SECURING PARAMETERS

As our society mobilises and more individuals use smart devices to access corporate data, cyber criminals are developing more sophisticated malware that operates at faster speeds. CNME reports on how attack methods are changing and how security strategies need to evolve to keep up.

"Security technology failures go through a predictable sequence: initial discovery by security professionals, followed by wide scale abuse by teenage vandals and, finally, appropriation by criminal enterprises. Now that the teenage vandals have largely dropped away, we are left with professionally executed attacks motivated solely by money. In less than five years, e-crime has changed from an anomaly into an industry," says Michael Barett, CISO at PayPal in his efforts to characterise the new cybercriminals.

To say that Barett is correct in his description of the latest cybercriminals would be an understatement. Cybercrime has changed from being a battle at the user's desktop, where antivirus and security software are effective in repelling attacks to being a battle encompassing the entire organisation, its network and brand identity.

Costin G. Raiu, director, global research and analysis team, Kaspersky Lab says, "The amount of malware has constantly increased for the past 15-20 years, mainly due to the boom that cybercrime has known since early 2000. Cybercrime itself is gaining popularity, because it is profitable, low risk and easy to do. Despite the best efforts of security companies and operating system developers, e-crime is still growing and poses a huge problem for individual users, corporations and governments around the world."

According to Justin Doo, security practice director for emerging regions at Symantec, "The lack of an international framework that protects users and prosecutes cyber criminals, coupled with the fact that most malware attacks originate from outside the victim's territory, means that these perpetrators have no fear of being caught.

"The lack of a common law related to cyber activity and the consumerisation of attack toolkits has significantly reduced the complexities associated with generating malicious code or content. Cyber criminals are selling crime packs for this very task, essentially developing their own black market. These guys are well aware of the difficulty in invading multiple samples and therefore generating new attack modules at faster speeds is also part of their strategy," explains James Lyne, director of technology strategy at Sophos.

Doo believes that attackers have also realised that it is much easier to target global brands because of the sheer number of stakeholders connected to the brand's identity, network and domain.

"It is virtually impossible for consumers to tell whether or not they've found the original brand or its authorised partners online. The Internet continues to harbour traffickers in counterfeit goods, fraudsters aiming to divert traffic away from legitimate sites and attackers aiming at identity theft," adds Mirza Asrar Baig, CEO, IT Matrix.

"Organisations aren't taking security policies seriously and often permit business units to drive technology without placing the appropriate security measures to protect the network and data in place. This makes the idea of targeting organisations, a lot more appealing," agrees Nick Black, technical manager, Trend Micro.

The growth of the digital universe and the mobility this entails also contributes to the increasing volumes of malware activity. According to the IDC Digital Universe Study 2010, the digital universe grew to 800 billion gigabytes, a 62% increase since 2008 and will expand to 35 trillion gigabytes by the year 2020.

Lyne points out that last year Sophos witnessed around 95,000 unique malware samples a day and today they're witnessing close to 150,000 unique samples a day. Security professionals believe that this trend is likely to continue as more identities become available online. "Attackers now know that a planned and targeted attack will almost always be successful. As long as there is data to be stolen and profit to be made, we're going to see rising numbers," he adds.

Justin Doo, Security Practice Director for Emerging Regions, Symantec

"Organisations aren't taking security policies seriously and often permit business units to drive technology without placing the appropriate security measures to protect the network and data. This makes the idea of targeting organisations, as opposed to individuals, a lot more appealing"

Intruder alert

Over the last few years phishing scams, where the attackers send out enormous amounts of spam including links to fraudulent Website controlled by the attackers, have garnered much attention in the cyber world. Phishers rely on the fact that because spam filters analyse billions of email there is a probability that at least some would get through.

According to Baig, phishing is not purely a technology problem but a combination of social engineering and technology prowess, the phishing email must entice the victim to act on it and at times voluntarily provide sensitive information for the attacks to succeed. "Phishers may even use the IP address of the server to confuse victims and may go as far as to register fake domain names, which are typically a variation of the legitimate institution's domain name. They can then create a sub-domain that includes this variation of the legitimate domain name."

Phishers have also been known to register bogus domain names using credentials stolen from their victims with IP addresses linked to multiple compromised PCs that are part of a botnet, which act as proxy connections to a botnet. These act as proxy connections to a handful of services that host pages of up to 20 fake Websites at a time.

Doo also points to the advent of "whaling" where malware is embedded within a single communication module, typically email, targeting senior executives of a particular organisation. The idea is for these emails to be forwarded across other executives in the organisation who act on it based on its source. "These attacks are normally architected keeping in mind even the most minute details, such as language and grammar, and makes them difficult to detect because they come from a trusted source from within the organisation."

Costin G. Raiu, Director, Global Research and Analysis Team, Kaspersky Lab

BY THE NUMBERS

Source: Trend Micro, Global Cloud Security Survey, June 2011

1200 IT decision makers from U.S., UK, Germany, India, Canada and Japan surveyed

93% of respondents are using various cloud computing services

50% of respondents had concerns over security of data or cloud infrastructure

43% of respondents reported a security lapse with their cloud provider

"While generic email blasts remain popular, they're also being supplanted by targeted, brand based solicitations. The malware is embedded in a carefully crafted unique email that targets users by leveraging on the trust they place in well known brands, particularly banking institutions," adds Baig.

Termed brand hijacking, these attacks not only lead to direct financial losses but can also cost an organisation loss of intellectual property and eventually may affect the brand's reputation and customer loyalty.

Security firm, MarkMonitor reports that phishing and malware attacks severely undermine consumer confidence and, due to the fear of becoming the victims of identity theft, of becoming the victims of identity theft over 150 million U.S customers don't bank online. The company also reports that more than 400 brands are attacked each quarter and expects the trend to accelerate as identity theft continues to be lucrative, employing a wide range of tactics including distribution (VOIP, drive-by downloads), infrastructure tools (botnets, fast-flux DNX) and credential theft schemes such as man-in-the-middle attacks.

Experts have also witnessed an increase in what IT security professionals call 'hacktivism,' a term popularly used to describe security breaches and hacks carried out to correct a moral injustice.

"The good news is that as end point security companies evolve and provide organisations with more intelligent data , organisations are more empowered through knowledge to recognise threats," says Alfred Huger, VP of development, cloud technology group at Sourcefire.

James Lyne, Director of Technology Strategy, Sophos

> "The malware problem is not necessarily larger but seems to have gained more visibility over the last few years. The good news is that as end point security companies evolve and provide organisations with more intelligent data they are more empowered through knowledge to recognise imposing threats"

One step ahead

Florian Malecki, senior product marketing manager at SonicWALL feels that as cybercriminals are using increasingly sophisticated attack techniques and exploit kits to perform targeted attacks security solutions developers and providers must also evolve to counter these attacks using a layered security approach.

Addressing the suitability of security applications and solutions that are currently available in the market, Black says, "Some are and some are not suitable. It is important that organisations are serious about security, and partner with and industry-leading security vendor who invests in solutions catered to combat both current and future cyber criminal trends. Businesses must start challenging their security provider. This is because implementation and ongoing support are becoming critical to provide the agility to protect both organisations its against constantly evolving threats."

Waseem F Hattar, IT security manager at eHDF on the other hand believes, "Existing solutions cannot be judged based on the vendor or the type of product because what may be a suitable solution today, may not be as effective tomorrow."

Raiu recommends building user awareness in the organisation. "Begin with a few short days with users defining how best to use the Internet- secure browser, setting passwords and the importance of not disclosing any personal or financial information over the Internet. This can be followed by giving them a list of well known security resources like antivirus packages and firewalls, and setting up a certification program to encourage users to teach others."

Hattar agrees, "Awareness campaigns must be conducted regularly on a monthly or quarterly basis. This makes the organisation's employees aware of the impact of downloading and scanning documents, and sharing critical corporate information with companies or parties not inside the same domain."

Doo believes that although organisations can indulge in regular security campaigns to educate users, these

PROMINENT SECURITY BREACHES IN 2011

RSA- the Security Division of EMC, revealed that they were the target of an Advanced Persistent Threat (APT) and that information extracted from their systems during the attack was related to RSA SecurID two-factor authentication products. This attack targeted the highest profile product of the company and trade secrets were compromised.

Sony- a sophisticated intrusion hit its data centre in San Diego. Data on all 77 million registered accounts was stolen including user names, e-mail addresses, login IDs and passwords. Although no credit card data seems to have been stolen, the attack cost Sony $171 million. Most importantly, due to the extent of the attack, Sony was forced to suspend services for two-and-a-half months.

will not help much unless the information to be shared is presented right. "Most IT users within an organisation are not tech savvy and therefore the most important task is to simplify the information being relayed to them. Personally, I suggest alerting employees about how the malware content may affect not only the business but also their personal lives. At the end of the day, end users pose the biggest threat to security within an organisation."

Professionals also say that the importance of establishing security policies at an organisational level grow in proportion with the size of the organisation, the reason being that larger organisations have more complex networks which makes them harder to secure. As Hattar says, "Security policies will help in defining user behaviour and need not be completely technical. They can be related to basic activities like email or document sharing, which can mitigate risks by controlling data movement."

Lyne adds, "Do the basics well, run up to date endpoint security, use strong passwords, patch your OS and applications. Also, organisations should look to deploy these controls across different platforms such as tablets and other handheld devices with the appropriate configuration." He recommends using a blended and complete set of security controls. "The more layers you can run, the tighter the net around your system and the harder it is for the attackers to slip through the holes," he adds.

Practical picture

One needs to only look at the recent spate of attacks on companies like Sony, RSA and others to see firsthand the serious implications of an attack, both financial and reputation-related (see box outs for detail).

Waseem F. Hattar, IT Security Manager, eHosting DataFort

Many professionals believe that changes and advances in technology are adding to the challenges of businesses and consumers. "The increase in applications and work environments moving into the cloud, the use of Web 2.0 applications, mobile devices, social networking sites, and the simultaneous growth in online transactions, poses a growing risk to enterprises and makes individuals more vulnerable to malware attacks," says Malecki.

There are multiple security solutions currently available in the market. Professionals feel, however, that the best solution would seamlessly integrate a dynamic range of technologies including cloud, heuristics, firewalls and application security.

According to IDC, fewer than 10% of organisations globally make use of behavioural Host Intrusion Prevention System (HIPS) technology. Security technology therefore needs to be adaptable and more cost effective to use, so that these new solutions can be run by organisations within their resource and budget constraints.

Lyne warns organisations against making the security infrastructure too restrictive. "Keep it simple, make sure you are doing the basics on each platform, and look for technologies that can work as effectively across a wider range of platforms, providing minimal increase in costs. Make sure you keep updating users on the threats they will face on these platforms too. It's not all well and good spending all your time protecting the PC, only to have the CEO get socially engineered into sending out sensitive data on his Mac," he states.

Doo believes that industry standards like ISO 27001 and ADSIC are notable initiatives to help organisations realise the importance of securing their infrastructure and information. Hattar says, "Although a scenario that guarantees 100% security does not exist, by investing in the right platforms organisations can prevent the damage that its users and other stakeholders may be subject to in the event of an attack."

Huger believes that aggressive security measures are no longer optional but a mandatory requirement, given the rapidly evolving threats. "It is not a question of whether or not the situation will change, but how soon it will change. Organisations can no longer allow security policies to take a back seat to other technology strategies," he adds.

Lyne concludes, "Compliance regulations demonstrated by ADSIC in the region are starting to develop and many businesses operating internationally are now subject to security compliance requirements in contracts with other overseas organisations. This will encourage the development of a robust security policy framework. As the threat landscape continues to evolve, the role of the chief information security officer will move from a technical one, to one involving the management of business risk and financial impact." ■

PROMINENT SECURITY BREACHES IN 2011

- **Citibank**- a hack devised by simply altering the bank's URL was used to steal 360,000 customers' credit card details including names, account numbers and email addresses. Citigroup suffered about US$2.7 million in losses from 3400 of these accounts.
- **Lockheed Martin**- It was reported that attackers got hold of the algorithm for tokens used by Lockheed Martin, the US government's top information technology services provider. They used these to install a key logger on one or more computers within the organisation. The firm's Maryland data centre was targeted. The backup data centre in Colorado was believed to be secure.