Newsletter – Issue No.0005/IT– July 2013

IT Security Newsletter

Hackers stole $45 million within few hours

There were no guns, not even threatening notes or black masks. A group of eight men netted $45 million by breaking into payment systems and eliminating withdrawal limits placed on prepaid debit cards.

By removing that limit, criminals had access to unlimited amount of money. The attackers removed the limits by breaking into two online payments processing companies for prepaid MasterCard debit card accounts issued by two banks — the National Bank of Ras Al-Khaimah PSC in the United Arab Emirates and the Bank of Muscat in Oman.

22 million IDs stolen from Yahoo! Japan

Yahoo! Japan suspects' security of almost 22 million user IDs may have been breached during an unauthorized attempt to access the administrative system of its portal.

It proves again that even big corporates are not having enough security mechanisms in place. In 2011, usernames, passwords and birth dates of more than 100 million people were compromised after attackers struck the PlayStation Network and Sony Online Entertainment services. Japan Aerospace Exploration Agency has also witnessed a similar attack last month where information related to the International Space Station leaked during an unauthorized attempt to access its system.

Cybercriminals using hijacked Cloud hosting accounts for targeted attacks.

A recent survey shows that cloud hosting service providers are constantly being targeted by criminals to organize financially motivated attacks. High availability of infrastructure in US makes it the attacker's favorite destination while other countries are also being targeted for politically motivated attacks.

The majority of these resources are used by attackers for executing various criminal activities ranging from distributed denial of service attacks and botnet management to watering hole attacks and phishing campaigns.

UK banks hit by malware and social engineering attacks

A variant of Ramnit malware, discovered back in 2010, has been returned and is targeting financial sector of UK.

The new variant has incorporated code from Zeus Trojan, thus making a powerful comeback.

To add spices to the already worst situation, social engineering were used to manipulate users. It is not detected by client side security mechanisms like anti-virus and firewall as they goes into an idle sleep mode straight away upon installation and continues sleeping till its victim logs into online bank account.

FBI and Microsoft seized Citadel banking Trojan servers

FBI and Microsoft have collaboratively taken down large botnet that had control over millions of computers. It is believed to have stolen more than $500 million for past one and half years.

Even though the cleaning process is active, Microsoft admitted that the botnet is not completely down and part of the network is still operating.

‘Security tip of the month’

Ensure your systems are protected with anti-virus software and it's regularly updated as new virus attacks are emerging daily. Anti-virus console monitoring is a preferred approach to detect and avoid virus attacks. It's always better to be safe than sorry.

Is Facebook more secure than online banking?

The past month has seen an enormous growth in cyber-attacks against financial institutions. This once again proves the lack of security in banks and other key important businesses. From a normal user's side, their social networking websites are far more secure than their online banking systems.

These breaches are not happening due to lack of security mechanisms and controls. There are already a bunch of security mechanism in banking systems that bother the users very much. Many of the financial institutions already started reconsidering their security procedures in the wake of these incidents. While the institutions are busy to implement more mechanism that is going to annoy the normal users, it's a fact that it is easier for someone to break into a bank account rather than breaking into Facebook or Twitter account.

We all are well aware that none of the systems can be completely secure. One of the main weak point of any information system is the end users. As long as people are careless about security measures to be taken, criminals will find a way to break into the system. "A chain is no stronger than its weakest link". Recent innovations and security measures in online security have focused on solutions that protect users from themselves. The vast majority of financial institutions have yet to follow this suit.

Banks should always assume that intruders are going to get access to the systems. It can also perform behavioral analysis to detect fraud. If a particular bank account is used in a way that it is not usually supposed to do, it can be brought under the scan.

Even if these are not going to stop criminals, it will offer a new line of defense. The mission should be to employ as many security measures as possible to make the fraudster’s task tougher.

It's a universal truth that none of the businesses wants to hinder the convenience of their users by introducing another barrier to entry. The result is, additional security measures like two factor verification are kept as optional.

Those who are concerned about security of their accounts will of course opt-in to such features. But the careless users who reuse and share passwords are not likely to opt-in for such features. At the end of the day, the people who do not need additional security measures will be the only ones who are using it.

For further information please contact:

Ranjith Kumar, Director, ranjith.kumar@keypoint.me
Nandakumar Narasimhan, Director, nandakumar.narasimhan@keypoint.me
Chahira Ashcroft, Senior Manager, chahira.ashcroft@keypoint.me