April 2012

VECTOR

Perspectives on what's happening in the world of Information Security

Hiren Shah
President, Net-Square
reach him at hiren@net-square.com

Secure • Automate • Innovate

Net-Square Solutions

is a niche Application and Network Security Service provider. Net-Square provides Consulting Services like Vulnerability Assessment, Penetration Testing, Code Review, Reverse Engineering and Security Architecture Consulting

Net-Square also offers Products like Server Defender Vulnerability Protection (SDVP), a web application Firewall for IIS applications and NS Webscan, an automated application vulnerability scanner

Last but not the least is the training programs. Net-Square offers a variety of customizable training programs for the benefit of end users and developers.

~~Breaking~~ Hacking News:

Indian military research bodies and Tibetan activists have been targeted by hackers based in China, with a former graduate student at a Chinese university emerging as a key figure responsible for the cyber breach, according to a report by a computer security firm.

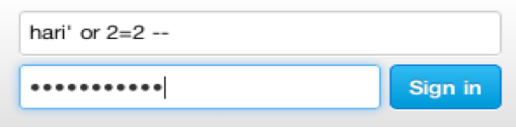
The hacking campaign, dubbed 'Luckycat' has been active since around June 2011 and has been linked to 90 attacks against targets in Japan and India as well as Tibetan activists.

The "Makers" and the "Breakers"

As I embarked on my journey to grow Net-Square with Saumil (for the rare few who don't know him – he is the CEO of Net-Square), I was given a very good induction in what we did as a business. The first question that came to my mind was "Why are we finding so many vulnerabilities in our clients' applications?" Saumil and I set out to find the answer through a tried and tested method - do a "Root Cause" analysis. We took a *3-Idiots (a famous Bollywood film)* approach and performed a "demo" to arrive at the root cause.

We asked a classroom of experienced developers to write a simple program. A login form for a web based application. Something that exists on almost every application on the planet. We drew a form in front of the developers with two input boxes, one for the login ID, another for the password, and a button labeled "Sign-in". We then asked the developers to write code for this simple login form.

The exercise was an eye-opener! The developers very accurately provided the design and the code for the functionality of the form, but missed some very obvious checks to protect against even a novice hacker. And Saumil demonstrated just that. In the very first attempt, he showed how the programmers had not covered themselves against a SQL Injection attack.



The answer was very clear. Developers are so focused on "building" that they have no time (and may I add inclination) to worry about securing the application against an attacker. And I don't blame them for it. Having watched the team at Net-Square, I have realized that building applications and breaking them are two entirely different skills.

The way out is not in forcing the developers to write secure code. But to ensure that each line of code written by them is tested thoroughly by a set of people who are experts at breaking applications. By no means do I suggest we do not train the development community to code securely – we just cannot depend on that unless certain maturity is reached. Training definitely helps in reducing the number of security holes that get left behind and therefore reduces the time and cost of remediation.

By the way, what I have said above is not new. We are already following a similar approach in our organizations - in the Finance division. Don't we have Auditors who come in and validate whether our Accountants have recorded all our financial transactions properly? Why can't such an approach be standardized for our code!

Our little "demo" made it clear to that we need both the makers and the breakers to work together for the applications to be robust and withstand the attacks posed by the complex world of IT today. To that end we encourage our clients to make security architecture a part of the development process. Lastly, to all my friends in Information Technology and Information Security, next time you see code going into production, ask yourself, has someone tried to break this?

Until next time, stay safe!

Best,

Hiren

Follow Hiren's views on IT and other matters on his blog http:// I -thought.blogspot.in or on twitter @hiren_sh

Google's Pwnium contest paid US$ 60,000 per Chrome Exploit

Saumil Shah
CEO, Net-Square
saumil@net-square.com

Google launched its new cash-for-vulnerabilities programmed called "Pwnium" at the CanSecWest 2012 information security conference held in Vancouver last month. Researchers were invited to submit working exploits against Chrome. Every successful Chrome hack would fetch a prize of $60,000!

Google set aside a total of $1mn in prizes. Pwnium saw two successful hacks against Chrome, and Google happily paid out $120,000. Google also demonstrated a patch deployment turn around of less than 24 hours since the exploit was reported. This is not a small feat.

Google's message was loud and clear. "We mean business when it comes to security". A successful exploit against Chrome would easily take 2-4 man months of effort. And $60,000 is enough money to keep researchers from selling their exploits to the underground market. Google's pro-active approach towards security stems from their mature internal security program. Other than Microsoft, few other organizations seem to recognize this. The writing is on the wall for the likes of Apple, Oracle, Mozilla and Adobe – "It is time they stepped up their infosec program as well". What is the takeaway for other large Organizations? By engaging with Infosec firms so that they can also have a private program like that of Google.

Saumil is a regular presenter at the CanSecWest security conference and also at the Hack-in-the-Box and BlackHat conferences. Catch him next in Singapore between April 24-25 conducting Advanced Exploit Laboratory workshop at the Syscan - http://syscan.org/syscan12-training/sys_12_05.php.

Picture below: Google Chrome's security researchers at the Pwnium contest table at the CanSecWest security conference in Vancouver.

The Mac comes of age

Trojans and Malware finally make their way to the Macintosh.

Apple's Mac OS X used to enjoy the reputation of being "virus free" – simply because there weren't any viruses written for it en masse.

As Macs penetrate the market, they prove to be a worthwhile target for hackers. Says Saumil Shah "Unless a platform gains critical mass in market share, it is not a fruitful target for attackers. That critical mass is 15% of the market share."

The Flashback Trojan saw a botnet of more than 600,000 Macs worldwide. The malware itself was installed using a "drive-by" attack, exploiting a vulnerability in the Java browser plugin.

Although the Macs are being cleaned up as we speak, it should be noted that Apple's Java patch came in way too late.

"We shall continue to see exploits targeting Mac OS X", says Saumil, who incidentally has been a Mac user since over a decade. "These are interesting times."