SMEs in the crosshairs

Cybercriminals target smaller businesses with an increasingly sophisticated array of weapons

by **CALYN YAP**

INTERNET threats aimed specifically at SMEs have increased threefold over the last year, says Symantec, and SMEs can no longer afford to believe they are immune.

Several main threats affecting SMEs are detailed in the Internet Security Threat Report 2013, explains Symantec Malaysia senior technical consultant Koh Ee Laine, and these include the fact that SMEs form the path of least resistance for attackers.

More recent is the threat of ransomware which creates new challenges for SMEs, and the Bring-Your-Own-Device (BYOD) trend which opens the door to attacks through mobile malware.

Focus shift

Worryingly, Symantec's 2012 statistics have shown a significant increase in attacks against SMEs, rising from 18% in 2011 to 31% in 2012.

Furthermore, attacks against manufacturing players have moved to the top position in 2012 at 24%, followed by finance, insurance and real-estate targets at 19% and non-traditional services at 17%.

This shows that cybercriminals are changing their targets to focus on SMEs instead of on larger corporations and, Koh says: "In the coming months and years, we anticipate that techniques currently being used to attack large enterprises and government entities for commercial gain will be employed against SMEs.

"The report shows that the threats against today's SMEs are not going away. In fact, they are showing constant growth. Gaining a clear picture of the dangers is an important step in improving security, and this year's report is a wake-up call that SMEs are now being specifically targeted by criminals."

Moreover, smaller companies are targets often as stepping stones to larger corporations and are also used as pawns in more sophisticated attacks. The reason SMEs are targets is they are the easiest to attack; larger counterparts have high levels of security in place, Koh explains.

Avira technical operations product manager Sorin Mustaca concurs: "Small businesses are the most vulnerable because they do not have dedicated or specialised personnel to deal with these complex threats."

He also says SMEs typically do not have the financial power to cover all attack vectors, making them vulnerable to cybercriminals. "This is actually the main difference between small and large businesses, with regard to threats," he says.

This view is echoed by Kaspersky Lab SEA business development manager Bryan Sat, who says cyber threats have increased exponentially and that SMEs must find solutions to them.

Forms of attack

There are many forms of attack; generally, Internet security providers agree there are loopholes or vulnerabilities that can be exploited by a cybercriminal attacking SMEs and end-users, and that attacks have been increasing in complexity and volume in tandem with technology advances.

Sat says updating applications is the first step to a secure IT environment

Koh says it is vital to create awareness on security threats

SMEs are generally easier to attack than larger corporations, says Mustaca

Sat says some of these threats can rear their heads easily as a result of consumer negligence, citing a recent analysis by Kaspersky Lab which shows 132 mil applications were vulnerable to cyber-attacks in 2012.

He adds: "The most alarming finding from this research is that users of the three most vulnerable programmes – which include Java, Flash Player and Adobe Reader – are highly reluctant to update to newer, safer versions."

One of the most common attacks is spear phishing, in which an email – which purports to come from an individual in a position of authority in the recipient's company – is sent to a person of interest.

As an example, the email may ask the employee to log in to a site requiring his or her user name and password, or click on a link to download malicious programmes. If the employee falls for the ploy, the attacker can use his or her identity to gain further access to confidential data.

The emergence of the "watering-hole attack" – an attack categorised under the term zero-day vulnerabilities – was cause for concern in 2012; cybercriminals study the profiles of their victims. They then access legitimate websites that these targets frequent, look for the site's vulnerabilities and inject malicious codes there to lie in wait for these victims.

This method can capture many victims at a time within 24 hours, as it is aimed at specific groups and cybercriminals take their time to understand and profile these groups.

A zero-day attack uses a new vulnerability which targets known customers of affected software, and there is no instant fix for this – which is advantageous for cybercriminals.

"Normally, such an attack happens on a very small scale, because this is the only way that enables the exploit to remain undiscovered for as long as possible," Avira's Mustaca explains.

Emerging threats

There are new threats as seen in focused attacks that also take the form of ransomware, which is malware that freezes computers and utilises messages from authoritative bodies to scare SMEs into making payment. The victimised SME is usually forced to pay sums of US$50 to US$400.

However, computers can remain frozen after payment, and the only way to remove the ransomware is to refresh or reformat the computer, Koh says.

The number of web attacks (or browser-based attacks) a day has also increased, with more cybercriminals moving to social media through mal-ads (legitimate ads injected with malicious codes); user machines are infected by clicking on the ad.

Practical solutions

Security awareness is key in preventing such attacks, internet security providers advise, since some of these attacks can be avoided if employees are aware of such threats.

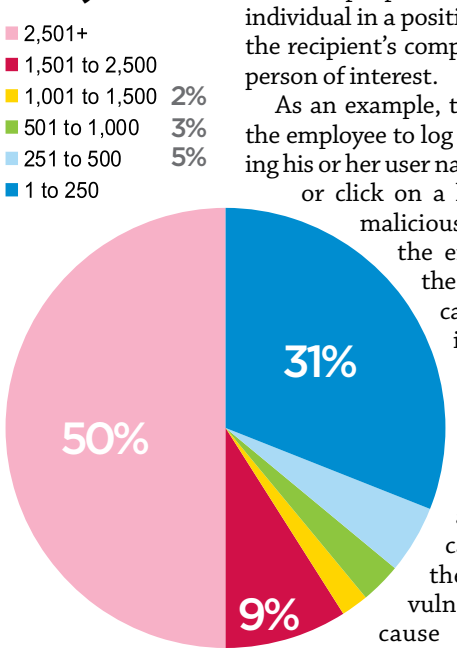
Mustaca says it is important for SMEs to stop thinking that cybercriminals will not focus on them because of their small size. "What they need to do is analyse what their most important assets are and the impact if someone accesses them without authorisation ... and protect these means of access.

"Investing a bit more at the beginning to do the analysis would help in ensuring the right fit and that they do not over-protect themselves," Mustaca says.

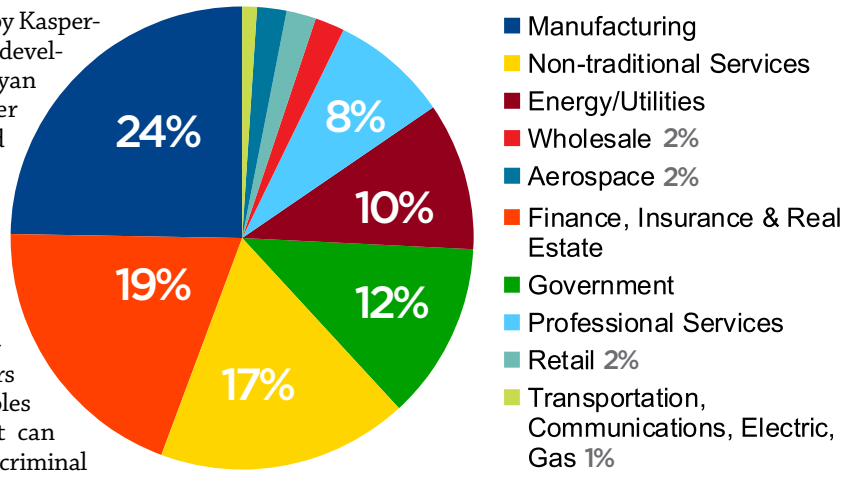
Koh says SMEs need to create awareness on security, educate employees about threats and assess their security status.

Sat says SMEs should ensure that they have updated all their applications to the latest version as the first step to a secure IT environment. FocusM

Targeted attacks (by company size)



Targeted attacks (by industry)



BYOD 'feeds' mobile malware

THE proliferation of mobile malware, which increased by 58% in 2012 from the previous year, is attributed largely to the growing Bring-Your-Own-Device (BYOD) trend. About 32% of all mobile malware is geared at information-stealing, followed by traditional threats at 25%, user-tracking at 15% and content-sending at 13%.

For example, mobile users receive an email with a link to an application. Once downloaded, the app steals all contact information and sends emails to these contacts promoting the same app, which is how the mobile malware spreads.

Symantec Malaysia senior technical consultant Koh Ee Laine warns that SMEs that use mobile devices or allow employees to bring their own devices face a serious security problem, as these devices are unmanaged and can be the weak link allowing attackers into the company's local network or giving them access to sensitive company information.

"They [SMEs] have to ensure that employee access to corporate information is protected by encryption or put in security measures," she adds.

Kaspersky Lab SEA business development manager Bryan Sat says BYOD is a huge risk for companies as there have been countless incidents in which a lost device has led to leaks of confidential business data, which in turn lead to financial penalties and a poor reputation.