March 2013

Vector

A Net-Square Initiative

A series of articles specially designed for the information security professionals.

Saumil Shah
CEO, Net-Square
reach him at saumil@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, Net-Square offers a variety of customizable training programs for the benefit of end users and developers.

~~Breaking~~ Hacking News:
Big cyber attack slows down internet!
According to a 29 March 2013 report in the Times of India, a "bazooka" cyber attack had slowed traffic on the internet in the week of march 25th. Attackers have targeted Spamhaus, a Geneva based group that publishes spam blacklists which are used by email admins to block spam. The attackers launched a massive distributed denial of service (DDOS) attack in which they threw a wave of digital traffic to DNS servers to bring down Spamhaus. Read more:http://articles.timesofindia.indiatimes.com/2013-03-29/security/38125150_1_spamhaus-anti-spam-servers

News from Infosec Conferences worldwide

It has been a very interesting month indeed. My 2013 infosec conference circuit began with Cansecwest '13 held in Vancouver. I had to sacrifice going to Nullcon in Goa because the dates clashed with our 4-day Advanced Exploit Laboratory class at Cansecwest.

An interesting set of events transpired at Nullcon 2013. For the first time, the Indian Government's National Technical Research Organization (NTRO) paid a prize of INR 35,000 to security researcher Rahul Sasi for tracing and defeating a command and control server run by external attackers. Last year, I made a remark in one of my lectures delivered at the Indian National Police Academy that law enforcement and defence agencies need to actively collaborate with security researchers. I am glad to see this trend finally kicking off in India. News link: http://heraldingoa.blogspot.in/2013/03/hacking-govt-server-fetches-him-rs-35k.html

Moving to Cansecwest, the biggest news item is usually the annual Pwn2Own contest. Hackers are invited to demonstrate their exploits against the latest operating systems and application software. Laptops are set up with the most up-to-date patched systems. A successful compromise lets them keep the laptops and also earns them cash prizes. This year, a staggering USD 4,80,000 was paid out in cash prizes! French security firm VUPEN made off with USD 2,50,000, demonstrating exploits on IE10 on a Microsoft Surface Pro tablet running a 64-bit version of Windows 8 with full sandbox bypass, a use-after-free exploit on Mozilla Firefox, another exploit on Adobe Flash and lastly, a yet-another-Java-exploit! MWRLabs researchers Nils and Jon earned USD 1,00,000 after successfully exploiting Google Chrome with full sandbox bypass using a Windows kernel flaw. George Hotz exploited Adobe Acrobat Reader and escaped the sandbox to win USD 70,000. James Forshaw, Joshua Drake, and Ben Murphy independently exploited Oracle Java to win USD 20,000 each.

Google Chrome and Mozilla Firefox both fixed the reported flaws in under 24 hours! Google's Chrome security team has always maintained rapid turnaround times. In one of my earlier Vector articles, I stated that today's turnaround times for vulnerabilities should never exceed 72 hours. As a long time Firefox (and Netscape Navigator) user, I was delighted to see Mozilla taking turnaround time seriously! Mozilla Advisory link: http://www.mozilla.org/security/announce/2013/mfsa2013-29.html

Cansecwest is also known for high quality conference talks. After 15 years in the world wide infosec conference circuit, I have become jaded to run-of-the-mill conference talks discussing yet another XSS bug or a new SQL injection vector. Cansecwest has always provided me with a fresh perspective! Two talks caught my attention this year. The first was by an upcoming security researcher SeungJin Lee a.k.a. "@Beist" on hacking Smart TVs. Smart TVs have a camera and microphone built into them so that a viewer can literally issue commands by talking to the TV and select menu options by waving their hands! Unfortunately for the TV makers, Beist demonstrated how to turn a Smart TV into a bedroom spying device, by recording images and audio of the viewer's room with the Smart TV's built-in camera and having them streamed live over the Internet! This is what happens when the "Idiot Box" tries to act "smart". Beist's slides: http://cansecwest.com/slides/2013/SmartTV%20Security.pdf

Another interesting talk was by a Chinese researcher Yang Yu a.k.a. "@tombkeeper". He blew the lid off a privately known technique to bypass ASLR and DEP without using complicated information leaks and ROP chains which are the de-facto techniques required for exploiting software today. Tombkeeper's talk:
http://cansecwest.com/slides/2013/DEP-ASLR+bypass+without+ROP-JIT.pdf

On the defense front, Microsoft weighed in one of their most voluminous "Patch Tuesdays" with seven bulletins released on March 13, 2013. Bulletin MS13-021 addresses a record 9 use-after-free vulnerabilities with all versions of Internet Explorer, where an attacker can achieve remote code execution by compromising users browsing with IE.

- contd on page 2

Responsible Reporting

A big challenge facing most of the companies, be it software products and services, or anything else, is to control the vulnerabilities in their products and contain them from being publicly announced by attackers in the open. And to do this, it becomes imperative to put in place an attractive responsible disclosure program! This program allows coordination between the company and security researchers for disclosure of vulnerability, supporting its fixing, patching the vulnerability within said period of time, and then publicly reporting it with the remediation.

But in this, is there any reward for the security researcher? While this seems to be a never ending debate, the most likely answer is on the mindset of the researcher. What does he want? Some researchers want recognition and name, the others are likely to go for compensation. And not all such vulnerability disclosure programs offer compensation. This leads to many researchers being unsatisfied with all the efforts that they have put in. Another bottleneck in the disclosure programs is the process itself where a lot of time is taken to accept the vulnerabilities disclosure, process the researchers request and give due recognition to the researcher. Sometimes, this can go as long as couple of months! This certainly does not go down well with the security community who are then tempted to explore alternative avenues like the commercial vulnerabilities market for receiving instant remuneration and recognition.

Companies like Microsoft and Google have already sensed importance of responsible reporting long time ago and have set up several initiatives to compensate security researchers. Microsoft has set up a "Microsoft Security Response Centre" which investigates all reported vulnerabilities in Microsoft products. They develop updates as quickly as possible with the help of researcher who has reported the vulnerability. They then publicly disseminate information about the vulnerability, its risk and how customers can protect themselves. Microsoft singles out such security researchers for a special appreciation and mentions their names in acknowledgement section of their security bulletins and advisories. They call this Coordinated Vulnerability Disclosure (CVD).

One of the companies, which financially support responsible disclosure by paying bug bounties, is Google. Starting from November 2010, Google's Vulnerability Reward Program invites cutting edge external research that would keep the users safe. The reward amounts range from $500 to $20,000 for various qualifying bugs. Such programs give researchers both, recognition and financial benefits. Google also has initiated contests like "Pwnium" and "Pwn2Own", where they reward contestants for finding vulnerabilities in their Chrome OS. According to a March 18 blog on their website: http://blog.chromium.org, at the recent CanSecWest conference where they host their Pwnium and Pwn2Own contests, they rewarded $40,000 to one such researcher for finding and submitting bugs in their Chrome platform. Other companies offering such incentives include Facebook, Mozilla and Barracuda Networks.

We at Net-Square believe in responsible reporting. Whether we are paid or not or whether we are acknowledged or not, we will never put out a vulnerability found by Net-Square out in the open. It stems from the Company's ethos to "work towards making Individuals and Organizations safer on the Web". If we find any vulnerabilities in any website or product of any organization, we directly report them to the owner and help them in remediation so that the customers and/or users are not affected in any way. Recently one of our security researchers, Jigar Soni, discovered critical time based SQL injection vulnerability in AT&T's Video Conferencing portal. He followed the standard responsible reporting procedure and intimated AT&T security team of this flaw along with a presentation on the step-by-step process of finding vulnerability with screenshots. Acknowledging Jigar's discovery, AT&T has mentioned his name in their Bug Bounty Program "Hall of Fame" recognizing his efforts to strengthen their application security. - *Link to the acknowledgement!* This is not the 1st time, neither is it the last time that this will happen at Net-Square. Though we believe companies should encourage and recognize such serious efforts, as this will increase responsible reporting.

- Hardik Kothari, Business Development, Net-Square

....Continued from Page 1

I have said it before and I will say it again, that browser vulnerabilities, especially use-after-free bugs, are going to be the weak spots in today's computing landscape. The other 6 Microsoft security bulletins fix remote code execution and privilege escalation bugs in MS Office, Office: Mac, Sharepoint and Windows Kernel Drivers. Microsoft's March 2013 bulletins:http://technet.microsoft.com/en-us/security/bulletin/ms13-mar

My last stop for March in the infosec conference circuit was Blackhat Europe 2013, where I taught the intermediate level Exploit Laboratory class. This marked my 11th year with Blackhat Europe! After teaching a class, I am rarely in a position to get up early to catch the opening keynote address. However, I am glad I got to attend Rick Falkvinge's keynote address titled "Shelters or Windmills - The Struggle For Power And Information Advantage".

Mr. Falkvinge is a member of the Pirate Party and an elected member of the European Parliament. It was an honest, thought provoking and inspiring talk. Those who have the information advantage have power. Those who have power hate losing it. Since centuries, innovations and innovators have brought forth technologies that have seriously disrupted strongholds of information advantage. And the powers-that-be have reacted sharply. "Most incumbents don't ignore new technology. They attack it and try to have it banned, killed, neutered." We are in the middle of an ongoing information revolution. The gist of the talk was based on a Chinese proverb: "When the wind of change blows, some build shelters and others build windmills."

That's all from me for this month. Next month takes me to HackCon 8 in Oslo and to SyScan 2013 in Singapore. We shall be teaching our advanced classes in exploit development at both conferences. SyScan is celebrating its 10th anniversary, bringing top notch security researchers from all over the world. I have known some of them for more than 10 years now, and I look forward to the reunion!

- Saumil Shah, CEO, Net-Square