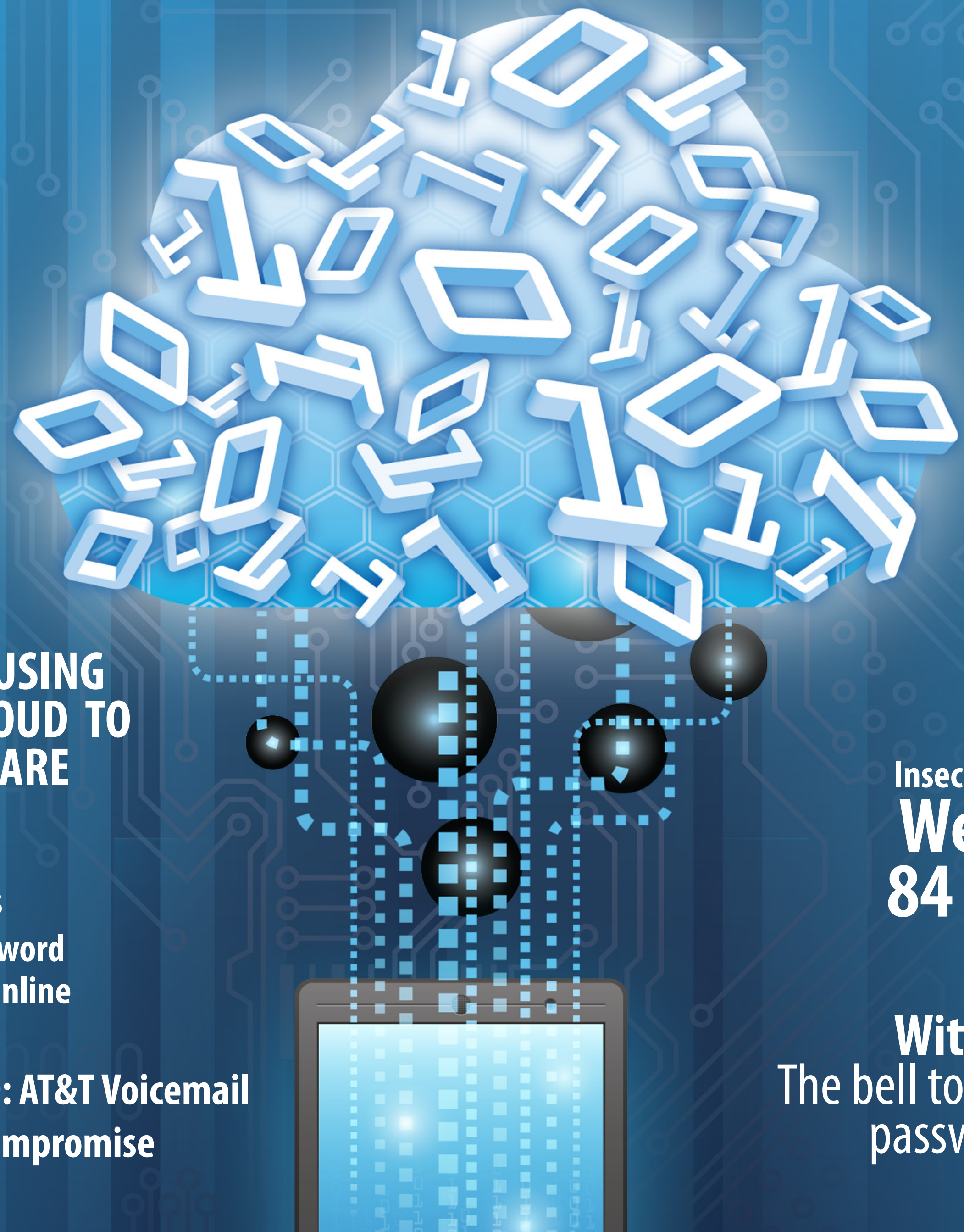
Spotlight Series

threatpost

The Kaspersky Lab Security News Service

# CLOUD (IN) SECURITY

## THE CLOUD: *WHAT IS IT?*



**ATTACKERS USING AMAZON CLOUD TO HOST MALWARE**

**Social Site Formspring Says 420K User Password Hashes Posted Online**

**Cloudflare CEO: AT&T Voicemail Hack Key To Compromise**

**Insecure Applications: We Are the 84 Percent!**

**With LinkedIn:** The bell tolls for simple password hashing

**Featured Articles:**

- Attackers Using Amazon Cloud to Host Malware
- Social Site Formspring Says 420k User Password Hashes Posted Online
- Insecure Applications: We Are The 84 Percent!
- With LinkedIn: The Bell Tolls For Simple Password Hashing
- Cloudflare CEO: AT&T Voicemail Hack Key To Compromise

## "The Cloud" - What Is it?

*"Cloud computing" is loosely defined as the technology revolution that has allowed both computing power and storage to be delivered as a service, using Internet-hosted resources. It is one of the most important technological developments of the last half century – as important as the development of the Internet, without which it couldn't exist. Today, cloud based computing resources power everything from Google's search engine, to Facebook to online banking, flight reservation and distance learning systems.*

*The cloud has been a boon to organizations of all sizes. Large companies have been able to drastically reduce the cost of running data centers by leasing cloud-based computing resources managed by a third party, such as Amazon.com. At the same time, small companies and entrepreneurs have seen the barriers to developing and launching entire new products all but disappear. Today, startups located virtually anywhere on the globe can quickly assemble, communicate, share ideas, market to customers and conduct business online. Office space, desks, chairs and telephones are optional. Forrester Research estimates that cloud computing would be a $240 billion industry by the start of the next decade.*

*Under the hood: cloud computing is the product of a number of important technological developments over the past few decades. There's the advent of the Internet and, within the last decade, high capacity data networks for businesses, private residences and, eventually, wireless devices. Then there are enabling technologies like hardware and software virtualization that allow many "virtual" computers to run on a single hardware platform, and development methodologies like Services Oriented Architecture (SOA) that have enabled the creation of modular, Web based services that link disparate applications. In all, cloud computing has changed the entire consumption model for computing power from one dominated by owner-operators – mostly big corporations and the government - to a "utility" model (akin to the electrical grid) in which computing resources are aggregated and managed more centrally and then distributed to customers of all sizes who pay based on their use of the service.*

## (In)Security in the Cloud

*Given the resilience and elastic nature of cloud based infrastructure, it is no surprise that organizations realized; early on, that the cloud can be a life saver, especially in the event of a cyber attack. The whistle blower web site Wikileaks famously moved its collection of a quarter million purloined State Department documents to Amazon.com's massive EC2 (Elastic Compute Cloud) infrastructure to sidestep crippling denial of service attacks in late 2010. The Tor Project, in 2011, announced plans to leverage EC2 to help its users – some political dissidents - set up Tor bridges to help skirt around* *repressive regimes that wish to block traffic to the clandestine communications network. But the massive scale of cloud operations and the relative anonymity with which individuals can access them has also been a boon to the folks who wear the black hats. A report in June, 2011, found that attackers are beginning to host their malicious domains and drive-by download sites on Amazon's EC2 cloud platform. The sites were being used to install malware as part of a spam and phishing campaign designed to steal banking credentials and other sensitive data.*

## Attackers Using Amazon Cloud to Host Malware

**By Dennis Fisher**

Attackers are beginning to host their malicious domains and drive-by download sites, and most recently researchers have discovered a number of domains on Amazon's cloud platform that are being used to install malware as part of a spam and phishing campaign designed to steal banking credentials and other sensitive data.

The current attack sites are installing a variety of malicious files on victims' machines, including a component that acts as a rootkit and attempts to disable installed anti-malware applications. Other components that are downloaded during the attack include one that tries to steal login information from a list of nine banks in Brazil and two other international banks, another that steals digital certificates from eTokens stored on the machine and one that collects unique data about the PC itself, which is used by some banks as part of an authentication routine.

Researchers say that the attacks likely originated in Brazil and are targeting users in Brazil, specifically. The domains that are being used in this attack have now been removed by Amazon, according to Kaspersky Lab researcher Dmitry Bestuzhev, who discovered the malicious domains.

"As of yesterday (June 6), all malicious links have been taken down by Amazon Web Services and are no longer active. Brazilian cyber criminals intentionally launched the attack on Friday night. They know that usually it takes more time to detect and neutralize threats launched during the weekend. The same technique has been widely used by phishers for a while," he wrote.

The attacks begin as spam/phishing campaigns in which users are sent spoofed emails with links that take them to one of the malicious domains, exactly the same sort of attack scenario that's been used in normal phishing campaigns for the better part of a decade now. The only difference is that instead of hosting the malicious site on a bulletproof hosting service or a compromised domain, they're using domains hosted by Amazon. It's simply a new twist on an old attack.

Attackers have been using compromised legitimate domains as launching pads for drive-by downloads for years now, and they also will utilize the services of hosting providers who actively ignore the presence of malicious domains on their servers. Some of these co-called bulletproof hosting providers will remove malicious domains when notified by researchers, but others will simply ignore those requests.

*Threatpost reported, also, that the cybercriminals responsible for the SpyEye family of malware jumped on Amazon's S3 cloud based storage offering. Using stolen identities, the fraudsters set up S3 accounts and used them as a jumping off point for SpyEye attacks.*

*More than just using massive cloud-based server farms to host malicious content, malicious actors are using cloud based systems like never before: harnessing the kind of raw computing power once reserved for governments and the military. Access to massive clusters of specialized GPU (graphics processing unit) –based systems on platforms like Amazons has torn down the barriers to cracking even complex passwords and password hashes, as Threatpost reported after hackers made off with millions of passwords from the online music streaming service Last.fm, professional networking site LinkedIn.com and, most recently, Web based Q&A site Formspring.com.*

## Social Site Formspring Says 420k User Password Hashes Posted Online

**By Dennis Fisher**

Hackers broke into a development server at Formspring, a social Q&A site, and made off with the password hashes for 420,000 users and later posted them online. The company has reset all of the users' passwords and said it also has changed the way that it handles passwords.

Formspring officials said on Tuesday that they had discovered the incident that morning and later discovered that some of the hashes had been posted online. The company decided to reset the passwords for all of its users.

"We were notified that approximately 420,000 password hashes were posted to a security forum, with suspicion from a user that they could be Formspring passwords. The post did not contain usernames or any other identifying information," the company said in a blog post.

"Once we were able to verify that the hashes were obtained from Formspring, we locked down our systems and began an investigation to determine the nature of the breach. We found that someone had broken into one of our development servers and was able to use that access to extract account information from a production database."

Formspring officials said that the company was using SHA-256 with random salts to protect user passwords. After the incident, the company switched to Bcrypt, a hash algorithm that's based on Bruce Schneier's Blowfish algorithm. SHA-256 is one version of the SHA-2 hash function and there are known security issues with it.

This leak is simply the latest in a years-long series of such incidents. One of the more recent breaches was the attack on LinkedIn, the huge professional social network, in which the hashes of more than 6 million users' passwords were leaked. In that case, LinkedIn was using SHA-1, an older and less secure hash function, to secure user passwords, and one woman affected by the breach later sued the company for failing to take adequate security measures.

## Insecure Applications: We Are The 84 Percent!

**By Paul Roberts**

You only have to glance at the headlines to know that the state of computer application security is bad. But a new report from Veracode makes clear how bad: just 16 percent of almost 10,000 applications tested in the last six months received a passing security grade on their first attempt.

The finding, presented in the latest, semi annual State of Software Security Report, is a marked departure from Veracode's report six months ago, in which 42% of the applications tested passed on their first try. Application security experts at the company reported continued problems with insecure Web applications in use by government agencies, and a plethora of insecure mobile applications.

The precipitous drop in the "pass" rate for applications was caused by the introduction of new, tougher grading guidelines, including a "zero tolerance" policy on common errors like SQL injection and cross site scripting holes in applications, Veracode said.

The report compiles the results of eighteen months of automated and manual testing on 9,900 applications said Sam King, Veracode's Senior Vice President of Marketing. Researchers at the company expected to see a drop in the pass rate after instituting the new, tougher standard. But they were still surprised by ho big a drop there was, King said.

The new, tougher policy on vulnerabilities like SQL injection and cross site scripting reflect the reality of the threat landscape and the demands of customers, said Chris Wysopal, Veracode's Chief Technology Officer.

"In the past, applications might get away with a certain number of medium criticality vulnerabilities. But our customers were saying: that's not right. We don't want to buy or build anything that has a SQL injection or cross site scripting hole."

SQL injection and cross site scripting vulnerabilities were among the most commonly used holes exploited by groups such as Anonymous and LulzSec in the last year, King noted. In just one attack in April, dubbed "Lizamoon," thousands of websites around the globe were targeted with SQL injection attacks that redirected visitors to a rogue anti-virus (AV) site. Indeed, many security experts consider SQL injection attacks to be an "epidemic."

Veracode found 40% of government Web sites were found to contain SQL injection vulnerabilities on their first scan, compared with 29% of Web sites for financial-sector firms and 30% of software vertical sites. Overall, the prevalence of SQL injection holes declined from the same period six months ago, Veracode found, though that wasn't the case with government sites.

The story was even more grim with cross site scripting vulnerabilities. Seventy five percent of the government Web sites Veracode tested had cross site scripting holes on their first try. Finance sites faired only slightly better: 67% contained at least one cross site scripting hole and 55% of software industry Web sites.

In past reports, Veracode has warned about the danger posed by the use and reuse of canned, third party application code. That continues to be a problem, said Wysopal. Between 30 percent and 70 percent of internally developed applications turn out to be reused, third party code, mostly in the form of third party libraries, Veracode found. Often that ties directly into the prevalence of vulnerabilities. For example, Veracode believes that the high incidence of cross site scripting holes in government applications is linked to the greater use of the Adobe ColdFusion development platform by developers working within the government.

Veracode researchers also surveyed mobile applications for Google's Android operating system. Wysopal said that many of the applications tested used encryption to protect data sent back and forth over mobile networks. However, often those applications had sloppy implementations of encryption, with cryptographic "private" keys hard coded into the mobile application. "If anyone gets access to the application - the phone is lost, for example - they could extract that key and have access to personal information," Wysopal said. "Its difficult for organizations to recover from that kind of loss, which is why its really bad practice to put credentials in applications."

Still, Wysopal and team found some reason for optimism. The increase in the number of applications tested is a testament to the growing demand for application testing. And Wysopal believes that many common development frameworks are getting better in helping developers spot and prevent common mistakes like SQL injection. There's more awareness of the problem of Web application vulnerabilities, also, he said.

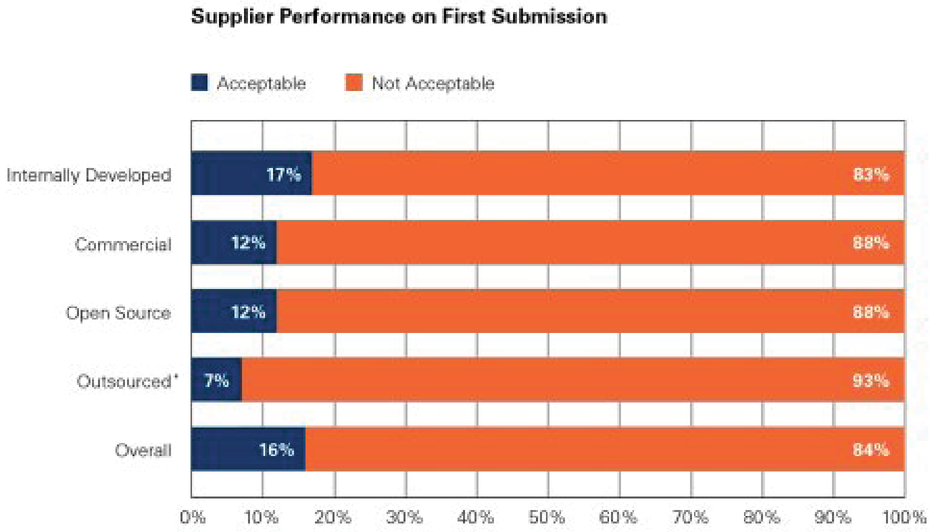


Figure 3: Supplier Performance on First Submission

*Low sample size

"Five years ago, it was rare to find a developer who even knew about SQL injection. That's definitely changing," he said.

*With cloud based computing, attackers suddenly have the power to break strong encryption algorithms. They have the luxury of checking every possible password combination (up to a certain length) in a short enough time period to make attacks plausible. At the same time, leaked lists of known passwords,  such as the 32 million passwords exposed in a breach of social media application developer RockYou in 2010 or the more recent Stratfor breach. Humans being what they are, the chances that a password in a list of leaked passwords will match a one used by someone else is good.*

*This is the public cloud working against you," Josh Shaul, the CTO of Application Security, Inc., told Threatpost's Paul Roberts. "You can spin up multiple (GPU) instances at Amazon and calculate rainbow tables at an amazingly fast rate," he said, referring to massive tables of hash digests and their corresponding message equivalents.*

## With LinkedIn: The Bell Tolls For Simple Password Hashing

**By Paul Roberts**

This week's revelations about leaks of user passwords from the professional networking site LinkedIn, dating Web site eHarmony.com and music site Last.fm suggest that even tech-savvy firms are slow to accept that hashes -a once-reliable technology for storing data online - now offer scant protection for sensitive data.

The exponential growth in computing power described by Moore's Law and the advent of massive pools of elastic computing power in cloud based pools like Amazon's EC2 have broken down the walls that used to make passwords protected by hashing algorithms like SHA-1 and MD-5 all but unbreakable. Despite that, many companies - including tech savvy Internet firms - continue to rely on insecure hashing algorithms and permit users to use inadequate passwords to protect sensitive accounts, data security experts say.

LinkedIn responded on June 6 to reports of a file containing hashed password values that had been posted on a Russian Web site. The company acknowledged that it was investigating a possible data breach that may have leaked 6.5 million password hashes. The passwords were posted on a Russian web forum, InsidePro, and hackers were encouraged to help decipher the reportedly unsalted SHA-1 hashes. In the days that followed, eHarmony.com and Last.fm followed suit and announced that hashed passwords for their users, also, had been leaked.

As Threatpost.com reported, eHarmony and Last.fmencouraged their users to change their passwords as a precautionary measure. In a blog post Thursday, LinkedIn Director Vicente Silveira said that his company was resetting the passwords of affected members, and that LinkedIn members who update their passwords will benefit "enhanced security" the company"recently put in place," that includes "hashing and salting of our current password databases." The company revealed previously that its passwords were encrypted using the SHA-1 hashing algorithm, but that no additional "salt" or unique additional data, was added to the password to complicate the work of potential crackers. In a remarkably similar announcement, Last.fm said in a blog post Friday that it has implemented 'more rigorous' security for customer account passwords in the wake of reports that some of those passwords had been leaked online.

Hashing is a so-called "one way" encryption process during which a block of data (or "message") of arbitrary length is fed into a specialized cryptographic function, such as an algorithm, which returns a string (or "digest") of fixed length. The string that is produced is unique to the data that was submitted and changing the input data in any way will change the string that is output on the other end. Hashing has proven to be an effective and desirable way to secure passwords because it allows companies to verify access to an account without having to store actual password values. Hashes are resistant to cracking and can be stored and queried efficiently.

But a steady stream of reports and breaches make it clear that, while useful, simple hashing is no longer sufficient to protect sensitive data like account passwords. In particular, the advent of massive pools of elastic computing power through servies like Amazon's EC2 cloud have put computing power necessary to crack password hashes in the hands of average consumers.

"This is the public cloud working against you," said Josh Shaul, the CTO of Application Security, Inc., a New York-based provider of database security software. "You can spin up multiple (GPU) instances at Amazon and calculate rainbow tables at an amazingly fast rate," he said, referring to massive tables of precomputed hash digests and their corresponding message equivalents.

Prior to the advent of the public cloud, only nation states could muster the computing power necessary to create rainbow tables for passwords of a credible length, but no longer, Shaul said.

"You'll need some money to do it. But not a lot."

Today, attackers benefit from precomputed hashes based on huge, public stores of leaked passwords, such as the 32 million passwords exposed in a breach of social media application developer RockYou in 2010 or the more recent Stratfor breach. Humans being what they are, the chances that any given password in a list of leaked passwords will match a password used by someone else is good.

So, while hashing passwords might be better than storing data in the clear, straight hashing of short or even moderate length passwords is really not much different from storing the passwords in the clear, says Shaul.

Security researchers and cryptographers are beginning to acknowledge that the advent of cloud based computing is making once secure technologies vulnerable. In a blog post on Thursday, Poul-Henning Kamp, who designed the md5crypt password scrambler, advised those using the tool that modern computing power made md5crypt, which he first released in 1995, insecure. "New research has shown that (md5crypt) can be run at a rate close to 1 million checks per second on COTS GPU (commercial off the shelf graphics processing unit) hardware," he wrote. "Any 8 character password can be found in a couple of days."

LinkedIn made it easier for attackers by failing to take steps to make the hash values harder to derive, says Terence Spies, Chief Technology Officer at Voltage Security, which provides encryption and key management products for cloud providers and enterprises. The social networking company employed the SHA-1 hashing algorithm to secure its passwords, but merely passed the password values through it a single time - what is referred to as a "non-iterated" hash. Many firms choose to put passwords and their subsequent hashes through the hashing algorithm multiple times to make them more secure, Spies said.

Second: the company didn't use a "salt" to lengthen the data to be encrypted. Salts are extraneous values that can be added to passwords or other data that needs to be hashed so that the hashed value is not the actual password. Organizations commonly append ready data like the user name or a timestamp as a salt, said Saul of Application Security Inc. Salts aren't foolproof. But, by lengthening the encrypted data, they make it far harder for attackers to crack hashes using rainbow tables, said Shaul.

With straight passwords hashed a single time using SHA-1, LinkedIn's data was highly vulnerable to automated guessing attempts using GPU-powered tools that can guess 500 million passwords a second, said Spies. "Even if you have a large dictionary, you can plow through a lot of passwords very quickly," he said.

The social media companies themselves appear to have already reached that conclusions. LinkedIn revealed after the breach that it had already implemented salting for its passwords, but hadn't extended that protection to all its users. The company, no doubt, was leery of forcing its tens of millions of users to update their passwords at once, said Shaul.

What's the solution? Shaul said that the LinkedIn breach was a wake-up call, but probably not an urgent security problem for members.

"This seems more hacktivist than criminal," he said. "And, because there were passwords but not user names, its not a real threat to anyone, anywhere." Still, he said, companies have lessons to learn. "If osomeone broke in, obviously you have to close the vulnerabilities that led to the breach." Beyond that, he said, data needs to be better protected within data stores and in transit.

Spies said that companies can already choose from a set of more sophisticated functions to protect data such as passwords. Companies like Becrypt make purpose-built one way functions that require significant CPU and memory to compute. That can dramatically raise the cost of cracking them for attackers. Spies said that Voltage researchers developed randomized key derivation functions that iterate hashes in ways that are impossible to determine in advance, complicating the job of cracking hashes.

Finally, companies can also bar users from choosing insecure passwords, or create strong incentives and tools for them to adopt longer pass phrases in lieu of crackable passwords. Slate writer Farhad Manjoo wrote this week about the wisdom of passphrases coupled with easy mnemonics and can lead to long and quite secure passwords. Alas, as many security experts have noted: many firms that manage passwords for their customers online go the opposite route: encourage - even requiring- weak and easy to guess passwords. Those are practices that need to change. Hopefully the attention to the breaches of LinkedIn, Last.fm and eHarmony will prompt that change to occur.

## Leaky Apps Spill User Data

*And, despite the considerable promise of cloud computing, it also comes with risks. The consolidation of computing resources and data in large, multi-tenanted cloud servers presents malicious hackers with a rich target for compromise. And, despite the vast changes in how they are deployed and accessed, most cloud-based servers still run common operating systems such as Windows Server and Linux, common applications such as Web servers and SQL databases, and common defenses developed for non-cloud deployments.*

*The escapades of hacktivist groups like Anonymous, LulzSec and TeamP0ison exposed the sad truth that even high profile and sophisticated technology firms like Sony are vulnerable to attacks against high value, Internet accessible assets. That company experienced a series of breaches on its PlayStation Network in April of 2011 that forced the company to take its entire online gaming environment offline, after the attackers made off with user account data. As guest contributor Alex Rothacker wrote at the time, Sony was using older, unpatched versions of common applications such as the Apache Web server on PlayStation Network and hadn't deployed firewalls and malicious activity monitoring tools to protect PSN –steps that are considered by most experts to be a basic safeguard.*

*Even with adequate security protections, hackers are often able to use vulnerabilities in front-end Web applications to gain access to data stored on back end servers that store customer accounts and feed that information to users. A study by application testing firm Veracode found that SQL injection and cross site scripting vulnerabilities caused 84 percent of the 9,000 applications the company tested to earn a failing grade.*

*Finally, cloud providers – like organizations in general – can fall due to self-inflicted wounds and faulty processes. In April, 2011, Amazon.com's EC2 experienced as sustained service outage after a faulty update to one of its cloud data centers on the East Coast of the U.S. misdirected traffic to a backup network that was incapable of supporting the load. And, in June, 2012, hackers targeting the tech firm CloudFlare, which provides hosted security services for Web-based businesses, were able to exploit a flaw in Google's Enterprise Apps cloud-based productivity suite to bypass a two-factor authentication feature that protected CloudFlare employees, giving them access to CloudFlare's e-mail servers.*

## Cloudflare CEO: AT&T Voicemail Hack Key To Compromise

**By Paul Roberts**

Loose security protecting voice mailboxes at mobile carrier AT&T provided a key element necessary to successfully hack the Google Enterprise Apps account of tech firm CloudFlare, according to an account of the hack posted by CEO Matthew Prince.

Writing on the company's blog on Monday, Prince said that attackers exploited a business process flaw in AT&T's voicemail system that allowed them to forward his cell phone to a fraudulent voicemail box they controlled. They then used a pre-recorded voicemail greeting to trick Google's system into leaving a PIN code necessary to reset Gmail password as a voicemail message - a second critical flaw in that allowed attackers to bypass Google's two factor authentication system.

Prince said that other security mistakes enabled the attack against CloudFlare, which relies on Google Apps to host both email and apps for CloudFlare.com. They include a flaw in Google's Enterprise Apps account recovery process that allowed hackers to bypass the two-factor authentication that protected CloudFlare employees accounts on Google Apps.

But CloudFlare itself was to blame. The company regularly copied administrative e-mail accounts on "transactional e-mails" such as password change notifications. That allowed the hackers who got access to Prince's e-mail account to move even deeper into CloudFlare's network.

The entire attack, which transpired on June 1, lasted less than two hours, with hackers in control of Prince's Gmail account for about 1 hour and 35 minutes, and in control of CloudFlare's email accounts for 28 minutes. Some of that time was spent battling for control with the CEO and other CloudFlare administrators.

CloudFlare is based in San Francisco and provides hosted security and content acceleration services for Web-based businesses. Prince said that his company has changed its internal procedures to stop copying administrators on transactional e-mail and that the company is working with AT&T to address the vulnerability that allowed his voicemail to be rerouted. Google, Prince said, has fixed the vulnerability that allowed attackers to bypass two factor authentication with its Enterprise Apps service.

## Conclusion

*The transition from traditional client-server computing models to cloud-based computing will accelerate in the years ahead. While cloud-based deployments offer considerable advantages in areas like cost, flexibility and management, security remains a sore point. A revolution in the way computing power is delivered and consumed, cloud-based infrastructure still suffers from many of the same flaws as non-cloud based IT infrastructure: poorly or insecurely coded applications, inadequate perimeter protections, poorly configured deployments and poor visibility of malicious activity.*

**About Threatpost**

Threatpost, The Kaspersky Lab security news service, is an independent news site which is a leading source of information about IT and business security for hundreds of thousands of professionals worldwide.

Threatpost's award-winning editorial team produces unique and high-impact content including security news, videos, feature reports and more.  They break important original stories, offer expert commentary on high-priority news aggregated from other sources, and engage with readers to discuss how and why these events matter.

Threatpost has been referenced as an authoritative source on information security by leading news outlets including The New York Times, The Wall Street Journal, MSNBC, USA Today and National Public Radio.

Threatpost's global editorial activities are driven by industry-leading security journalists Dennis Fisher, editor-in-chief and Paul Roberts, editor. They are assisted by Christopher Brook and Brian Donohue.

Make Threatpost your first stop for security news and analysis to stay informed and keep your organization safe.