-looking malicious sites and services, fraudulent and stolen certificates also let them sign malicious code to make that code appear legitimate. Browser makers generally decide which certificates

Click here to download this free white paper.

For more information on Symantec SSL certificates visit www.symantec.com
Or call 1-866-893-6565 or 1-650-426-5112.

to trust, but businesses do have control over their own encryption keys and certificates.

Poor certificate management can lead to expensive incidents. The average large company is expected to lose $35 million in the next two years from certificate-related incidents, according to a Ponemon Institute study funded by Venafi, a certificate management provider. Venafi often finds companies storing certificates in the open on developer systems. Instead, they should create a centralized and well-secured repository where they can track certificate use and revoke certs when they're found to be compromised.

7. The Cross-Site Scripting Problem

Attacks exploiting cross-site scripting flaws let the attacker run scripts as if they came from a vulnerable website. They don't give the attacker access to the vulnerable website but instead target the users that go to that site. An attacker going after a banking site with a cross-site scripting vulnerability could run a script for a login box on the bank's page and steal users' credentials. "XSS exploits the trust that a browser has for a website," WhiteHat's Grossman says.

More than 70% of the applications checked by code-security firm Veracode contain cross-site scripting flaws. The vulnerability is the top issue affecting commercial open source and internally developed software, Veracode says.

Automated code-checking tools, such as those from Hewlett-Packard's Fortify, Veracode and WhiteHat, can detect cross-site scripting issues. Companies should modify their development processes to check code for defects before it's put into production. This approach will catch common coding mistakes and trains developers to avoid them in the future.

8. The Insecure 'Internet Of Things'

Routers and printers, videoconferencing systems, door locks and other devices are now networked via Internet protocols and even have embedded Web servers. In many cases, the software on these devices is an older version of an open source library that's difficult, if not impossible, to update. Welcome to the Internet of things.

An Internet-enabled device is "a great stealth back door into an enterprise for an attacker," says Zscaler's Sutton. "It has everything you need to get in."

Most companies don't bother securing their Internet-accessible printers and videoconferencing systems, for instance, so attackers find those vulnerable systems and take them over. Once a device is owned by the attacker, it serves as a bridge into the company's network.

A recent Internet scan by vulnerability management firm Rapid7 found 40 million to 50 million accessible devices using one of three libraries for the Universal Plug and Play protocol, which are known to contain vulnerabilities.

End users, businesses and ISPs should identify and disable any Internet-exposed UPnP endpoints in their environments, says HD Moore, Rapid7's chief security officer. "UPnP is pervasive. It's enabled by default on many home gateways, nearly all network printers and devices ranging from IP cameras to network storage servers," he says.

Hunting down vulnerable network devices needs to be easier, Zscaler's Sutton says. General-purpose tools designed to scan PCs and servers usually don't give reliable information about

REAL RISKS

Trustwave's analysis of attacks at its clients, which typically include restaurants and retailers.

61% of client-side attacks exploit vulnerabilities in the Adobe Reader plug-in

70% are generated by the Blackhole exploit kit

73% of attacks on Web servers involved either SQL injection or remote-file inclusion

Data: Trustwave's 2013 Global Security report

embedded devices, but there are tools that will identify vulnerable devices, such as Rapid7's ScanNow and open source tools such as Nmap.

9. Getting In The Front Door

Not all attacks are aimed at breaching a company's defenses. Automated Web bots scrape from Web pages information that can give a competitor better intelligence on your business. For example, if you have an online store, a competitor could collect data on your pricing from publicly available information on your site, says Marc Gaffan, co-founder of Web security firm Incapsula. "Are they breaching your site? No, but they are harming your business," he says. More than 30% of Web traffic to the average site is this sort of unwanted, potentially business-sapping traffic, Gaffan says.

Web application firewall services such as Incapsula and CloudFlare let businesses identify which traffic is connected to good search-indexing bots and which are bad market intelligence services or even fake Google bots. Such services block the requests, preventing information from going to competitors.

10. New Technology, Same Problems

Stanford graduate student and computer security researcher Feross Aboukhadijeh recently showed how an HTML5 feature could let an attacker pull off a convincing phishing attack. Using HTML5's ability to trigger full-screen mode, Aboukhadijeh created a large database of simulated pages that could fool users into thinking they had gone to a bank's website when, in fact, they were on an attacker's site.

Using Firefox on Mac OS X to click on a link that appears to go to Bank of America's consumer banking site? No problem. With Aboukhadijeh's attack that link is on an attacker-controlled page, and your click is intercepted. Since some browsers don't notify users that they're entering full-screen mode, attackers can throw up a full-screen disguise for any site and then use the fake site to obtain victims' login credentials.

In this case, rather than sending you to *bankofamerica.com*, the attacker throws up a full-screen page that makes it appear you're on the real Bank of America site. A careful inspection could tip off users to the fact that parts of the screen, such as the menu bar, don't match their normal desktop, but most people won't look that closely.

"Links are the bread and butter of the Web," Aboukhadijeh wrote on his site. "People click links all day long — people are pretty trained to think that clicking a link on the Web is safe. Savvy users may check the link's destination in the status bar before clicking. However, in this case, it won't do them any good." That's because the attacker can make the fake site appear to go to the real site, say, *bofa.com*.

The automated security tools that could eliminate HTML5 security issues aren't available yet, says NT Objectives' Kuykendall. "People are outpacing their security tools, which is going to leave them exposed," he says.

Training developers in secure practices, especially with new platforms such as HTML5, is a critical first step to preventing security problems. In addition, having developers check one another's code can cut down on vulnerabilities.

As with any collection of threats, businesses will find themselves with different exposures. An online business may have SQL injection and HTML5 issues, while a firm with a lot of telecommuters may have mobile issues, including exposed devices with embedded vulnerabilities. Rather than attempt to minimize the dangers from every threat, companies should focus on the subset of vulnerabilities where they're most exposed.

Write to us at editors@darkreading.com.

dark READING *Online, Newsletters, Events, Research*

Tim Wilson Dark Reading Site Editor
timothy.wilson@ubm.com 703-262-0680

Kelly Jackson-Higgins Dark Reading Senior Editor
kelly.jackson.higgins@ubm.com 434-960-9899

Rob Preston VP and Editor In Chief
rob.preston@ubm.com 516-562-5692

Chris Murphy Editor
chris.murphy@ubm.com 414-906-5331

Stacey Peterson Executive Editor, Quality
stacey.peterson@ubm.com 516-562-5933

Lorna Garey Content Director, Reports
lorna.garey@ubm.com 978-694-1681

Jim Donahue Chief Copy Editor
james.donahue@ubm.com

Mary Ellen Forte Senior Art Director
maryellen.forte@ubm.com

Sek Leung Associate Art Director
sek.leung@ubm.com

Business Contacts

Chief Sales Officer, Business Technology Media, Martha Schwartz
(212) 600-3015, martha.schwartz@ubm.com

Sales Specialist, Sal Silletti
(212) 600-3029, salvatore.silletti@ubm.com

SALES CONTACTS—WEST

Western U.S. (Pacific and Mountain states) and Western Canada (British Columbia, Alberta)

Western Regional Sales Director, Sandra Kupiec
(415) 947-6922, sandra.kupiec@ubm.com

Strategic Account Director, Coretta Wright
(415) 947-6245, coretta.wright@ubm.com

District Sales Manager, Vanessa Tormey
(805) 284-6023, vanessa.tormey@ubm.com

Account Manager, Ashley Cohen
(415) 947-6349, ashley.i.cohen@ubm.com

Strategic Accounts

Account Manager, Vesna Beso
(415) 947-6104, vesna.beso@ubm.com

SALES CONTACTS—EAST

Midwest, South, Northeast U.S. and Eastern Canada (Saskatchewan, Ontario, Quebec, New Brunswick)

District Manager, Jenny Hanna
(516) 562-5116, jenny.hanna@ubm.com

District Manager, Michael Greenhut
(516) 562-5044, michael.greenhut@ubm.com

District Manager, Cori Gordon
(516) 562-5181, cori.gordon@ubm.com

Inside Sales Manager East, Ray Capitelli
(212) 600-3045, raymond.capitelli@ubm.com

Strategic Accounts

District Manager, Mary Hyland
(516) 562-5120, mary.hyland@ubm.com

Account Manager, Tara Bradeen
(212) 600-3347, tara.bradeen@ubm.com

SALES CONTACTS—MARKETING AS A SERVICE

Director of Client Marketing Strategy, Jonathan Vlock
(212) 600-3019, jonathan.vlock@ubm.com

Director of Client Marketing Strategy, Julie Supinski
(415) 947-6887, julie.supinski@ubm.com

SALES CONTACTS—EVENTS

Senior Director, InformationWeek Events, Robyn Duda
(212) 600-3046, robyn.duda@ubm.com

MARKETING

VP, Marketing, Winnie Ng-Schuchman
(631) 406-6507, winnie.ng@ubm.com

Senior Marketing Manager, Monique Lutrell
(949) 223-3609, monique.luttrell@ubm.com

Promotions Manager, Angela Lee-Moll
(516) 562-5803, angela.lee-moll@ubm.com

UBM TECH

Paul Miller CEO

Kathy Astromoff CEO, Electronics

Robert Faletra CEO, Channel

Edward Grossman President, Business Technology Media

Marco Pardi President, Business Technology Events

David Berlind Chief Content Officer

Sandra Wallach CFO

David Michael CIO

Martha Schwartz Chief Sales Officer, Business Technology Media

Scott Vaughan Chief Marketing Officer

Simon Carless Exec. VP, Game & App Development and Black Hat

Lenny Heymann Exec. VP, New Markets

Angela Scalpello Senior VP, People & Culture

Copyright 2013 UBM LLC. All rights reserved.

READER SERVICES

DarkReading.com The destination for the latest news on IT security threats, technology, and best practices

Electronic Newsletters Subscribe to Dark Reading's daily newsletter and other newsletters at darkreading.com/newsletters/subscribe.jhtml

Events Get the latest on our live events and Net events at informationweek.com/events

Reports reports.informationweek.com for original research and strategic advice

How to Contact Us
darkreading.com/aboutus_editorial.jhtml

Editorial Calendar informationweek.com/edcal

Back Issues
E-mail: customerservice@informationweek.com
Phone: 888-664-3332 (U.S.)
847-763-9588 (Outside U.S.)

Reprints Wright's Media, 1-877-652-5295
Web: wrightsmedia.com/reprints/?magid=2196
E-mail: ubmreprints@wrightsmedia.com

List Rentals Specialists Marketing Services Inc.
E-mail: PeterCan@SMS-Inc.com
Phone: (631) 787-3008 x30203

Media Kits and Advertising Contacts
createyournextcustomer.com/contact-us

Letters to the Editor E-mail editors@darkreading.com. Include name, title, company, city, and daytime phone number.

Subscriptions
Web: informationweek.com/magazine
E-mail: customerservice@informationweek.com
Phone: 888-664-3332 (U.S.)
847-763-9588 (Outside U.S.)

UBM Tech