October 2012

V e c t o r

A Net-Square Initiative

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

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:*

3.6 million social security numbers, 3,87, 000 card numbers stolen in USA!

A recent report by Infosecurity-magazine.com reveals that millions of social security numbers (SSN) and lacs of credit/debit card numbers of taxpayers in South Carolina have been stolen. None of the SSN's were encrypted. Investigations tell that intrusions have occurred some 5 times from August till October. This has left a lot of anger amongst citizens with the government failing to provide acceptable answers.
To read more visit link:
http://www.infosecurity-magazine.com

Blacklisting or Whitelisting?

Traditionally, IT Security is thought off from a threats perspective. It always brings to fore thoughts of protecting the Applications, Systems and Infrastructure from Virus, malwares and other threats posed to the IT Assets. And therefore one is always focused on identifying new threats and making sure they get integrated into the "Blacklist – allow all except" that is maintained to protect the IT Assets. This is the same principle on which many Anti-viruses, Anti-malware and other Security product providers work. You update the signature; the "Blacklist" is updated so you will be protected from a certain threat, which by the way is out there in the open known to everyone. While we have our thoughts on whether this approach is truly effective or not in protecting against viruses and malwares, our views on Application Security is very clear. "Blacklist" approach doesn't work. Definitely not today when the attacks have become very sophisticated.

For one, we are fast reaching a saturation point in the Blacklist approach being effective since the volume of Blacklists to be maintained is just so huge. As one Senior IT Manager in one of our Client Organization once put to us…"How much will I filter? There is no end to it". This is not the first time we have come across this frustration. We recognize this challenge for the drivers of IT in an Organization. As their core function is to improve productivity and drive innovation.

And second, because the Attack Vectors have become complex and the attackers more innovative and skillful in evading detection, the "Blacklist" approach will not work. I was personally seized of this challenge when we were working on putting together an Anti-Spam solution in my earlier stint. The sheer number of SPAM messages meant that some of them would definitely filter through. Unfortunately, the same scenario is now playing out in the Application Vulnerability space, but with potentially disastrous implications.

So then what is the answer. Well, take the "Whitelist" approach. In the "Whitelist" approach you structure the application to only accept the legitimate functionality and stop everything else. Some simplistically put it as diagonally opposite of "Blacklist" i.e. the "deny all except" philosophy. In the past this approach has faced a roadblock because nobody wanted to take a chance of blocking a legitimate transaction. Recognizing this challenge we are now helping our customers design applications by integrating the "Whitelist" approach. What we do here is sit with the Architecture or development team and review the business case for each user input and then work out different solutions of applying a "Whitelist" on these inputs. We believe that this approach works best as now you are only allowing a legitimate functionality to get executed. In what form does this whitelist approach take? It takes many different forms like filtering input characters against an array of allowable characters or doing a comparison of input values against legitimate values from the database. Using the "Blacklist" approach is like chasing your tail. How long can you do it! Until next time, stay safe!

- Hiren

Follow Hiren's views on Twitter @hiren_sh *or on his blog:* The Thought That Counts

Linked IN and HR – Does it make the attacker the LION!

LinkedIn.com has been one of the few really big success stories of Social Media. And one of the very few that has found immediate application in the Corporate context. Especially the HR departments have taken to LinkedIn.com like fish to water. In their quest to hunt down the best talent for the Organizations, HR Associates, Managers and Leaders have built connections with thousands of people. Many of them have opted to become LIONs - Linked In Open Networker. If someone has put a tag of LION on their Linked In profile that means they are open to connections with people they have never met before. Why am I talking about it?

As you know, modern day hackers and attackers are using hybrid attack techniques. They use different methods to get their malwares and keyloggers on to the victim's machines. And the Social Media site like LinkedIN.com is a very good platform to do that. What we have found so far is that the most vulnerable group within a Corporate is the HR Department. In their eagerness to connect with as many people as they can, they tend to accept connections from just about anyone. After that the next steps are easy for any attacker. Collect the information about the environment in which these users operate like browser footprint etc. and after identifying a vulnerable piece within it, launch the exploit.

In order to help Organizations understand the threat posed by Social Media we offer a Social Media evaluation exercise for our colleagues in the Infosec departments of Corporates. In all our exercises we have found that the easiest to hit are Managers and Executives from the HR team. Even when our fictitious profile is also an HR Profile! Recently in one of our exercise, we were able to connect with the multiple HR Executives and Managers in a matter of minutes after we sent out a connections request.

How can Corporates protect their Infrastructure from an attacker powering his / her way through the LION configuration of one of their employees? First and foremost, disallow any access to a Social Media sites from any m/c connected on the network. As a best practice, let users who need to use Social networking sites do so only on specified m/cs not connected to the network, like standalone PCs. Users have to be explained one-on-one on the dangers of accepting or accessing any file sent through any Social Media sites. It is also important to test what vulnerabilities exist on the desktops, which can be exploited by the attackers. We believe the best way to do that is to conduct a Social Threat evaluation exercise. It will provide you the necessary insight on what needs to be done to protect your IT Infrastructure from Social Media Threat.

- Net-Square Team

DDOS strikes U.S. Banks

The last 5 weeks have seen a wave of DDOS attacks on several US Banks. A report by the magazine, Bank Info Security, informs that there have been a series of planned Distributed Denial of Service attacks on several bank websites. The report claims that on Oct 17, BB&T Corp, a North Carolina based bank, acknowledged its website was suffering from intermittent outages related to a DDOS attack. BB&T is the ninth bank to be affected by such a DDOS strike in the last 5 weeks. Similar attacks were faced by Capital One, a big Bank head quartered out of Virginia, US. On Oct 16, Capital One's online banking and corporate sites suffered outages. This was a second attack on CapOne, after the first one on Oct 9.

And who's causing all this trouble? A post on Pastebin from the hacktivist group Izz ad-Din al-Qassam, Cyber Fighters claimed responsibility for the attacks with the new attacks to be waged between Oct 16- 18. The group has targeted a series of attacks against CapOne, SunTrust Bank, Regions Financial Corp, Bank of America, JP Morgan Chase, Wells Fargo, US Bank and PNB. They say they have been particularly offended by a YouTube movie trailer which they find to be anti-Islam and want it to be removed. The attacks will continue till the time the trailer goes off the Internet.

Security experts however assert that these attacks are not just fame claimers, but there's more to it. The perpetrators are looking for targets that have footprints on employee's desktops so that they can compromise those employee's and get access to accounts with money. Experts also caution that unlike traditional DDOS where hackers take over multiple computers, this time, the attackers seem to be operating from a fleet of virtual servers which helped them to automate and speed their attacks getting more information.

We feel as a first line of defense Banks should inform customers about the attacks, what's new, what is the banks strategy, and how the attacks will be resolved. Educating customers more on such security issues will ease concerns. Sometimes, being just honest helps!

-Net-Square Team