The Changing Face Of The Cyber Criminal

Discover how the evolving cyber criminal underground is changing the online threat landscape as we explore into the top emerging business security trends affecting Small- and Medium-Businesses (SMBs) today.

**THE GOOD, THE BAD AND THE UGLY**

As we arrive at a new informative era characterized by the data explosion across various digital media, we now witness the emergence of new collaborative technologies, mobile applications and devices, and P2P networks in the SMB landscape. Along with the cautious spending trend tightening the reins on IT budgets and expenditure, this has forced the hands of business owners to leverage on more affordable applications and services to cope with the rising cost and productivity demands of an increasingly-pervasive web and turbulent business environment.

First, the good news. Monitoring web and network access, authentication, intrusion prevention and detection, online user protection, securing business information, et al has always been a perennial business concern. And the bad? With the advent of online collaboration, information and data exchanges across more liberal channels such as social networking platforms, mobile applications and devices, remote computing and cloud services, the security task has just been tilted further uphill.

Your security nightmare has just begun.

**THE CYBER CRIMINAL UNDERGROUND ECONOMY**

As we descend into deep, dark realms of the cyber criminal underworld, it is critical to understand the anatomy of the increasingly-sophisticated cyber criminal economy. With the real world painting a gloomy picture of rising global unemployment, the world of cyber crime now presents an ideal, attractive alternative for the jobless IT-competent and tech-savvy.

---

Do You Know?

75 per cent of businesses have suffered a cyber attack in the past 12 months, losing an average of US$2 million annually.

Source: SearchSMB
They Are Everywhere...
Cyber criminals, who are often part of global syndicates, can remotely control all of the machines in a “botnet” whilst retaining almost complete anonymity. This occurs when these cyber criminals get together to infect, or hijack a large number of computers to achieve a common purpose. And you can be part of a “botnet” – without even being aware of it. The phenomenal rise of the “botnet” was epitomised by the launch of the legendary Conficker worm. When it was first unleashed in November 2008, it represented the biggest “botnet” to have ever hit the Internet, with Symantec first estimating 6.5 million infected machines (with this figure having been reported to have risen up to over 15 million recently). It made such big news that it forced technology bigwigs Microsoft into offering a $250,000 bounty for anyone who could offer information on the cyber criminals who was involved in the original infection. While its existence has been questioned in recent times, many still fear the awakening of the dormant Conficker worm. It may have left many people’s memories, but it certainly hasn’t left all of their machines.

The cyber criminal community is growing, as displayed by the increasing numbers of security breaches and cyber crimes reported recently. As two security researchers tried to justify the probable cause behind, “A lot of people we were talking to were not really very sophisticated. All it really requires is a little bit of time, reaching out to the right people, getting the right tools and then deploying them.”

And They Are Evolving
What exactly does this mean? Cyber criminals are now innovating their strategies – studying novel means and methods – to hurt your business.

But haven’t they been doing this all along? Where’s the scary part?
Well, they’re just getting warmed up.

HOW CYBER CRIME IS EVOLVING

<table>
<thead>
<tr>
<th>CYBER ATTACKS HURT BUSINESSES:</th>
<th>75 per cent of enterprises have suffered a cyber attack in the past 12 months, losing an average of USD $2 million annually.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CREDIT CARDS ARE NUMBER ONE ITEM FOR SALE:</td>
<td>Credit Card information is the most commonly advertised item for sale on the underground economy, accounting for 18 per cent of all goods and services.</td>
</tr>
<tr>
<td>BANKS GET PHISSED:</td>
<td>76 per cent of brands used in Phishing attacks in 2010 were in the financial sector.</td>
</tr>
<tr>
<td>OUT WITH TRADITIONAL SPAM, IN WITH TARGETED SCAMS:</td>
<td>The total number of scam and Phishing messages came in at 21 per cent of all spam, which is the highest level recorded since 2007.</td>
</tr>
<tr>
<td>NEWS AGENDA DRIVES ATTACKS:</td>
<td>Natural disasters such as the earthquake in Haiti drove up the volume of scam and Phishing messages as spammers used the tragic event to their benefit.</td>
</tr>
<tr>
<td>CYBER CRIMINALS FOLLOW THE MASSES:</td>
<td>In Asia Pacific and Japan, the top web-based attack for Oct – Dec 2009 was related to the Microsoft® Internet Explorer ADODB.Stream Object File Installation Weakness, which accounted for 41 per cent of the total.</td>
</tr>
<tr>
<td>INCREASING POPULARITY OF NEW PLATFORMS WILL DRIVE NEW ATTACKS:</td>
<td>Whilst an increase in iPad related search terms for SEO attacks and phishing attacks were observed during the Apple iPad launch.</td>
</tr>
<tr>
<td>CYBER CRIMINALS AFTER INFORMATION RATHER THAN INFRASTRUCTURES:</td>
<td>Theft of intellectual property was reported as the top cyber loss for Singapore businesses.</td>
</tr>
</tbody>
</table>

Source: SearchSMBAsia
FORGET CONFICKER, HERE COMES KOOBFACE

Gone were the days when hackers were cracking computers simply for fame, where spreading worms and virus were for the sole purpose of a quick thrill, with “glory” the biggest name of the game. Albeit having our usual viruses, Trojans and worms still hanging around, recent developments has witnessed more sophisticated and blended threats – on a much more potent scale.

We now witness larger amounts of spam emails (A MessageLabs survey report recently revealed that 83 per cent of all spam originates from “botnet” controlled computers1), and more potent forms of denial of service (DDoS) attacks with new “botnets” such as the recent Web 2.0 “botnet” – Koobface virus which infected thousands of Facebook and MySpace users, effectively dwarfing the impacts previously felt during the Conficker peak. Other malware threats such as FAKEAV variants use different social engineering tactics such as spammed messages or fake codecs, to trick users into downloading and installing FAKEAV into their systems.2 Most recently, FAKEAV created a storm when it preyed on unsuspecting users while posing under the guise of legitimate anti-virus application downloads.

In addition to these, because “botnets” are controlled remotely, cyber criminals can leverage on software such as key loggers to steal passwords and confidential personal information. What are the implications to this? Data security threats have become more sophisticated, as perpetrators take advantage of increasingly sophisticated tools and techniques to pilfer confidential information for illegal gains.3

More bank accounts and social networking profiles are becoming increasingly susceptible to security breaches with Phishing, key loggers, botnets, “drive-bys” now presenting the biggest forms of malware threats used to harvest information, computers, access corporate networks or retrieve personal data.

THE GLOBAL CYBER CRIME WAVE

The largest hacker loot – of 130 million credit card numbers – was achieved by SQL injection in August 2009.

In June 2009, more than 40,000 websites were hit by a mass-compromise attack dubbed “Nine Ball” that injected malware into pages and redirected victims to a site that attempted to download further malware.

In May 2009, a series of rapidly spreading website compromises known as “Gumblar” garnered media headlines. Gumblar-infected sites delivered key loggers and other malware to visitors.

In February 2009, my.barackobama.com, the Obama campaign blogging site, was used to deliver malware infecting content to visitors. The travel website of the US government, govtrip.com, was also hacked into and used to distribute malware to other government agencies.


This represents perhaps the most significant development in the cyber criminal landscape as perpetrators are now empowered to commit financial and intellectual fraud and threats at ease, as well

---

1 Botnets responsible for 83% of All Spam, Lee, 16 July 2009

2 Unmasking FAKEAV, Trendmicro White Paper, June 2010

EMERGING TRENDS IN BUSINESS SECURITY:
THE NEXT CYBER CRIME FRONTIERS

As we explore into the following emerging trends in business security, what should you look out for in 2010 that can aid in your preparation for the planning, strategizing and implementation of various security solutions to counter these emerging security threats?

P2P marks the spot
According to security research experts, the coming year will see a shift from attacks via websites and applications towards attacks originating from file-sharing (P2P) networks. With this method having already seen its debut over previous years in the forms of TDSS and Virut as well as the first backdoor for Mac OS X, 2010 will witness a proliferation for this category of attacks.

Vying for “cash” traffic
Cyber criminals will be looking towards commercial gains as they compete for traffic. The modern cyber criminal world is making more efforts to legalize itself in a bid to earn money online via traffic, which can be acquired via “botnets”. “Grey schemes” and “partner programs” will become the order of the day, where “botnet” owners stand to profit from spam blasts, different variants of DoS attacks and malware distribution.

Mobility – the next cyber crime vehicle
According to recent research reports, the mobile sector is earmarked as the new frontier for fraud irresistible to cyber criminals. In particular, the iPhone and Android will witness an increase in cyber attacks in 2010. The first malicious programs for these mobile platforms appeared in 2009. With the increasing popularity of mobile phones running the Android OS combined with a lack of effective checks to ensure secure third-party software applications, this will lead to a number of high profile malware outbreaks.

Is your business vulnerable?
This is the biggest security question for SMBs as detection of new vulnerabilities will become the greatest challenge in 2010. These vulnerabilities will be detected in both software developed by third parties (such as Adobe, Apple, etc.) and in Windows 7, the new operating system that has just entered the market. SEO (search engine optimization) strategies for your business in order to reach out to this new group of customers?
SMB SOLUTIONS FOR THE NEW ONLINE THREAT LANDSCAPE

Prioritize your security needs
SMBs must prioritize against the IT security threats they face. By having simple firewalls, VPN or data encryption, this will not be enough to insulate your business from threats such as fraud and identity theft anymore. Preventing fraud, more likely from tech-enabled social engineering than sophisticated hacking, must be front-and-center for SMBs.

Hosted security as your key to business continuity
With the online threat environment becoming increasingly sophisticated, the deployment of traditional security controls is no longer sufficient against evolving technologies and attack techniques. Finding, training and retaining knowledgeable security personnel is also a challenge for most SMBs with limited budgets. The answer to this complex challenge lies in a company's ability to leverage on the ideal combination of people, processes and technology. Along with hosted security solutions specially-designed to help deliver real-time protection and strengthen overall defenses against ever-evolving threats, this will ensure only authorized users have access to internal network resources.

Take a new business-driven approach
Finally, by taking a holistic approach toward business-driven security, this will help SMBs manage risk and orchestrate security operations in a way that enforces compliance and optimizes business results. SMBs can also ensure that its various security domains work together in a holistic and synergetic manner, in alignment with business objectives. Aligning IT security with a business-driven approach can also place organizations in a favourable position in line with meeting unique business objectives and driving compliance goals.
# KEY SUMMARY

The data explosion in the new informative era and a cautious spending trend has given rise to a greater challenge in coping with the rising cost and productivity demands of an increasingly-pervasive web and turbulent business environment.

Cyber criminals often operate as part of global syndicates, or “botnets”, in complete anonymity.

Businesses can have their systems infected, and be part of a “botnet” without even being aware.

Sophisticated data security threats are the currently the biggest concern for SMBs as perpetrators take advantage of advanced tools and techniques to pilfer confidential information for illegal (and often commercial) gains.

File-sharing (P2P) networks will be a main target for cyber criminals in 2010.

“Botnet” owners will be vying for traffic via “grey schemes” and “partner programs” to make commercial gains.

The mobile sector is earmarked as the new frontier for fraud irresistible to cyber criminals.

Detection of new vulnerabilities will become the greatest business challenge for 2010.

SMBs should prioritize security needs in the face of increasingly-sophisticated threats.

Hosted security services can help enable business continuity.

Taking a new holistic approach toward business-driven security can help SMBs manage risks and orchestrate security operations better.